МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М.П. ДРАГОМАНОВА

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Методичні рекомендації до підготовки
та проведення практичних занять

для студентів спеціальності
029 «Інформаційна, бібліотечна та архівна справа»
галузі знань 02 «Культура і мистецтво»

Київ 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ М.П. ДРАГОМАНОВА

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

Методичні рекомендації до підготовки
та проведення практичних занять

для студентів спеціальності
029 «Інформаційна, бібліотечна та архівна справа»
галузі знань 02 «Культура і мистецтво»

Київ 2018

УДК 378.091.33-027.22:004-049.5
І-74

Друкується за рішенням Вченої ради
Навчально-наукового інституту неперервної освіти
НПУ імені М.П. Драгоманова
(протокол № 6 від «21» грудня 2017 р.)

Рецензенти:
Луцик І.Б. – кандидат технічних наук, доцент кафедри комп'ютерних технологій Тернопільського національного педагогічного університету імені В. Гнатюка;
Войтович І.С. – доктор педагогічний наук, професор, завідувач кафедри комп'ютерної інженерії та освітніх вимірювань НПУ імені М.П. Драгоманова.

І-74 Інформаційна безпека та захист інформації: Методичні рекомендації до підготовки та проведення практичних занять для студентів спеціальності 029 «Інформаційна, бібліотечна та архівна справа». / Укл. О.М. Фендьо, О.І. Охмуш-Ковалевська, О.В. Галицький. – К.: Вид-во НПУ імені М.П. Драгоманова, 2018. – 32 с.

У методичному виданні представлено рекомендації до підготовки та проведення практичних занять з дисципліни «Інформаційна безпека та захист інформації» для фахової підготовки студентів за спеціальністю 029 «Інформаційна, бібліотечна та архівна справа». У методичному виданні представлено: тематичний план дисципліни; тематику лекційних занять з рекомендованою літературою; плани практичних занять та контрольні запитання для самоперевірки студентів; перелік питань для підготовки до заліку з навчальної дисципліни «Інформаційна безпека та захист інформації»; список рекомендованої літератури.

Представлений матеріал дає змогу в цілому ознайомитись зі структурою навчальної дисципліни «Інформаційна безпека та захист інформації» та перейти до більш глибокого вивчення під час підготовки до практичних занять. Поєднання теоретичних відомостей і вказівок щодо виконання поставлених завдань дає змогу студентам отримати практичні навики реалізації набутих знань.

Тематика лекційних та практичних занять корелює з навчальною програмою дисципліни «Інформаційна безпека та захист інформації».

© О.М. Фендьо, О.І. Охмуш-Ковалевська, О.В. Галицький, 2018

ПЕРЕДМОВА

Глобальна інформатизація суспільства, яка пов’язана з нестримним розвитком інформаційних технологій та практично необмеженим використанням мережі Інтернет, вимагає захисту основного ресурсу сучасності – інформації. Перехід державних та приватних установ на електронний документообіг, а також впровадження електронних паспортів, електронних платіжних систем, електронних медичних карток та ін. вимагають надійного захисту даних від несанкціонованого втручання.

В епоху інформаційних воєн зросли вимоги щодо методів отримання, передачі та обробки інформації, в тому числі державної, військової, комерційної та персональної інформації. Тому сучасні технології, методи та засоби захисту інформації набувають першочергового значення та вимагають детального вивчення.

Метою вивчення дисципліни «Інформаційна безпека та захист інформації» є засвоєння студентами сучасних методів захисту інформації (зокрема технічного, інженерного, криптографічного та організаційного); вивчення нормативно-законодавчої бази України щодо захисту інформації; придбання практичних навичок реалізації захисту персональних даних в процесі введення, виведення, передавання, оброблення, накопичення і зберігання; застосування заходів та засобів, спрямованих на технічний захист інформації на об’єктах інформаційної діяльності.

Основними завданнями вивчення дисципліни є: формування у студентів знань про інформаційну безпеку та захист документної інформації; вивчення принципів забезпечення конфіденційності інформації; дослідження засобів захисту інформації від стороннього втручання, пошкодження чи знищення; виявлення технічних каналів витоку інформації; здобуття практичних навичок із захисту інформаційних і комунікаційних систем.

