МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

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

М. В. Афанасьєв

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ 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):
Євсеєв С.П, д.т.н., с.н.с., завідувач кафедри КІТ
Гаврилова А. А. 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:

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.

Організаційні заходи відіграють важливу роль у створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей найчастіше обумовлені не тільки технічними аспектами, а й зловмисними діями, а також недбальством, недбалістю, халатністю користувачів або обслуговуючого персоналу, що ігнорує елементарні правила захисту. Закони та нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, що створюються в державі, відомствах, установах і організаціях. При розгляді питань захисту інформації така діяльність розглядається як організаційні методи забезпечення.

В інформаційних системах організаційні заходи виконують стрижневу роль в реалізації комплексної системи захисту інформації. Тільки за їх допомогою можливе об'єднання на правовій основі інженерно-технічних, програмно-апаратних, криптографічних та інших засобів захисту інформації в єдину комплексну систему.

Мета навчальної дисципліни:

Метою викладання дисципліни є формування теоретичних знань щодо проведення аналізу і оцінки загроз інформаційній безпеці об'єкта, оцінки збитків внаслідок протиправного розкриття інформації обмеженого доступу, організації і забезпечення режиму таємності, підбору, розстановки і роботи з кадрами.

Курс	**4**	
Семестр	**7**	
Кількість кредитів ECTS	**4**	
Аудиторні навчальні заняття	**лекції**	**24**
	семінарські, практичні	**–**
	лабораторні	**24**
Самостійна робота		**72**
Форма підсумкового контролю	**екзамен**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Забезпечення інформаційної безпеки	Проектування систем захисту мереж наступного покоління
Організація та інформаційне забезпечення управлінської діяльності	Теорія ризиків
Комплексні системи захисту інформації	Переддипломна практика

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
засвоєння основ побудови організаційного захисту інформації на підприємстві	Знати класифікацію всіх можливих на сьогоднішній день загроз інформаційній безпеці підприємства
розроблення превентивних заходів щодо запобігання виникнення загроз інформаційній безпеці підприємства	Знати існуючі способи несанкціонованого доступу та вміти розробляти превентивні заходи щодо запобігання виникнення загроз інформаційній безпеці підприємства
розроблення структури служби безпеки підприємства	Знати та вміти розробляти типову структуру служби безпеки для підприємства
підбору персоналу до служби безпеки підприємства	Знати та вміти проводити процедуру відбору персоналу на роботу до служби безпеки підприємства
здатність організовувати технологічний процес захисту інформації обмеженого доступу	Знати та контролювати життєвий цикл секретної документації

3. Програма навчальної дисципліни

Змістовий модуль 1. Роль організаційного забезпечення при здійсненні захисту інформації

Тема 1. Завдання організаційного забезпечення захисту інформації

Загальна характеристика інформаційної діяльності. Види інформаційної діяльності. Напрями інформаційної діяльності. Складові інформаційної діяльності: наукова (аналітико-синтетична) обробка документів, Науково-технічна обробка документів.

Організаційно-технічні та організаційно-правові заходи методи захисту інформації. Основні властивості методів і засобів організаційного захисту.

Роль організаційних заходів в створенні надійного механізму захисту інформації. Завдання, які вирішуються на організаційному рівні для забезпечення безпеки функціонування інформації

Тема 2. Аналіз і оцінка загроз інформаційної безпеки об'єкта щодо його організаційного забезпечення

Класифікація загроз щодо інформаційної безпеки за базовими ознаками. Три основних види загроз

Тема 3. Оцінка збитків внаслідок протиправного розкриття інформації обмеженого доступу і заходи щодо його локалізації

Перелік інформації з обмеженим доступом: державна, комерційна, банківська, професійна, службова таємниці, персональні дані і інтелектуальна власність. Огляд способів несанкціонованого доступу. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією. Показник критерію ступеня відсутності або наявності завданої об’єкту матеріальної та моральної шкоди. Параметри вартості ризику від настання події

Тема 4. Служба безпеки об'єкта

Основні завдання служби безпеки. Принципи системи безпеки підприємства. Функції служби захисту інформації підприємства. Перелік підрозділів служби безпеки об'єкта обробки інформації або підприємства і їх функції

Тема 5. Підбір, розстановка і робота з кадрами

Етапи процедури відбору персоналу. Перевірка персоналу на благонадійність. Процес перевірки керівних кадрів. Укладання контрактів та угод про секретності. Особливості звільнення співробітників, які володіють конфіденційною інформацією. Підбір, розстановка і робота з кадрами служби безпеки. Дотримання трудової дисципліни і законності, зміцнення фізичного розвитку, здоров'я, підвищення культури. Соціальний захист персоналу служби безпеки.

Змістовий модуль 2. Заходи з організації забезпечення захисту інформації на підприємствах

Тема 6. Організація і забезпечення режиму таємності

Особливості режиму секретності. Порядок організації режиму секретності. Закриті роботи режиму секретності. Документи, регламентуючі роботу підрозділів із захисту державної таємниці. Права працівників підрозділів із захисту державної таємниці. Основні завдання постійно діючих технічних комісій. Структура і зміст переліку відомостей, що становлять конфіденційну інформацію підприємства. Порядок допуску співробітників до відомостей, що становлять комерційну таємницю. Життєвий цикл документів, які містять комерційну таємницю.

