

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ



"ЗАТВЕРДЖУЮ"

Заступник керівника

(професор з науково-педагогічної роботи)

М.В. Афанасьєв
М.В. Афанасьєв

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

робоча програма навчальної дисципліни

Галузь знань
Спеціальність
Освітній рівень
Освітня програма

12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"
125 "КІБЕРБЕЗПЕКА"
перший(бакалаврський)
"КІБЕРБЕЗПЕКА"

Вид дисципліни
Мова викладання, навчання та оцінювання

базова
українська

*Завідувач кафедри кібербезпеки
та інформаційних технологій*

Євсєєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 6 від 10.12.2019 р.

Розробник(-и):
Мілевський С. В., к.е.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:

Дисципліна присвячена вивченню основ менеджменту інформаційної безпеки. В дисципліні передбачено вивчення 16 навчальних тем, об'єднаних єдиним задумом. Викладаються погляди на інформацію, як об'єкт захисту з виділенням характерних властивостей інформації, що захищається. На основі єдиного підходу розглядаються напрямки управління інформаційною безпекою. Викладаються моделі управління процесом інформаційного захисту. Завершується вивчення дисципліни двома темами, присвяченими двом найбільш істотним загрозам інформаційної безпеки - інформаційним злочинам та інформаційним війнам. В рамках зазначених тем наводиться класифікація інформаційних і комп'ютерних злочинів, пояснюються їх причини, дається кримінально-правова характеристика деяких злочинних діянь, розглядаються основні стратегії інформаційних воєн і види інформаційної зброї.

Мета навчальної дисципліни: формування у студентів знань в області теоретичних основ управління інформаційною безпекою; навичок практичного забезпечення захисту інформації та безпечного використання програмних засобів в обчислювальних системах.

Курс	2	
Семестр	4	
Кількість кредитів ECTS	5	
Аудиторні навчальні заняття	лекції	32
	семінарські, практичні	16
	лабораторні	26
Самостійна робота	76	
Форма підсумкового контролю	залік	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Операційні системи	Забезпечення інформаційної безпеки
Вища математика	Адміністрування в інформаційних системах
	Бази даних
	Обчислювальні системи, мережі та телекомунікації
	Інформаційні системи та технології

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
здатність розуміти сутність і проблеми розвитку сучасного інформаційного суспільства	здатність усвідомлювати соціальну значущість своєї майбутньої професії, володіти високою мотивацією до виконання професійної діяльності
здатність працювати з інформацією в глобальних комп'ютерних мережах	здатність самостійно здобувати і використовувати в практичній діяльності

Компетентності	Результати навчання
	нові знання і вміння, прагне до саморозвитку
здатність використовувати нормативні правові документи у професійній діяльності	здатність усвідомлювати небезпеку і загрози, що виникають в процесі розвитку сучасного інформаційного суспільства
дотримуватися основних вимог інформаційної безпеки	здатність здійснювати і обґрунтовувати вибір проектних рішень за видами забезпечення інформаційних систем

3. Програма навчальної дисципліни

Змістовий модуль 1. Інформаційна безпека та рівні її забезпечення

Тема 1. Передумови і основні напрямки розвитку менеджменту в сфері інформаційної безпеки

Проблема інформаційної безпеки суспільства. Визначення поняття "інформаційна безпека"

Тема 2. Діяльність міжнародних організацій у сфері інформаційної безпеки. Робота міжнародних професійних об'єднань:

International Telecommunication Union (ITU) - Міжнародний союз електрозв'язку

Institute of Electrical and Electronics Engineers (IEEE) - Інститут інженерів з електроніки та електротехніки

Association for Computing Machinery (ACM) - Асоціація обчислювальної техніки

World Wide Web Consortium (W3C) - Консорціум Всесвітньої Павутини

International Organization for Standardization (ISO) - Міжнародна організація по стандартизації

Тема 3. Діяльність спеціалізованих міжнародних організацій і об'єднань в сфері інформаційної безпеки:

CERT Coordination Center (CERT / CC) - Координаційний центр CERT

X-Force security intelligence team - Дослідницька група X-Force

Альянси великих технологічних компаній

Smart Card Alliance (SCA) - Альянс за смарт-картками

Internet Security Alliance (ISA) - Альянс з безпеки мережі Інтернет

The International Biometric Industry Association (IBIA) - Міжнародна асоціація компаній-виробників біометричного устаткування

Тема 4. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.

Загальна методологія організаційного забезпечення інформаційної безпеки на рівні великих постачальників інформаційних систем

Тема 5. Організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній (Корпорація Microsoft, Корпорація Cisco Systems)

Управління інформаційною безпекою в Microsoft. Розробки та протоколи інформаційної безпеки компанії Cisco.