ОСНОВНІ РЕЗУЛЬТАТИ НАВЧАННЯ ТА КОМПЕТЕНТНОСТІ, ЯКІ ВОНИ ФОРМУЮТЬ

№	Результати навчання	Компетентності
1.	***знати:*** понятійний апарат дисципліни, зокрема «інформаційна безпека», «захист інформації», «цілісність, достовірність, автентичність інформації», «конфіденційність інформації», «несанкціонований доступ», «комп'ютерні віруси», «цифровий підпис» ***вміти:*** здійснювати аналіз та узагальнення інформації, що підлягає захисту; розпізнавати методи несанкціонованого доступу до інформації	Здатність до аналізу та узагальнення інформації щодо захисту від несанкціонованого доступу
2.	***знати:*** основні положення законодавства в галузі захисту інформації; вимоги правових та нормативних актів, що визначають систему захисту інформації в державі ***вміти:*** представляти та подавати інформацію згідно вимог правових та нормативних актів	Вміння організовувати представлення інформації з положень законодавства в галузі захисту інформації
3.	***знати:*** принципи побудови систем захисту інформації ***вміти:*** систематизувати методи захисту даних і комп'ютерних систем	Здатність систематизації методів захисту інформації для підвищення рівня безпеки інформації
4.	***знати:*** сучасні способи боротьби з несанкціонованим доступом, копіюванням, зміною і збором інформації ***вміти:*** практично використовувати технології, методи та засоби захисту інформації з метою уникнення її пошкодження чи знищення	Здатність виконувати адміністрування доступу до комп'ютерних систем з метою призначення невиправданих привілей
5.	***знати:*** основні види вірусів та способи хакерських атак з метою знищення чи пошкодження інформації	Вміння проводити програмний захист комп'ютерних систем від вірусів, хакерських атак,

	вміти: використовувати основні прийоми та програмні засоби захисту від вірусів та комерційного шпигунства для підвищення надійності захисту інформації	комерційного шпигунства
6.	***знати:*** алгоритми шифрування даних і проведення їх порівняльного аналізу при створенні ефективної системи захисту інформації ***вміти:*** створювати ефективну систему захисту інформації	Здатність до виконання моніторінгу з пошуку каналів витоку інформації

Вивчення навчальної дисципліни «Інформаційна безпека та захист інформації» базується на принципах кредитно-модульної системи і передбачає активну роботу студентів на лекціях, практичних заняттях, а також у процесі виконання самостійної роботи.

Самостійна робота студентів є невід'ємною складовою успішного засвоєння навчального матеріалу і передбачає роботу зі спеціальною літературою, стандартами з питань захисту інформації в інформаційних системах і може виконуватись у бібліотеці вищого навчального закладу, навчальних кабінетах, комп'ютерних класах. Самостійна робота студента є основним засобом оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять.

Метою виконання індивідуального завдання є систематизація знань, а також поглиблене вивчення основоположних принципів побудови механізмів захисту інформації, ознайомлення з основними положеннями законодавства в сфері захисту інформації, визначення критеріїв захищеності комп'ютерних систем, закріплення теоретичних знань та практичне застосування знань студента з навчального курсу.

Оцінювання знань студентів по завершенню вивчення дисципліни здійснюється на основі результатів поточного модульного контролю і підсумкового контролю знань.

Поточний модульний контроль знань студентів здійснюється через проведення аудиторних письмових контрольних робіт, комп'ютерного тестування, публічних доповідей, виконання практичних завдань і передбачає поступове накопичення балів.

Підсумковий контроль знань направлений на перевірку знань студентів з дисципліни в цілому і передбачає вміння представляти своє бачення розв'язання проблемних ситуацій.

Форма підсумкового контролю успішності навчання – диференційований залік.

ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ

На вивчення навчальної дисципліни відводиться 3 кредити ECTS, 90 годин.

№ з/п	Назви модулів і тем	Кількість годин *(денна форма навчання)*					Кількість годин *(заочна форма навчання)*				
		Аудиторні	Лекції	Практичні	Лабораторні	СРС	Аудиторні	Лекції	Практичні	Лабораторні	СРС
1	2	3	4	5	6	7	8	9	10	11	12
Змістовий модуль І. *Сутність і поняття інформаційної безпеки*											
1.	Тема 1. Поняття інформаційної безпеки, характеристика її складових	3	1	2		4	1	1			4
2.	Тема 2. Місце інформаційної безпеки в системі національної безпеки	1	1			4	1		1		4
3.	Тема 3. Загрози інформаційній безпеці	3	1	2		4	1	1			4
4.	Тема 4. Політика інформаційної безпеки	3	1	2		4	1		1		4
5.	Модульний контроль					2					
6.	**Разом за змістовим модулем І**	**10**	**4**	**6**		**18**	**4**	**2**	**2**		**16**
Змістовий модуль ІІ. *Поняття і сутність захисту інформації та її місце в системі інформаційної безпеки*											
7.	Тема 5. Поняття, сутність, цілі і принципи захисту інформації	2	2			4					4
8.	Тема 6. Критерії, умови та принципи віднесення інформації до такої, що потребує захисту	4	2	2		4	1	1			3
9.	Тема 7. Правовий захист інформації	3	1	2		4	1		1		3

1	2	3	4	5	6	7	8	9	10	11	12
10.	Тема 8. Методологічні підходи до захисту інформації та принципи її організації	3	1	2		4	1	1			3
11.	Тема 9. Реалізація системи захисту інформації в комп'ютерних системах і мережах	4	2	2		4	1		1		3
12.	Модульний контроль					2					
13.	**Разом за змістовим модулем II**	**16**	**8**	**8**		**22**	**4**	**2**	**2**		**16**
Змістовий модуль III. *Забезпечення інформаційної безпеки підприємства*											
14.	Тема 10. Проблеми захисту інформації на підприємстві	4	1	2		4	1		1		6
15.	Тема 11. Характеристика каналів витоку інформації на підприємстві	2	1	2		4	1		1		5
16.	Тема 12. Основні напрями забезпечення інформаційної безпеки підприємства	4	2	2		4	2		2		5
17.	Модульний контроль					2					
18.	**Разом за змістовим модулем III**	**10**	**4**	**6**		**14**	**4**		**4**		**16**
Разом		**36**	**16**	**20**		**54**	**12**	**4**	**8**		**48**

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

На вивчення навчальної дисципліни «Інформаційна безпека та захист інформації» відводиться 3 кредити ECTS, 90 годин.