Тема 7. Організація пропускного, внутрішньооб'єктового і протипожежного режиму

Заходи, які регламентує пропускний режим. Встановлення відповідальності за забезпечення пропускного режиму і збереження матеріальних цінностей у структурних підрозділах. Документація з пропускного режиму.

Заходи внутрішньооб'єктового режиму.

Забезпечення протипожежного режиму

Тема 8. Захист інформації при аваріях та інших екстремальних ситуаціях

Особливості інформаційного впливу в екстремальних умовах. Превентивні заходи. Питання, які вирішуються і документуються при складанні попереджувального плану дій. Перелік відомостей плану дій.

Тема 9. Забезпечення захисту інформації при здійсненні міжнародного науково-технічного та економічного співробітництва

Джерела та канали поширення конфіденційної інформації.

Лабораторні заняття

Тема 1. Розробити організаційну структуру відділу захисту інформації в межах організаційної структури підприємства

Тема 2. Розробити посадові інструкції відділу захисту інформації підприємства з врахуванням міжпосадових зв'язків та зв'язків з відділами підприємств

Тема 3.Визначення функцій системи захисту інформації підприємства

Тема 4. Формування вимог щодо внутрішньооб'єктового режиму

Тема 5. Розробка вимог щодо забезпечення охорони підприємства

Тема 6. Проведення оцінки персоналу за допомогою модуля "HR" середовища "1С "Підприємство: Управління підприємством "

Тема 7.Підбір, набір та облік кадрів за допомогою модуля "HR" середовища "1С "Підприємство: Управління підприємством "

Тема 8.Контроль участі персоналу у заходах за допомогою модуля "HR" середовища "1С "Підприємство: Управління підприємством "

Тема 9.Контроль за проведенням підвищення кваліфікації персоналом за допомогою модуля "HR" середовища "1С "Підприємство: Управління підприємством "

Тема 10.Розроблення вимог щодо організації пропускного режиму на підприємстві

Тема 11.Розроблення плану заходів та проведення аналітичної роботи щодо організації захисту інформації на підприємстві. Представлення результатів за допомогою ресурсу створення карти розуму

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 та 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 5 практичних ситуацій (два стереотипних, два діагностичних 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	Поточні КР	Екзамен	Усього
Роль організаційного забезпечення при здійсненні захисту інформації	**Тема 1**	1тиждень	0,5	2				2,5
	Тема 1	2 тиждень	0,5	2				2,5
	Тема 2	3 тиждень	0,5	2				2,5
	Тема 3	4 тиждень	0,5	2				2,5
	Тема 3	5 тиждень	0,5	2				2,5
	Тема 4	6 тиждень	0,5	2	3			5,5
	Тема 4	7 тиждень	-	3				3
	Тема 5	8 тиждень	0,5	2		10		12,5
Заходи з організації забезпечення захисту інформації на підприємствах	**Тема 5**	9 тиждень	-	2				2
	Тема 6	10 тиждень	1	-				1
	Тема 7	11 тиждень	-	3				3
	Тема 8	12 тиждень	1		3			4
	Тема 8	13 тиждень	-	3				3
	Тема 9	14 тиждень	0,5			10		10,5
	Тема 9	15 тиждень	-	3				3
	Екзамен						40	40
Усього			6	28	6	20	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. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

2. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.

3. Логінова Н. І. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

4. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

5.2 Додаткова

5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.

6. Яремчук Ю. Є. Дослідження комбінаційних характеристик вітчизняних радіо непрозорих тканин М1, М2 та М3 / Ю. Є. Яремчук, В. С. Катаєв, В. В. Сінюгін // Реєстрація, зберігання та обробка даних. – 2015. – Том 17. №3 – С. 56-65.

7. Яремчук Ю. Є. Дослідженняя характеристик вітчизняних радіо непрозорих тканин Н1, Н2 та Н3 при різних комбінаціях їхнього застосування / Ю. Є. Яремчук, В. С. Катаєв, М. Ю. Гижко, П. В. Павловський // Реєстрація, зберігання та обробка даних. – 2016. – Том 18, № 1. – С. 42-51.

5.3 Інформаційні ресурси в мережі Інтернет

8. НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" – К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 2000. [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_1023_75718671.pdf]

9. НД ТЗІ 2.7-011-2012 "Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних

пристроїв". – 2012 [Електронний ресурс]. – Режим доступу : [http://www.dut.edu.ua/uploads/l_5623_75714589.pdf].

10. Про затвердження Змін до Зводу відомостей, що становлять державну таємницю / 27 березня 2019 р. за N 306/33277 [Електронний ресурс]. – Режим доступу : [http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920].

11. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс]. – Режим доступу : [http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=302408&cat_id=89734&ctime=1547122731920].