ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 17 «ОСНОВИ КІБЕРБЕЗПЕКИ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека та захист інформаційя»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
Андрій ЄФІМЕНКО
Гарант освітньо-професійної програми
Андрій ЄФІМЕНКО

Розробник: кандидат технічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки Лобанчикова Надія Миколаївна

Житомир
2024-2025 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів 3	Галузь знань 12 «Інформаційні технології»	нормативна
Модулів – 3	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки:
Змістових модулів – 3		2
		Семестр
Загальна кількість годин – 90		3
Тижневих годин для денної форми навчання: Аудиторних – 3 самостійної роботи – 2,6	Освітній ступінь «бакалавр»	Лекції
		32 год.
		Практичні
		0 год.
		Лабораторні
		16 год.
		Самостійна робота
		42 год.
		Вид контролю: екзамен

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями кібербезпеки та захисту інформації в інформаційно-телекомунікаційних системах, методологічними та законодавчими основами організації, планування та впровадження систем кібербезпеки та захисту інформації в інформаційних системах управління на підприємствах, а також основним аспектам практичної діяльності по їх створенню, забезпеченню функціонування та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завданнями вивчення навчальної дисципліни є:

– оволодіння принципами побудови систем кіберзахисту;

– розуміння головних задач та сервісів кібербезпеки;

– оволодіння загальними теоретичними поняттями та основними нормативно-правовими документами у сфері кібербезпеки;

– отримання знань щодо основних складових інформаційної безпеки;

– отримання знань щодо існуючих моделей загроз та порушника, основних причин порушення безпеки;

– отримання знань щодо класифікації засобів кібербезпеки, організаційних та технічних заходів забезпечення кіберзахисту;

– оволодіння принципами захисту інформації від несанкціонованого доступу, методами аутентифікації та ідентифікації користувачів інформаційно-телекомунікаційних систем, методами контролю доступу;

– оволодіння теоретичними основами криптографічних та стеганографічних методів захисту інформації;

– оволодіння методами та засобами здійснення процедури оцінки ефективності систем кіберзахисту;

– оволодіння технологіями реалізації криптографічних алгоритмів захисту інформації;

– оволодіння методами розробки моделі загроз та моделі порушників інформаційної безпеки

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності код 125 «Кібербезпека»:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека»:

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

РН 12. Розробляти моделі загроз та порушника;

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

РН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

3. Програма навчальної дисципліни

Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі.

Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.

Дефініція основних понять і визначень у сфері кібербезпеки. Основні нормативно-правові документи із захисту інформації.

Тема 2. Загрози безпеці інформаційних систем

Джерела загроз інформаційній безпеці. Системна класифікація і загальний аналіз загроз безпеці інформації. Модель загроз та порушника і кіберпросторі.

Тема 3. Інциденти у сфері високих технологій

Основні поняття та визначення. Класифікація кібернетичних втручань і загроз. Особливості найпоширеніших кібератак

Змістовий модуль 2. НСД та криптографічні методи захисту інформації

Тема 4. Методи та засоби захисту інформації від НСД

Способи та методи НСД в сучасних ІТС. Основні принципи захисту інформації від НСД. Рівні інформаційно-комунікаційної системи. Несанкціонований доступ на різних рівнях інформаційно-комунікаційної системи. Класичні моделі розмежування доступу. Ідентифікація і аутентифікація користувачів.

Тема 5. Криптографічні методи захисту інформації

Історична довідка. Основні поняття криптографії. Загальна класифікація алгоритмів шифрування. Кваліфікований електронний підпис. Реалізація алгоритмів шифрування. Стеганографія.

Змістовий модуль 3. Захист інформації в розподілених інформаційних системах та організація кібербезпеки

Тема 6. Технології віртуалізації

Ключові терміни. Переваги та недоліки. Типи віртуалізації. Платформи віртуалізації.

Тема 7. Шкідливе програмне забезпечення та захист від нього

Шкідливе програмне забезпечення та захист від нього. Організаційно-технічні заходи забезпечення захисту інформації.

Тема 8. Політика безпеки. Оцінка ефективності систем захисту інформації.