ЗМІСТОВИЙ МОДУЛЬ 1. СУТНІСТЬ І ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 1. Поняття інформаційної безпеки, характеристика її складових

1.1. Дати визначення інформаційної безпеки для суб'єктів інформаційних відносин.

1.2. Класифікувати і таблично представити властивості та основні види інформації.

1.3. Охарактеризувати об'єкти та суб'єкти інформаційної безпеки.

1.4. Аргументувати сутність інформаційної безпеки, виразити основні властивості інформаційної безпеки.

1.5. Пояснити концептуальну модель інформаційної безпеки.

Завдання для самостійної роботи:

- опрацювати основні терміни та визначення теми лекції;
- аргументувати роль інформації в сучасному інформаційному суспільстві та значення інформаційної безпеки;
- виділити основні принципи побудови профілю захисту інформації.

Рекомендована література: [12, 15, 19, 25, 26]

ТЕМА 2. Місце інформаційної безпеки в системі національної безпеки

2.1. Охарактеризувати сутність інформаційної інфраструктури держави.

2.2. Ідентифікувати державні органи, що забезпечують інформаційну безпеку. Пояснити сутність національної системи конфіденційного зв'язку.

2.3. Класифікувати відділи спецслужб держави. Доповісти про роль та функції державної служби спеціального зв'язку та захисту інформації.

2.4. Обґрунтувати роль та функції департаменту стратегії розвитку спеціальних інформаційно-телекомунікаційних систем.

2.5. Упорядкувати у вигляді таблиці законодавчі вимоги з урегулювання інформаційної безпеки.

2.6. Порівняти та зіставити сучасну та попередню концепції інформаційної безпеки держави.

Завдання для самостійної роботи:

- дослідити основні міжнародні та національні стандарти із захисту інформації;
- проаналізувати основні положення законодавства в галузі захисту інформації;
- оцінити державні стандарти України стосовно засад безпеки інформації.

Рекомендована література: [7, 13, 15, 19, 24]

ТЕМА 3. Загрози інформаційній безпеці

3.1. Упорядкувати дестабілізуючі фактори інформаційної безпеки.

3.2. Класифікувати у вигляді таблиці загрози інформаційній безпеці.

3.3. Ілюструвати джерела загроз інформаційній безпеці.

3.4. Сформулювати загрози комерційного шпигунства.

Завдання для самостійної роботи:

- класифікувати основні вразливі елементи інформаційних систем;
- розкрити методи проникнення до інформації (хакінг, кракінг, піратство, фішинг) в комп'ютерних системах;
- сформулювати ризики безпеки інформації.

Рекомендована література: [15, 20, 22, 25, 28, 31]

ТЕМА 4. Політика інформаційної безпеки

4.1. Визначити основні поняття політики безпеки.

4.2. Узагальнити види моделей політики інформаційної безпеки.

4.3. Оцінити та порівняти дискреційну політику безпеки, мандатну політик, рольову політику безпеки.

4.4. Ілюструвати життєвий цикл розробки системи безпеки.

4.5. Аргументувати значення політики безпеки інформації.

Завдання для самостійної роботи:

- провести аналіз архітектури системи захисту інформації;
- обґрунтувати сутність інформації як матеріальної цінності;
- пояснити суть трьохрівневої політики інформаційної безпеки.

Рекомендована література: основна [14, 15, 24, 25, 28]

додаткова [2, 12]

ЗМІСТОВИЙ МОДУЛЬ 2.
ПОНЯТТЯ І СУТНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЇЇ МІСЦЕ В СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ТЕМА 5. Поняття, сутність, цілі і принципи захисту інформації

5.1. Обґрунтувати концептуальні основи захисту інформації.

5.2. Розробити та представити програму та план захисту інформації в організації.

5.3. Сформулювати правила роботи та допуску до відомостей, що становлять державну таємницю.

5.4. Визначити принципи і правила розмежування доступу до комерційних секретів.

5.5. Оцінити методи забезпечення захисту та збереження документів, справ і виробів на підприємстві.

5.6. Сформулювати методи контролю при роботі з відомостями, що містять комерційну таємницю.

Завдання для самостійної роботи:

- розкрити основні принципи організації захисту інформації в інформаційних системах;
- оцінити, як здійснюється контроль цілісності даних в інформаційних системах;
- охарактеризувати правовий статус електронного документу.