Тема 6. Управління інформаційною безпекою на державному рівні: Загальні принципи і українська практика.

Передумови розвитку державного управління в сфері інформаційної безпеки.

Тема 7. Загальна методологія і структура організаційного забезпечення інформаційної безпеки на рівні держав.

Спеціальні державні структури та їх роль в забезпеченні інформаційної безпеки. Документи з оцінки захищеності автоматизованих систем

Тема 8. Організаційне забезпечення інформаційної безпеки на державному рівні: практика США.

Загальна політика США у сфері інформаційної безпеки. Структура органів державної влади, що забезпечують інформаційну безпеку в США. Федеральні програми та ініціативи, підтримувані державою

Змістовий модуль 2. Механізми забезпечення управління інформаційною безпекою

Тема 9. Менеджмент інформаційної безпеки на Рівні підприємства: основні напрямки и структура політики безпеки.

Передумови розвитку менеджменту в сфері інформаційної безпеки на Рівні підприємств. Загальна структура управлінської роботи по забезпечення інформаційної безпеки на Рівні підприємства. Формування політики інформаційної безпеки на підприємстві. Структура політики інформаційної безпеки та процес її розробки. Політика інформаційної безпеки підприємства: верхній рівень. Політика інформаційної безпеки підприємства: середній рівень

Тема 10. Зміст деталізованої політики безпеки. Політика інформаційної безпеки підприємства: Нижній рівень.

Стандарти інформаційної безпеки на підприємстві. Сімейство стандартів управління інформаційною безпекою

Тема 11. Департамент інформаційної безпеки та робота з персоналом.

Департамент інформаційної безпеки. Організаційна структура і персонал департаменту інформаційної безпеки. Робота з персоналом підприємства.

Тема 12. Організація реагування на надзвичайні ситуації (інциденти).

Класи загроз в інформаційній безпеці. Канали несанкціонованого доступу до інформації.

Тема 13. Аудит стану інформаційної безпеки на підприємстві.

права працівників на доступ до серверів і баз даних колективного використання;

способи підтвердження входу кожного користувача (аутентифікація);

принципи резервного копіювання даних;

конфігурація і налаштування мережевих пристроїв, систем зберігання та передачі даних;

робота антивірусного і антишпигунського програмного забезпечення, наявність ліцензії;

теоретичні та практичні знання працівників підприємства про захист даних.

Тема 14. Програмні засоби, що підтримують управління інформаційною безпекою на підприємстві.

Використання програмних засобів для підтримки управління безпеки. Програмна підтримка роботи з політикою безпеки. Програмна підтримка аналізу ризиків. Програмні засоби, що інтегруються в інформаційну систему підприємства.

Тема 15. Надання послуг в сфері інформаційної безпеки.

Передумови розвитку Сайти Вся послуг Із забезпечення інформаційної безпеки и его структура. Особливості Деяк відів услуг. Інфраструктура публічних

ключів. Страхування інформаційних ризиків. Основи Методології страхування інформаційних ресурсів. Ринок страхових послуг.

Тема 16. Економіка інформаційної безпеки.

Методичні основи економіки інформаційної безпеки. Аналіз вкладень в засоби захисту інформації.

Лабораторні роботи:

Лабораторна робота 1. Налаштування параметрів IP ОС Windows для її безпечного функціонування. Статична маршрутизація

Лабораторна робота 2. Встановлення та конфігурування систем Firewall (в ОС Windows та Ubuntu). Розробка політики міжмережевої взаємодії

Лабораторна робота 3. Налаштування безпечного віддаленого доступу за технологією VPN на базі ОС Windows та Ubuntu

Лабораторна робота 4. Конфігурування та випробування стійкості захищених бездротових систем передачі даних (Wi-Fi)

Практичні заняття:

Практичне заняття 1. Аналіз стану існуючої інформаційної системи організації. Аналіз вимог до ІС

Практичне заняття 2. Стратегічне та оперативне планування ІС організації

Практичне заняття 3. Управління ризиками впровадження та використання ІС

Практичне заняття 4. Оцінка економічної ефективності системи інформаційного захисту

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, практичні, 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 та практичних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума, що дозволяє студенту отримати позитивний результат – 60 балів);

модульний контроль, що проводиться у формі контрольної роботи, 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.

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

здатність до використання інформаційних і комунікаційних технологій з метою управління інформаційною безпекою;

здатність проводити дослідження у практичній професійній діяльності.