Поняття політики безпеки. Види політик безпеки. Організація секретного діловодства. Підходи до оцінки ефективності систем захисту інформації.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	практичні	Самостійна робота	усього	лекції	практичні	Самостійна робота
Модуль 1								
Змістовий модуль 1. Принципи організації захисту інформації в кіберпросторі								
Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.	8	4		4				
Тема 2. Загрози безпеці інформаційних систем	10	4	2	4				
Тема 3. Інциденти у сфері високих технологій	8	4		4				
Разом за змістовий модуль 1	26	12	2	12				
Змістовий модуль 2. Основи криптографічних методів кіберзахисту								
Тема 4. Методи та засоби захисту інформації від НСД	10	4	2	4				
Тема 5. Криптографічні методи захисту інформації	16	4	4	8				
Разом за змістовий модуль 2	26	8	6	12				
Змістовий модуль 3. Організація захисту інформації								
Тема 6. Технології віртуалізації	10	4	2	4				
Тема 7. Шкідливе програмне забезпечення та захист від нього	16	4	4	8				
Тема 8. Політика безпеки. Оцінка ефективності систем захисту інформації	12	4	2	6				
Разом за змістовий модуль 3	38	12	8	18				
ВСЬОГО	90	32	16	42				

5. Теми лабораторних робіт

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Дослідження процесів складання імовірнісного прогнозу та моделі порушника	2	-
2	Дослідження процесів кіберзахисту інформації від несанкціонованого доступу	2	-
3	Дослідження процесів захисту інформації за допомогою криптографічних алгоритмів	2	-
4	Дослідження процесів нанесення цифрових водяних знаків у зображення	2	-

5	Дослідження процесів налаштування параметрів безпеки операційної системи Windows 10 із застосуванням програми VirtualBox	2	-
6	Дослідження процесу розробки політики безпеки та програмної реалізації дискреційної політики безпеки організації	2	-
7	Дослідження методів, засобів та технологій технічного захисту інформації	2	-
8	Дослідження процесів визначення міцності захисту інформації	2	-
РАЗОМ		16	-

6. Завдання для самостійної роботи

Тема 1. Теоретичні основи та нормативно-правове забезпечення кіберзахисту.

1. Самостійна робота за темою:
   – ознайомитися з основними поняттями електронного документообігу;
   – ознайомитись із класифікацією документів, що використовується у сучасному діловодстві;
   – проаналізувати основні атрибути документів;
   – ознайомитися з основними документами в сфері захисту інформації та кібербезпеки.

Рекомендована література 1-26, 50-53.

Тема 2. Загрози безпеці інформаційних систем.

1. Самостійна робота за темою:

– проаналізувати основні складові системи захисту інформації.

– проаналізувати поняття «система», «системний аналіз», «системний підхід» та «методи дослідження»;

–визначити джерела небезпеки комп'ютерного класу навчального корпусу, де проходять заняття;

–розробити концепцію безпеки комп'ютерного класу навчального корпусу;

–провести аналіз існуючих системи захисту інформації.

Рекомендована література 2-5, 12, 14-16, 19, 23, 26-35, 51-54

Тема 3. Інциденти у сфері високих технологій а

1. Самостійна робота за темою:

- дослідити приклади кіберінцидентів;
- вивчити карти кіберзагроз

Рекомендована література: 2-5, 12, 14-16.

Тема 4. Методи та засоби захисту інформації від НСД

1. Самостійна робота за темою:

- захист інформації від несанкціонованого доступу програмними методами;
- методи та засоби захисту інформації в телекомунікаційних системах;
- основні шляхи несанкціонованого доступу (НСД) до інформації та їх практична реалізація стосовно комп'ютерної інформації;
- існуюча статистика вірусної активності в поточному році;
- принципи здійснення віддалених (зовнішніх) атак на комп'ютерні мережі та інформаційні системи.

Рекомендована література 2, 3, 4, 6-7,10-13, 24, 27, 31- 39, 41-43.

Тема 5. Криптографічні методи захисту інформації

1. . Самостійна робота за темою:

-опрацювання термінології сучасної криптографії та алгоритмів шифрування;

- принципи побудови сучасних підсистем криптографічного захисту;
- алгоритм PGP;
- комп'ютерна стеганографія.

Рекомендована література 15,16,24, 28, 33-35, 43, 49,56,58

Тема 6. Технології віртуалізації

1. Самостійна робота за темою:
   - аналіз платформ віртуалізації;
   - аналіз кіберзагроз при використанні систем віртуалізації;
   - особливості використання платформ віртуалізації.