Рекомендована література: основна [6, 7, 11, 13, 16, 19]

додаткова [1, 4, 5, 7, 11]

ТЕМА 6. Критерії, умови та принципи віднесення інформації до такої, що потребує захисту

6.1. Класифікувати види інформації за ступенями доступу.

6.2. Таблично узагальнити види носіїв інформації, що підлягають захисту.

6.3. Пояснити правила засекречування та розсекречування відомостей і їх носіїв.

6.4. Узагальнити правила встановлення і зняття грифу «Комерційна таємниця» з документів і виробів.

6.5. Розкрити сутність понять «Інтелектуальна власність», «Авторське право», навести конкретні приклади.

Завдання для самостійної роботи:

- охарактеризувати механізми й протоколи забезпечення аутентичності інформації в інформаційних системах;
- пояснити сутність основних сервісів безпеки та механізмів безпеки;
- оцінити інформацію як об’єкт інтелектуальної власності.

Рекомендована література: основна [11, 12, 18, 19, 23]

додаткова [7, 16]

ТЕМА 7. Правовий захист інформації

7.1. Узагальнити у вигляді таблиці інформацію, доступ до якої обмежений відповідно діючого законодавства.

7.2. Сформулювати правила роботи з інформацією, що містить державну таємницю.

7.3. Пояснити правила доступу до інформації з обмеженим доступом.

7.4. Дати визначення поняття «державна таємниця», сформулювати проблеми захисту державної таємниці.

7.5. Аргументувати основні види порушень законодавства в сфері інформації.

7.6. Порівняти і зіставити дисциплінарну, адміністративну, цивільно-правову та кримінальну відповідальність за порушення правового захисту інформації.

Завдання для самостійної роботи:

- узагальнити основні канали витоку інформації;
- обґрунтувати, як здійснюється контроль за інформацією, що обробляється засобами комп'ютерної техніки;
- охарактеризувати значення правового захисту конфіденційної інформації.

Рекомендована література: основна [12, 13, 19, 23, 25, 28]

додаткова [6, 7]

ТЕМА 8. Методологічні підходи до захисту інформації та принципи її організації

8.1. Дослідити методологічні підходи до захисту інформації та принципи її організації.

8.2. Охарактеризувати об'єкти і суб'єкти інформаційного захисту.

8.3. Класифікувати методи і засоби захисту інформації.

8.4. Узагальнити заходи щодо забезпечення захисту конфіденційної інформації.

8.5. Встановити організаційно-правові методи захисту персональних даних.

8.6. Зробити висновки щодо інформаційного та правового захисту електронних видань і цифрової передачі даних в Україні.

Завдання для самостійної роботи:

- зіставити механізми та протоколи забезпечення конфіденційності інформації;
- охарактеризувати поняття стеганографія та сфери його використання;
- обґрунтувати необхідність використання технологічної та інформаційної стеганографії при роботі з носіями інформації;
- проаналізувати персональні дані як об'єкт захисту.

Рекомендована література: основна [3, 11, 19, 21, 23, 27, 29, 30]

додаткова [8, 9, 16]

ТЕМА 9. Реалізація системи захисту інформації в комп'ютерних системах і мережах

9.1. Оцінити технологію реалізації атак на комп'ютерну систему та мережу.

9.2. Класифікувати види атак на комп'ютерну мережу. Привести загальну методику та поширені засоби реалізації атак.

9.3. Охарактеризувати класичну модель симетричної системи секретного зв'язку за К. Шенноном: основні типи шифрів, загальні алгоритмічні проблеми, пов'язані зі стійкістю сучасних криптоалгоритмів.

9.4. Розкрити сутність ідеї односторонньої функції з лазівкою. Провести порівняльну характеристику асиметричних криптосистем, встановити її переваги та недоліки.

9.5. Встановити правила використання цифрового підпису. Розкрити сутність поняття «криптографічні протоколи».

Завдання для самостійної роботи:

- охарактеризувати недоліки симетричних систем секретного зв'язку;
- аргументувати використання криптографії та криптоаналізу в системах захисту інформації;
- узагальнити основні вили атак на комп'ютерну систему «зсередини»;
- розкрити зміст вірусних атак типу «троянський кінь», фальшиві програми реєстрації, використання «логічних бомб», «таємних дверей» і помилок у програмному забезпеченні. Зовнішні атаки на комп'ютерну систему.

Рекомендована література: [2, 3, 4, 9, 10, 11, 21, 25, 27]

ЗМІСТОВИЙ МОДУЛЬ 3.
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ТЕМА 10. Проблема захисту інформації на підприємстві

10.1. Сформулювати проблематику збереження конфіденційності документованої інформації відповідно до законодавства.

10.2. Класифікувати методи запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації.

10.3. Запропонувати способи запобігання несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації.

10.4. Обґрунтувати захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в інформаційних системах.

10.5. Підсумувати концептуальні причини втрати і пошкодження інформації.

Завдання для самостійної роботи:

- охарактеризувати механізми та протоколи забезпечення цілісності даних при їх передачі на відстань;
- спроектувати модель управління доступом в інформаційних системах;
- оцінити критерії захищеності інформації в інформаційних системах.