Результати навчання:

розробляти проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних

усвідомлювати небезпеку і загроз, що виникають в процесі розвитку сучасного інформаційного суспільства

здійснювати і обґрунтовувати вибір проектних рішень за видами забезпечення інформаційних систем

виконувати налаштування інформаційних систем та комунікаційного обладнання.

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

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 заліку, 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	Практичні заняття	Контрольна робота	Усього
ЗМ1	1	Тема 1	1 тиждень	1	3			4
	2	Тема 2	2 тиждень	1	3	3		7
	3	Тема 3	3 тиждень	1	3			4
	4	Тема 4	4 тиждень	1		3		4
	5	Тема 5	5 тиждень	1	3			4
	6	Тема 6	6 тиждень	1	3	3		7
	7	Тема 7	7 тиждень	1	3			4
	8	Тема 8	8 тиждень	1		3	10	14
ЗМ2	9	Тема 9	9 тиждень	1	3			4
	10	Тема 10	10 тиждень	1	3	3		7
	11	Тема 11	11 тиждень	1	3			4

Теми змістового модуля				Лекційні заняття	захист лабораторних робіт	Практичні заняття	Контрольна робота	Усього
12	Тема 12	12 тиждень		1		3		4
13	Тема 13	13 тиждень		1	3			4
14	Тема 14	14 тиждень		1	3	3		7
15	Тема 15	15 тиждень		1	3			4
16	Тема 16	16 тиждень		1	4	3	10	18
Усього				16	40	24	20	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		
60 – 63	E	задовільно	Не зараховано
35 – 59	FX	незадовільно	
1 – 34	F		

5. Рекомендована література

5.1. Основна

1. Баскаков А. В., Остапенко А. Г., Щербаков В. Б. Политика информационной безопасности как основной документ организации // Информационная безопасность. 2016. - №2. – С. 43-47.
2. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. – Режим доступа: <http://znanium.com>
3. Белов Е.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов, Гелиос АРВ, 2006.
4. Борисова К. В., Кудашкин Я. В. Международная информационная безопасность как основополагающий фактор национальной безопасности// Сборник научных трудов. Национальная безопасность: противодействие экстремизму и терроризму и перспективы преодоления глобальных проблем. – 2016. – С. 68-73.
5. Галушкин А. А. К вопросу о значении понятий «национальная

безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. – 2015. - №2. – С. 8.

6. Государственная тайна и её защита. Серия «Закон и право» М.: Ось-89, 2004 г.

7. Дойникова Е. В. Оценивание защищенности информационных систем и реагирование на инциденты информационной безопасности с учетом текущей ситуации по безопасности // Материалы конференции «Информационные технологии в управлении». – 2014. – С. 601-604.

8. Дорожкин А.В., Ясенев В.Н. Информационная безопасность как инструмент обеспечения экономической безопасности хозяйствующего субъекта. Журнал «Экономика и предпринимательство», № 5 (1), 2015.

9. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции. Журнал «Вопросы кибербезопасности» №1 (2) – 2014.

10. Жукова М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб.пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2012. – Режим доступа: <http://znanium.com>

11. Защита конфиденциальной информации: учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. – М.: ФОРУМ, 2009. - 256 с.: ил. - (Высшее образование).

12. Зегжда Д.П., Ивашко А.М.. Основы безопасности информационных систем. М., Горячая линия-Телеком, 2005.

13. Зефилов С. Л., Голованов В. Б. Система менеджмента информационной безопасности организации // Труды международного симпозиума «Надежность и качество». – 2016. – С. 364-366.

14. Информационная безопасность гос.организаций. [Электронный ресурс]: http://library.tuit.uz/skanir_knigi/book/infor_bezop/infor_2.htm

15. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. – Режим доступа: <http://znanium.com>

16. Мельников В.П. Информационная безопасность и защита информации: учебное пособие для вузов.- М.: Академия, 2008.- 336 с.

17. Тенденции кибербезопасности в 2016 году [Электронный ресурс]: краткое руководство по наиболее важным выводам в области безопасности.- Электрон.дан.- М.: Корпорация Майкрософт, 2016.- Режим доступа: <https://www.microsoft.com/ru-ru/security/default.aspx>.

18. Цюк О. А. Международная организация по стандартизации // Мир науки, культуры и образования. – 2014. - №4. – С. 67-78.

19. Юсупов Р. М., Шишкин В. М. Информационная безопасность, кибербезопасность и смежные понятия // Информационное противодействие угрозам терроризма – 2016. - №1. – С. 27-35.

5.2. Інформаційні ресурси в Інтернеті

20. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Менеджмент інформаційної безпеки” <https://pns.hneu.edu.ua/course/view.php?id=4924>