Рекомендована література 2, 3, 4, 6-7,10-13, 24, 27, 31- 39, 41-43.

Тема 7. Шкідливе програмне забезпечення та захист від нього

1. Самостійна робота за темою:
   - склад та призначення елементів підсистеми антивірусного захисту;
   - програмні методи антивірусного захисту;
   - загальні шляхи боротьби із програмними вірусами.

Рекомендована література 1-5, 10, 11, 14-16, 25, 29-41, 44, 47, 48, 50-55, 57.

Тема 8. Політика безпеки. Оцінка ефективності систем захисту інформації

-відмінність загроз від вразливості;

-класифікація атак, методики та підходи;

-правове забезпечення захисту інформації в автоматизованих та телекомунікаційних системах, засобах зв'язку;

-основні загрози інформації в ІТС (АСУ) та шляхи їх реалізації;

- особливості реалізації класичного підходу до оцінки ефективності комплексної системи захисту інформації;
- організаційні принципи побудови систем кіберзахисту;

– неформальні методи визначення ефективності систем захисту інформації; вимоги до ефективності систем захисту інформації.

Рекомендована література 2-8, 11, 16, 18-20, 24, 26-35, 41-43, 50-53.

Виконання самостійної роботи студентів можливе у вигляді проходження зазначеного викладачем курсу Cisco. Здача фінального тесту з вказаного курсу переводиться в 15 балів та заноситься до рейтингу поточного оцінювання студента.

Вимоги до оформлення звітів з самостійної роботи студентів:

Звіт з самостійної роботи студентів оформлюється на аркушах формату А4 (210х297 мм) на одній стороні листа білого паперу у вигляді: титульний аркуш, теоретичні питання, список використаної літератури.

Звіт виконується в електронному варіанті (система Windows, текстовий процесор Word) *Вимоги до тексту*: заголовок – 16 пт, текст відповіді – 14 пт, вирівняти по ширині, абзаци зі стандартним відступом першого рядка, інтервал міжрядковий – 1,5, поля: ліве – 3 см, праве – 1 см, верхнє, нижнє – 2 см, колонтитули із зазначенням ПІБ, номера сторінки. Об'єм звіту з самостійної роботи по темі складає 4-7 сторінки.

Якість роботи оцінюється з урахуванням правильності відповідей, підбору літератури, проведеного аналізу та відповідність звіту вказаним вимогам щодо оформлення. Захист звітів (рефератів) з самостійної роботи відбувається шляхом опитування на лабораторній роботі або консультації та представлення презентації реферату.

Критерії оцінювання знань та вмінь студента за результати виконання самостійної роботи за національною шкалою

За результати виконання самостійної роботи студенту виставляється оцінка:

Відмінно, якщо студент вміє використовувати основну та додаткову літературу, в письмовій доповіді повністю і якісно розкрив тему, методично обґрунтовано використав теоретичні знання та практичні навички, у висновках дав вірну технічну інтерпретацію, грамотно оформлену роботу подав в установлений термін, доповідь студента чітка, грамотна, супроводжується комп'ютерною презентацією. Студент вірно та обґрунтовано відповів на поставлені питання з наведенням прикладів та аргументуванням своєї власної точки зору. Допускається наявність незначної кількості огріхів та несуттєвих неточностей, які не призвели до помилок у відповіді;

Добре, якщо студент вміє використовувати основну та додаткову літературу, в письмовій доповіді повністю і якісно розкрив тему, методично обґрунтовано використав теоретичні знання для виконання завдань, у висновках дав вірну технічну інтерпретацію, допустив несуттєву помилку у відповіді або

висновках, допустив незначні відхилення від чинних стандартів при оформленні роботи;

Задовільно, якщо студент в письмовій доповіді розкрив тему, але виконану роботу подав більше двох тижнів після встановленого терміну, допустив помилки у відповіді або висновках, оформлення роботи, не зовсім відповідає чинним вимогам стандартів, доповідь не супроводжується комп'ютерною презентацією.

Не задовільно, якщо студент в письмовій доповіді не розкрив тему, не виконав завдання, отримані результати у висновках інтерпретуються невірно, робота оформлена неохайно.