Рекомендована література: [1, 5, 15, 19, 23, 29, 30]

ТЕМА 11. Характеристика каналів витоку інформації на підприємстві

11.1. Проаналізувати відкриті загальні й спеціальні публікації й бази даних.

11.2. Передбачити вплив клієнтів, постачальників, інвесторів, кредитних організацій, посередників та агентів на можливий витік інформації з підприємства.

11.3. Охарактеризувати роль та функції адвокатських контор, аудиторських фірм, страхових компаній, консультантів, податкових інспекцій, санітарних та пожежних служб, органів статистики, правоохоронних органів.

11.4. Розкрити сутність представництв фірми на ярмарках, салонах, конференціях.

Завдання для самостійної роботи:

- пояснити основні загрози під час проведення нарад та конференцій;
- обґрунтувати причини витоку мовної інформації;

– узагальнити, як відбувається захист інформації в мережі Інтернет та соціальних мережах.

Рекомендована література: [1, 2, 6, 11, 18, 23, 25, 28, 31]

ТЕМА 12. Основні напрями забезпечення інформаційної безпеки підприємства

12.1. Охарактеризувати систему правового захисту комерційної таємниці підприємства, визначити її елементи та складові.

12.2. Сформулювати правила організації допуску та доступу до комерційної інформації на підприємстві.

12.3. Встановити основні цілі системи захисту інформації на підприємстві.

12.4. Класифікувати складові безпеки за типами загроз: захист від злочинного світу; захист від недобросовісної конкуренції; захист від протиправних дій власних співробітників.

12.5. Роз'яснити принцип технології аналізу захищеності, технології виявлення порушника, технології захисту від НСД, технології антивірусного захисту.

Завдання для самостійної роботи:

– проаналізувати механізми та протоколи захисту електронної пошти, що використовується на підприємстві;

– опрацювати склад та призначення основних підсистем захисту інформації на підприємстві.

Рекомендована література: [1, 15, 23, 25, 28, 31]

ІНДИВІДУАЛЬНА РОБОТА

Індивідуальна робота виконується студентом самостійно і здається викладачу для перевірки наприкінці семестру. Індивідуальна робота студентів передбачає виконання наступних завдань:

1. Скласти термінологічний словник з теми «Поняття інформаційної безпеки».
2. Скласти тези до доповіді «Історія становлення інформаційної безпеки».
3. Скласти схему «Концептуальна модель інформаційної безпеки» з наступними блоками: загрози, цілі загрози, джерела загрози, джерела інформації, напрямки захисту, об’єкти загрози, методи захисту, способи захисту, засоби захисту.
4. Підготувати опорний конспект з теми «Політика інформаційної безпеки».
5. Охарактеризувати сутність поняття «Комп’ютерна злочинність» та її основні риси.
6. Опрацювати законодавство та нормативно-правову базу у сфері захисту інформації.
7. Скласти опорний конспект з теми «Характеристика каналів витоку інформації на підприємстві».
8. Охарактеризувати поняття «Оранжева книга» - перший стандарт у галузі оцінки захищеності комп’ютерних систем.
9. Обґрунтувати основні напрями забезпечення інформаційної безпеки підприємства.
10. Визначити проблемні питання, пов’язані з використанням різних видів інформації в діяльності людини, суспільства і держави; викласти свою точку зору щодо вдосконалення використання інформаційних ресурсів, підготовки інформаційних продуктів та надання інформаційних послуг в сучасних умовах.
11. Проаналізувати основні нормативно-правові акти, пов’язані зі сферою захисту різних видів інформації.

12. Визначити проблемні питання у сфері формування інформаційних ресурсів, у підготовці інформаційних продуктів і надання інформаційних послуг і викласти свою позицію щодо вдосконалення використання різних видів інформації у підприємницькій діяльності.
13. Скласти схему **можливих** каналів витоку і несанкціонованого доступу до інформації в комерційній організації і дати їм коротке пояснення.

Завдання, обов'язкове для виконання усіма студентами (оцінюється 10 балів):

– обрати один із об'єктів захисту (будівля інформаційно-обчислювального центру комерційної організації, територія виробничої зони фірми, великий торгово-промисловий комплекс, виставковий салон з новими технологіями в галузі автомобільного виробництва):

– оцінити загрози інформаційних ресурсів вибраного об'єкту, можливі канали витоку і несанкціонованого доступу до конфіденційної інформації;

– визначити способи зняття інформації з технічних каналів витоку інформації;

– виявити можливі способи перехоплення мовної інформації зловмисниками при її передачі технічними каналами.

ПИТАННЯ ДЛЯ ПІДГОТОВКИ ДО ЗАЛІКУ

1. Значення інформаційної безпеки для суб'єктів інформаційних відносин.
2. Реалізація систем захисту інформації в комп'ютерних системах.
3. Властивості та основні види інформаційних продуктів.
4. Загрози інформаційної безпеки в Україні.
5. Українське законодавство про захист персональних даних.
6. Об'єкти та суб'єкти інформаційної безпеки.
7. Основні принципи захисту інформації.
8. Класифікація джерел та загроз інформаційній безпеці.
9. Конфіденційність інформації в мережі Інтернет.
10. Проблеми захисту інформації на підприємстві.