Критерії переводу балів за результати виконання самостійної роботи з національної шкали в бали ECTS

Відповідність балів національної і кредитно-модульної шкали за виконання самостійної роботи:

Оцінка виконаної студентом самостійної роботи за національною шкалою	Бали ECTS	Оцінка ECTS
5	13,5...15,0	A
4	12,3...13,4	B
	11,1…12,2	C
3	9,6...11,0	D
	9,0...9,5	E
2	5,3…8,9	F
	<5,3	FX

7. Індивідуальні завдання

Виконання індивідуального завдання (ІЗ) є важливою частиною дисципліни «Основи кібербезпеки» та представляє собою самостійне дослідження студента, який оформив індивідуальний графік навчання, або навчається на заочній формі та є альтернативним варіантом виконання лабораторних робіт з дисципліни.

Мета виконання ІЗ є закріплення, узагальнення та поглиблення знань, одержаних студентами під час вивчення дисципліни та їх застосування при самосійній роботі, активізація творчих здібностей студентів, розвиток навичок роботи з нормативно-технічною літературою, прийняття самостійних рішень, набуття практичних навичок роботи щодо захисту інформації програмними та криптографічними засобами.

ІЗ повинно бути результатом самостійних досліджень студента, які:

– сприяють розвитку ініціативності студентів у їх виробничій і дослідницькій діяльності;

– поглиблюють, систематизують та закріплюють теоретичні знання та практичні навички, отримані під час навчання;

– перевіряють уміння студента самостійно освоювати та використовувати сучасні інформаційні технології;

– розвивають у студента навички ведення самостійного науково-практичного пошуку, оволодіння методикою дослідження й експериментування в ході вирішення проблем і питань, поставлених до виконання;

– сприяють набуттю вміння аналізувати отримані результати досліджень, формулювати висновки та положення.

За всі відомості, що викладені в ІЗ, порядок використання в ході підготовки фактичного матеріалу та іншої інформації, пропозиції, технології, обґрунтованість і вірогідність висновків та положень, що захищаються, несе відповідальність безпосередньо автор.

Викладач надає студенту допомогу у виборі теми роботи, проводить консультації з проблемних питань, що виникають у процесі виконання, надає допомогу в пошуку методичної та технічної документації, науково-технічної літератури.

Номер варіанта завдання відповідає порядковому номеру студента в журналі списку групи. Варіанти завдань на ІЗ представлено в таблиці 1.

Таблиця 1 – Варіанти індивідуальних завдань

№ варіанту	**№ питання 1**	**№ питання 2**	**№ питання 3**	**№ задачі 1**	**№ задачі 2**	**№ задачі 3**
1.	1	70	91	35	11	1
2.	2	69	92	34	12	2
3.	3	68	93	33	13	3
4.	4	67	94	32	14	4
5.	5	66	95	31	15	5
6.	6	65	96	30	16	6
7.	7	64	97	29	17	7
8.	8	63	98	28	18	8
9.	9	62	99	27	19	9
10.	10	61	100	26	20	10
11.	11	60	105	25	30	11
12.	12	59	104	24	31	12
13.	15	58	103	23	32	13
14.	16	57	102	22	33	14
15.	13	56	101	21	34	15
16.	14	55	90	20	35	16
17.	30	54	89	1	21	17

№ варіанту	№ питання 1	№ питання 2	№ питання 3	№ задачі 1	№ задачі 2	№ задачі 3
18.	31	53	88	2	22	18
19.	35	52	87	3	23	19
20.	32	51	86	4	1	20
21.	33	50	85	5	2	21
22.	34	49	84	6	3	22
23.	17	48	83	7	4	23
24.	18	47	82	8	5	24
25.	19	46	81	9	6	25
26.	20	45	65	10	7	26
27.	21	44	66	11	8	27
28.	22	43	67	12	9	28
29.	23	42	68	13	10	29
30.	24	41	69	14	24	30
31.	25	40	80	15	25	31
32.	26	39	71	16	26	32
33.	27	38	72	17	27	33
34.	28	37	73	18	28	34
35.	29	36	74	19	29	35

Теоретичні питання:

1. Дайте визначення поняттям: «експлойт (exploit)», «блокування інформації», «авторизація», «несанкціонований доступ до інформації».
2. Дайте визначення поняттям: «люк (backdoors)», «MAC-адреса (Media Access Control) », «база даних», «комп’ютерний злочин».
3. Дайте визначення поняттям: «adware (spyware)», «OSI (Open System Interconnect Reference Model)», «підробка інформації», «біометричні методи аутентифікації».
4. Дайте визначення поняттям: «API (Application Programming Interface)», «витік інформації», «побічне електровипромінювання і навід», «авторизація».
5. Дайте визначення поняттям: «ботнет (botnet)», «відстань єдності шифру», «порт», «адміністрування».
6. Дайте визначення поняттям: «клавіатурні перехоплювачі (keyloggers)», «втрата інформації», «портал», «аудит».
7. Дайте визначення поняттям: «дифейсмент (defacement)», «дані», «поштовий клієнт», «аутентифікація».
8. Дайте визначення поняттям: «відмова в обслуговуванні (DoS)», «дифузія», «поштовий сервер», «суб’єкт доступу».
9. Дайте визначення поняттям: «DDoS (Distributed Denial of Service)», «доступність інформації», «провайдер», «ідентифікатор».

10. Дайте визначення поняттям: «Firewall», «загроза безпеці інформації», «псування інформації», «користувач».

11. Дайте визначення поняттям: «експлойт (exploit)», «загроза безпеці інформації в системах обробки інформації», «розкриття інформації», «фактор аутентифікації».

12. Дайте визначення поняттям: «IRC (Internet Relay Chat)», «закладка», «розсіювання», «парольна аутентифікація».

13. Дайте визначення поняттям: «логічні бомби (Logic bombs)», «захист інформації», «стек», «однонаправлені хеш-функції ».

14. Дайте визначення поняттям: «MAC-код», «ідентифікація», «таємна інформація», «PIN-код».

15. Дайте визначення поняттям: «поштові бомби (Mail bombs)», «OSI (Open System Interconnect Reference Model)», «стек мережних протоколів», «біометрична характеристика».

16. Дайте визначення поняттям: «фішинг (Phishing)», «ім’я хосту», «трасування програм», «статичні біометричні характеристики».

17. Дайте визначення поняттям: «фармінг (Pharming)», «інсайдер», «троянські коні», «динамічні біометричні характеристики».

18. Дайте визначення поняттям: «pornware», «інформація з обмеженим доступом», «тезаурус», «одноразові паролі».

19. Дайте визначення поняттям: «riskware», «інформаційна безпека», «уразливість», «OTP-токен».

20. Дайте визначення поняттям: «руткіт (Rootkit)», «інформаційна система», «технічний захист інформації», «симетрична криптографія».

21. Дайте визначення поняттям: «SDK (Software Development Kit)», «канал просочування інформації», «флеш-накопичувач», «асиметрична криптографія».

22. Дайте визначення поняттям: «сніфінг (sniffing)», «комп’ютерна система», «хост», «електронний цифровий підпис».

23. Дайте визначення поняттям: «спуфінг (spoofing)», «комп’ютерне шахрайство», «цілісність», «порушник безпеки».

24. Дайте визначення поняттям: «бомби з годинниковим механізмом (time bobms)», «контроль доступу», «конфіденційність», «загроза безпеці».

25. Дайте визначення поняттям: « UDP (User Datagram Protocol)», «конфіденційна інформація», «доступність», «концепція безпеки».

26. Дайте визначення поняттям: «VLAN (Virtual Local Area Network)», «персональні дані», «черв’як», «DES (Data Encryption Standart)».

27. Дайте визначення поняттям: «вішинг (vishing)», «крадіжка інформації», «інформаційно-комунікаційна системи», «алгоритм RSA ».

28. Дайте визначення поняттям: «XSL-атака», «критичні комп’ютерні системи», «інформаційно-комунікаційна система», «шифр IDEA».

29. Дайте визначення поняттям: «зомбі (zombies)», «марштуризатор», «інформаційно-телекомунікаційна система», «державна таємниця».

30. Дайте визначення поняттям: «автентифікація», «мережний протокол», «комплексні системи захисту інформації», «комерційна таємниця».

31. Дайте визначення поняттям: «автентичність», «метод», «криптографія», «лікарська таємниця».

32. Дайте визначення поняттям: «апельованість», «навмисна силова дія», «криптологія», «шифрування».

33. Дайте визначення поняттям: «атаки методом підбору пароля (Brute force attacks)», «дампер», «стаганографія», «ключ».

34. Дайте визначення поняттям: «безпека інформації», «обчислювально стійка криптосистема», «автоматизована система класу 1», «гамування».

35. Дайте визначення поняттям: «безпечний час», «перемішування», «автоматизована система класу 2», «імітовставка».

36. Акт обстеження об’єкту інформаційної діяльності.

37. Рівні інформаційно-комунікаційної системи.

38. Функціональні сервіси безпеки і механізми, що їх реалізують.

39. Підсистеми керування доступом.

40. Підсистема ідентифікації та аутентифікації.

41. Підсистема аудиту.

42. Підсистема забезпечення цілісності.

43. Захист інформації від випадкових загроз.

44. Технічні методи й засоби захисту інформації.

45. Захист інформації від несанкціонованого доступу.

46. Моделі дискреційної політики безпеки.

47. Моделі мандатної політики безпеки.

48. Помилки переповнення буферу.

49. Помилки оброблення текстових рядків.

50. Класифікація шкідливого програмного забезпечення. Люки.

51. Програмні закладки, методи та засоби боротьби.

52. Комп’ютерні віруси, їх класифікація, методи та засоби боротьби.

53. Мережеві хробаки: класифікація, методи та засоби боротьби.

54. «Троянські коні»: класифікація, методи та засоби захисту.

55. Нормативно-правова база України в сфері захисту інформації та забезпечення захисту інформації в інформаційно-комунікаційних системах.

56. Захист інформації на рівні операційної системи: апаратне забезпечення засобів захисту.

57. Поняття захищеної операційної системи.

58. Типова архітектура комплексу засобів захисту операційної системи.

59. Безпека UNIX-операційних систем.

60. Адміністрування засобів безпеки UNIX.

61. Засоби захисту в операційних системі сімейства Windows

62. Політика безпеки: основні поняття, структура, розробка політики безпеки.

63. Міжнародні стандарти інформаційної безпеки.

64. Симетричні криптографічні системи.

65. Асиметричні криптографічні системи.
66. Кваліфікований електронний підпис.
67. Управління криптоключами.
68. Аутентифікація на основі багаторазових паролів.
69. Аутентифікація на основі одноразових паролів.
70. Аутентифікація на основі PIN-коду.
71. Протоколи аутентифікації в локальній мережі.
72. Механізми аутентифікації при здійсненні підключення.
73. Аутентифікація в захищеному з'єднанні.
74. Застосування апаратних засобів аутентифікації та зберігання ключової інформації.
75. Active Directory. Адміністрування домену Active Directory ОС Windows Server.
76. Системи оброблення конфіденційної інформації Trusted Solaris.
77. Операційна система Фенікс.
78. Архітектура захищених мереж.
79. Міжмережні екрани.
80. Системи виявлення атак.
81. Системи аналізу й оцінювання вразливості.
82. Особливості функціонування міжмережних екранів на різних рівнях моделі OSI.
83. Схеми мережевого захисту на базі між мережевих екранів.
84. Віртуальні захищені мережі, концепція побудови.
85. Захисті інформації на сеансовому рівні.
86. Захисті інформації на канальному рівні.
87. Захисті інформації на мережному рівні.
88. Організація захищеного віддаленого доступу.
89. Управління доступом по схемі однократного входу з авторизацію Single Sign-On.
90. Протокол Kerberos.
91. Інфраструктура управління з відкритими ключами PKI.
92. Засоби виявлення мережевих атак.
93. Створення комплексних систем захисту інформації.
94. Технічні засоби захисту інформації.
95. Методи управління засобами мережної безпеки.
96. Аудит і моніторинг безпеки.
97. Рівні реалізації віртуальних захищених мереж.
98. Захист віртуальних каналів на сеансовому рівні.
99. Захист віртуальних каналів на мережному рівні.
100. Захист віртуальних каналів на канальному рівні.
101. Групові політики ОС Windows Server.
102. Процеси управління обліковими записами користувачів і груп користувачів в ОС UNIX/Linux.

103. Засоби безпеки ОС Windows Server.

104. Відновлення системи та резервне копіювання даних.

105. Логічна і фізична структури, управління реплікацією Active Directory. Управління організаційними підрозділами, делегування повноважень.

Практичні завдання:

Задача №1. Провести шифрування текстових даних за допомогою криптографічного шифру Цезаря з використанням гасла, таблиця 2.