11. Загрози комерційного шпигунства.
12. Технічні канали витоку інформації.
13. Державна служба спеціального зв’язку та захисту інформації.
14. Загрози мовного перехоплення інформації зловмисниками
15. Види моделей політики інформаційної безпеки.
16. Встановлення і зняття грифу «Комерційна таємниця».
17. Значення політики захисту безпеки інформації.
18. «Вірусні атаки» на комп’ютерну систему.
19. Допуск до відомостей, що становлять державну таємницю.
20. Запобігання витоку, розкраданню, втраті, підробці інформації.
21. Допуск до відомостей, що становлять комерційну таємницю.
22. Причини втрати і пошкодження інформації.
23. Види інформації за ступенем доступу.
24. Технології антивірусного захисту інформації.
25. Засекречування та розсекречування відомостей та їх носіїв.
26. Захист від недобросовісної конкуренції.
27. Електронний цифровий підпис як програмно-технічний та правовий засіб захисту інформації.
28. Конфіденційна інформація та державна таємниця.
29. Найбільш розповсюджені загрози безпеці інформації в Україні.
30. Правовий інститут державної таємниці, його складові.
31. Захист персональних даних.
32. Параметри приватності та умови безпечного користування інформаційними ресурсами мережі Інтернет.
33. Типи комп’ютерних вірусів та їх шкода безпеці інформації.
34. Адміністративна, дисциплінарна, кримінальна відповідальності за порушення інформаційної безпеки.
35. Найбільш популярні джерела зараження комп’ютера вірусами.
36. Заходи щодо забезпечення захисту конфіденційної інформації.
37. Охорона комерційних таємниць підприємства.

38. Об’єкти і суб’єкти інформаційного захисту.
39. Промислове шпигунство як загроза комерційній таємниці.
40. Соціально-психологічні заходи захисту інформації на підприємстві.
41. Класифікація методів і засобів захисту інформації.
42. Канали витоку інформації на думку зарубіжних фахівців.
43. Правовий захист інформації та його основні завдання.
44. Технічні канали витоку інформації.
45. Інформації та її види за ступенем доступу.
46. Загрози безпеці інформації від підключення реєструючої апаратури.
47. Сучасна концепція інформаційної безпеки.
48. Основні види загроз безпеці інформації.
49. Структура політики безпеки та її основні складові.
50. Поняття шифрування даних, сучасні криптосистеми та основні вимоги.

КОНТРОЛЬ ЯКОСТІ ЗНАНЬ СТУДЕНТІВ

Форми і методи поточного контролю

Контроль успішності студентів з врахуванням поточного і підсумкового оцінювання проводиться відповідно до визначених видів робіт, а також у чітко визначений термін.

Поточному оцінюванню підлягають наступні види робіт: конспект студента, робота на семінарських заняттях, співбесіди з нормативної бази дисципліни, участь у дискусіях, що визначені тематикою курсу та виконання індивідуальних завдань.

Після завершення вивчення навчального матеріалу кожного модуля проводяться заходи модульного контролю. Перевірка знань студента здійснюється за допомогою співбесіди, тестування та контрольної роботи. Оцінювання тестів проводиться за власною методикою з приведенням підсумку до встановленої в рейтинговій шкалі балів.

У разі не підготовки до семінарського заняття або іншого виду робіт за викладачем залишається право нарахувати штрафні бали, які відпрацьовуються в індивідуальному порядку.

Система рейтингових балів для різних видів контролю та порядок їх переводу до національної (4-х бальної) та європейської (ECTS) шкали представлені в таблиці наприкінці цього пункту.

Модульний контроль – оцінка фіксується не пізніше ніж 3 дні після проведення. В разі незадовільної оцінки – студент має обов’язково перескласти.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

Поточне тестування та самостійна робота														Підсумковий контроль	Сума
Змістовий модуль 1				**Змістовий модуль 2**					**Змістовий модуль 3**				**ІНДЗ**	**0-100**	**Поточна оцінка + підсумкова/ 2=0-100**
1	**2**	**3**	**М**	**4**	**5**	**6**	**7**	**М**	**8**	**9**	**10**	**М**			max100
*	*	*	**10**	*	*	*	*	**10**	*	*	*	**10**			
			25					**30**				**25**	**20**	**100**	**100**

Примітка.

0-10 балами пропонується оцінити виконання модульних завдань.

0-5 балів (в таблиці *) – решту завдань, наприклад, виконання практичної та самостійної роботи студентами.

Додатковим стовпчиком (цифри жирним) визначено мах суму балів за модуль.

ПОТОЧНИЙ МОДУЛЬНИЙ КОНТРОЛЬ ЗНАНЬ СТУДЕНТІВ

Модульний контроль знань студентів здійснюється через проведення аудиторних письмових контрольних робіт або комп’ютерного тестування.