Таблиця 2 – Варіанти завдань для виконання Задачі № 1

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
1.	Захист	Вимоги безпеки до технологічного обладнання та процесів
2.	Підручник	Інтерфейс прикладного програмування системи
3.	Синема	Для створення шифрованого тексту на вихідний накладається гама.
4.	Зупинка	Атака, що має на меті змусити сервер не відповідати на запити
5.	Порушник	Безліч людей розмовляють в масштабі реального часу шляхом набору повідомлень на клавіатурі
6.	Гроза	Сьогодні є чимало каналів просочування інформації з організації
7.	Модель	У першій частині розглядаються загальні проблеми безпеки інформаційних систем
8.	Форма	У другій частині увага приділяється методам та засобам можливого вирішення цих проблем
9.	Техніка	Роль інформації в сучасному світі та необхідність її захисту
10.	Слова	Разом з поняттям інформація, важливе значення має поняття дані
11.	Ключ	Від інформації дані відділяються конкретною формою подань.
12.	Пароль	Інформація на стадії даних характеризується певною формою подання й додатковою характеристикою
13.	Футляр	Нематеріальність інформації полягає у тому, що не можна виміряти параметри відомими фізичними методами
14.	Вірус	Таким чином, інформація зберігається і передається на матеріальних носіях
15.	Клей	Все що є матеріальним об’єктом, інформацією бути не може

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
16.	Користувач	Інформація не може існувати сама по собі, у відриві від матеріального носія
17.	Логін	Матерія ж не може не нести інформації, оскільки завжди перебуває в певному стані
18.	Флешка	Матеріальними носіями інформації можуть бути мозок людини, звукові та електромагнітні хвилі
19.	Тенол	Інформація, якщо вона міститься на матеріальному носієві, доступна людині.
20.	Техніка	Цінність інформації визначається мірою її корисності для власника
21.	Захист	Якщо доступ до інформації обмежується, то така інформація є конфіденційною
22.	Крипто	Для позначення цінності конфіденційної комерційної інформації використовується категорія конфіденційно
23.	Граф	Інформацію правочинно розглядати як товар, що має певну цінність
24.	Модель	Кількість інформації тим більша, чим нижча ймовірність події
25.	Теорія	Підхід ентропії широко використовується при визначенні кількості інформації, переданої по каналах зв’язку
26.	Процес	Тезарусний підхід заснований на розумінні інформації як знань
27.	Директор	У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна зменшується
28.	Завуч	Проблеми захисту інформації непокоїли людство з давніх-давен.
29.	Равлик	Необхідність захисту інформації виникла через потребу таємного передавання інформації (повідомлень)
30.	Таємниця	Створення сучасних комп’ютерних систем і мереж радикально змінили характер і діапазон проблем захисту інформації.
31.	Краб	Античні спартанці шифрували свої військові повідомлення
32.	Шифр	Завдяки персональним комп’ютерам працювати з інформацією дуже просто

№ варіанту	Гасло-шифр	Текст, який необхідно зашифрувати
33.	Портал	Зловмисникам стало набагато простіше викрадати конфіденційну інформацію
34.	Ложка	Краще вчитися на чужих помилках. Нехай навіть безглуздих
35.	Монстер	Чим безглуздіша помилка, тим передбачливішими треба бути, щоб її передбачити.

Задача №2. Провести шифрування текстових даних із використанням криптографічного шифру перестановки з наступними параметрами:

№ варіанту	Ключове слово	Текст, який потрібно зашифрувати
1.	Файл	Існують різні методи боротьби з фішингом
2.	Засіб	Ніколи не відповідайте на листи, що запитують вашу конфіденційну інформацію
3.	Фітинг	У разі одержання інформації з джерела, яке викликає у вас недовіру перевірте його сайт
4.	Фішинг	Регулярно перевіряйте стан своїх електронних рахунків
5.	Рівень	Перевіряйте рівень захисту відвідуваного вами сайту
6.	Метод	Будьте обережними, працюючи з електронними листами й конфіденційними даними
7.	Захист	Забезпечте якісний захист свого комп’ютера
8.	Копія	Завжди повідомляйте по виявлену підозрілу активність
9.	Диск	Алгоритми симетричного шифрування використовують ключі не дуже великої довжини.
10.	Інтер	Алгоритми симетричного шифрування можуть швидко шифрувати великі обсяги даних.
11.	Буква	Ключ шифрування в асиметричних системах називається відкритим ключем
12.	Шифр	Ключ розшифрування потрібно тримати в секреті
13.	Рупор	На противагу тайнопису криптографією з ключем називають сьогодні алгоритми шифрування
14.	Колесо	У криптографічних системах ключ формує людина або він створюється автоматично
15.	Інформація	Усі крипто алгоритми з ключем поділяються на симетричні і асиметричні
16.	Мережа	У симетричних криптоалгоритмах використовуються ідентичні ключі