Критерії оцінювання модульного контролю знань студентів

Письмова контрольна робота	**Критерії оцінювання**
13-15	У повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу.
10-12	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних

	завдань використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини га аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки.
7-9	У цілому володіє навчальним матеріалом, викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури: допускаючи при цьому окремі істотні неточності та помилки.
4-6	Не в повному обсязі володіє навчальним матеріалом, фрагментарно, поверхово (без аргументації та обґрунтування) і викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому істотні неточності.
1-5	Частково володіє навчальним матеріалом, але не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому істотні помилки.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань.

Студент, який з різних обставин не отримав необхідної кількості балів з будь-якої теми, має можливість самостійно її підготувати і пройти індивідуальний поточний контроль знань з цієї теми способом комп'ютерної діагностики або виконати завдання до самостійної робо ти. що пропонуються в робочій програмі до теми.

ПІДСУМКОВЕ КОНТРОЛЬНЕ ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ

Підсумкове модульне оцінювання знань студентів означає поступове накопичення балів від одного поточного модульного контролю до іншого в кінцевому рахунку отримання середнього підсумкового балу.

За системою НПУ імені М.П. Драгоманова	**За шкалою ECTS**	**За національною системою**	**Визначення**
90-100	A	5 (відмінно)	Повно та ґрунтовно засвоїв всі теми навчальної програми вміє вільно та самостійно викласти зміст всіх питань програми навчальної дисципліни, розуміє її значення для своєї професійної підготовки, повністю виконав усі завдання кожної теми та поточного модульного контролю в цілому. Брав участь в олімпіадах, конкурсах, конференціях.
80-89	B	4 (дуже добре)	Достатньо повно та ґрунтовно засвоїв основні питання робочої програми. Вміє самостійно викласти зміст. Виконав завдання кожної теми та модульного поточного контролю в цілому.
70-79	C	4 (добре)	Недостатньо повно та ґрунтовно засвоїв деякі теми робочої програми, не вміє самостійно викласти зміст деяких запитань програми навчальної дисципліни. Окремі

			завдання кожної теми та модульного поточного контролю в цілому виконав не повністю.
65-69	D	3 (задовільно)	Засвоїв лише окремі теми робочої програми. Не вміє вільно самостійно викласти зміст основних питань навчальної дисципліни, окремі завдання кожної теми модульного контролю не виконав.
60-64	E	3 (достатньо)	Засвоїв лише окремі питання навчальної програми. Не вміє достатньо самостійно викласти зміст більшості питань програми навчальної дисципліни. Виконав лише окремі завдання кожної теми та модульного контролю в цілому.
35-59	F	2 (незадовільно)	Не засвоїв більшості тем навчальної програми не вміє викласти зміст більшості основних питань навчальної дисципліни. Не виконав більшості завдань кожної теми та модульного контролю в цілому.
1 -34	FX	2 (незадовільно)	Не засвоїв навчальної програми, не вміє викласти зміст кожної теми навчальної дисципліни не виконав модульного контролю.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна

1. Алексеенко В.Н. Система защиты коммерческих объектов. Технические средства защиты. Практическое пособие для предпринимателей и руководителей служб безопасности / В.Н. Алексеенко, Б.В. Сокольский. – М., 1992. – 94 с.
2. Бабак В.П. Інформаційна безпека та сучасні мережеві технології. Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 668 с.
3. Баричев С.Г. Основы современной криптографии: навчальний посібник. [Електронний ресурс]. URL: http://www.ict.edu.ru/ft/002447/crypto1-3.pdf
4. Вакалюк Т.А. Захист інформації в комп'ютерних системах: навчально-методичний посібник. – Житомир: Вид-во ЖДУ, 2013. – 136 с. [Електронний ресурс]. URL: http://eprints.zu.edu.ua/9650/1/1.pdf
5. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.
6. Грицяк Н.В. Електронний документообіг та захист інформації: навчальний посібник / Н.В. Грицяк. – К.: НАДУ, 2015. – 84 с.
7. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15 грудня 1997 року. [Електронний ресурс]. URL: www.iu.org.ua
8. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
9. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К. : Держстандарт України, 1997. – 11 с.

10. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.
11. Єсін В.І. Безпека інформаційних систем і технологій: навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»] / В.І. Єсін, О.О. Кузнецов, Л.С. Сорока. – Х.: ХНУ імені В.Н. Каразіна, 2013. – 632 с [Електронний ресурс]. URL: http://www.univer.kharkov.ua/images/ redactor/news/2013-03-01/Esin.pdf
12. Закон України «Про інформацію» від 02 жовтня 1992 р. № 2657-XII // Відомості Верховної Ради України, 1992. № 48. С. 650.
13. Закон України «Про державну таємницю» // Відомості Верховної Ради України, 1999. № 49. С. 428.
14. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
15. Інформаційна безпека України: Зб. наук. доп. та тез науково-технічної конференції; м. Київ, 12-13 березня 2015 р., Київський національний університет імені Тараса Шевченка / Редкол.: І.О. Анісімов (голова) та ін. – К.: Київський національний університет імені Тараса Шевченка, 2015. 156 с.
16. Концепція технічного захисту інформації в Україні. [Електронний ресурс]. URL: http://zakon1.rada.gov.ua/cgibin/laws/main.cgi?nreg=1126-97-%EF
17. Корченко О.Г. Захист та зламування програм. Навчальний посібник / О.Г. Корченко, А.С. Морозов. – К.: НАУ, 2001. – 84 с.
18. Кузнецов О.О. Захист інформації в інформаційних системах / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2011. – 512 с.
19. Логінова Н.І. Правовий захист інформації: навчальний посібник / Н.І. Логінова. – Одема: Фенікс, 2015. – 264 с.
20. Макнамара, Дж. Секреты компьютерного шпионажа, тактика и контрмеры / Дж. Макнамара – М.: Бином, 2006. – 255 с.

21. Мінгальова Ю. Новітні криптографічні методи захисту інформації. [Електронний ресурс]. URL: http://eprints.zu.edu.ua/13902/1/Mingaleva3.pdf
22. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ.– К., 1999. – 34 с.
23. Організаційно-правові основи захисту інформації з обмеженим доступом. Навчальний посібник. / За ред. В. С. Сідака. − К., 2006.
24. Основи інформаційної безпеки / С.В. Кавун, О.А. Смірнов, В.Ф. Столбов. – Кіровоград: Вид. КНТУ, 2012. – 414 с.
25. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов. – Х.: Вид. ХНЕУ, 2013. – 476 с.
26. Понарина Н.Н. Глобализация и информационное общество // Общество: политика, экономика, право. – 2012. – №1. – С.19–24
27. Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ... 22.05.98 р. № 505/98 // Уряд. кур'єр, 1998. – 9 липня. − С. 2.
28. Про затвердження Концепції технічного захисту інформації в Україні: Постанова... 8 жовтня 1997 р. № 1126 // ДВУ, 1997. – № 12. – С. 1714.
29. Проект Закону України «Про інформацію персонального характеру». [Електронний ресурс]. URL: www.khpg.org.ua
30. Тополевський Р. Зауваження та пропозиції до проекту Закону України № 2618 від 01.10.2003 р. «Про захист персональних даних». [Електронний ресурс]. URL: www.khpg.org.ua
31. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – НиТ:Санкт-Петербург, 2004. – 348 с.

Додаткова

1. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.

2. Домарев В.В. Безопасность информационных технологий. Методы создания систем защиты / В.В. Домарев. – К.: ООО ТИД ДС, 2001. – 688 с.
3. ДСТУ 3396.1-96 Захист інформації. ТЗІ. Порядок проведення робіт.
4. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV. URL: https://zakon5.rada.gov.ua/laws/main/851-15
5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852IX
6. Захаров Є. Свобода доступу до урядової інформації. [Електронний ресурс]. – URL: www.khpg.org.ua
7. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Затверджена постановою Кабінету Міністрів України від 27.11.98. № 1893 // Офіційний вісник України, 1998. - № 48. – С. 1764
8. Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру. Страсбург, 28 січня 1981 року. [Електронний ресурс]. URL: www.iu.org.ua
9. Конвенція про захист прав людини і основоположних свобод (Рим, 4.XI.1950). [Електронний ресурс]. – Режим доступу до ресурсу: www.iu.org.ua
10. Нестеренко О. Чи зможе прийняття Законопроекту «Про інформаційну відкритість органів державної влади та вищих посадових осіб України» забезпечити інформаційну відкритість влади? [Електронний ресурс]. URL: www.khpg.org.ua
11. Постанова Кабінету Міністрів України від 28.10.04 р. №1453 «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади».
12. Правила посиленої сертифікації, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3, зареєстровані в Міністерстві юстиції України 27.01.2005 за № 104/10384 (у редакції наказу Департаменту)

13. Проект Закону України «Про інформаційну відкритість органів державної влади та вищих посадових осіб України». [Електронний ресурс]. URL: www.iu.org.ua
14. Речицький В. Юридичний коментар Харківської правозахисної групи до проекту Закону України Про інформаційну відкритість органів державної влади та вищих посадових осіб України. [Електронний ресурс]. URL: www.khpg.org.ua
15. Тополевський Р. Зауваження та коментарі до проекту Закону України «Про реєстрацію фізичних осіб в Україні» від 12.11.2003. [Електронний ресурс]. URL: www.khpg.org.ua
16. Ященко В.В. Введение в криптографию: навчальний посібник / В.В. Ященко. – 4-е изд., доп. М.: МЦНМО, 2012. – 348 с. [Електронний ресурс]. URL: http://cryptography.ru/wp-content/uploads/2013/09/intro_to_crypto.pdf

Навчально-методичне видання

Інформаційна безпека та захист інформації

Методичні рекомендації до підготовки та проведення практичних занять

О. М. Фендьо, О. І. Охмуш-Ковалевська, О. В. Галицький

Пробне видання