№ варіанту	Ключове слово	Текст, який потрібно зашифрувати
17.	Літера	Ключ несе у собі всю інформацію про засекречування повідомлення
18.	Коефіцієнт	Електростатичне і магнітостатичне екранування ґрунтується на замиканні екраном
19.	Україна	На високій частоті застосовується виключно електромагнітне екранування
20.	Небо	Двері і вікна приміщення серверної кімнати повинні бути екрановані
21.	Соловей	Усі системи захисту телефонних ліній поділяються на пасивні і активні
22.	Калина	Для контролю стану ліній зв’язку використовуються різні індикатори
23.	Сонце	Апаратура пригнічення радіовипромінюючих пристроїв прослуховування являє собою генератор шумових перешкод
24.	Козак	Робоче місце користувача автоматизованої системи має бути обладнане відповідно до рекомендацій
25.	Гетьман	Помилкові операції або дії можуть викликати відмови апаратних і програмних засобів.
26.	Мороз	Деякі помилкові дії можуть привести до порушень цілісності інформації
27.	Загрево	Для блокування помилкових дій використовуються технічні й апаратно-програмні засоби
28.	Цінність	Дублювання інформації є ефективним способом забезпечення цілісності інформації
29.	Конфіденційність	Найбільш простим методом дублювання інформації є використання виділених ділянок на робочому диску
30.	Руйнування	Найбільшого поширення комп’ютерні віруси зазнали з розвитком персональних комп’ютерів
31.	Наклеп	Особливістю пакетного вірусу є розміщення його голови в пакетному файлі
32.	Техніка	Копіювання вірусу в середину файлу може статися в результаті помилки вірусу
33.	Практика	До шкідливого програмного забезпечення відносять також віруси і хробаки
34.	Зошит	Найуразливішими з точки зору безпеки є критичні комп’ютерні системи
35.	Папір	Технічні засоби і системи можуть лише випромінювати в довкілля сигнали

Задача №3 Виконати практичне завдання відповідно до варіантів.

№ варіанту	Завдання
1.	Описати програму антивірусного захисту, якою Ви використовуєте. Навести скріншоти інтерфейсу даного програмного продукту.
2.	Засобами операційної системи створити 5 облікових записів та задати паролі на вхід. Навести скріншоти виконання завдання та перевірити правильність входу.
3.	Провести налаштування політики облікових записів: мінімальна довжина паролю 12 символів; максимальний термін дії паролю – 30 днів; пароль повинен відповідати вимогам складності – включено; зберігати паролі, використовуючи зворотне шифрування – включено. Навести скріншоти виконання завдання.
4.	Провести налаштування політики облікових записів: мінімальна довжина паролю 7 символів; максимальний термін дії паролю – 25 днів; пароль повинен відповідати вимогам складності – включено; зберігати паролі, використовуючи зворотне шифрування – включено. Навести скріншоти виконання завдання.
5.	Провести налаштування політики блокування облікових засобів: порогове значення блокування 5 спроб на 10 хвилин. Навести скріншоти виконання завдання.
6.	Провести налаштування політики блокування облікових засобів: порогове значення блокування 3 спроби на 5 хвилин. Навести скріншоти виконання завдання.
7.	Провести налаштування політики блокування облікових засобів: порогове значення блокування 4 спроби на 8 хвилин. Навести скріншоти виконання завдання.
8.	Провести налаштування політики блокування облікових засобів: порогове значення блокування 6 спроби на 15 хвилин. Навести скріншоти виконання завдання.
9.	Провести налаштування політики блокування облікових засобів: порогове значення блокування 3 спроби на 4 хвилини. Навести скріншоти виконання завдання.
10.	Провести налаштування політики облікових записів: мінімальна довжина паролю 9 символів; максимальний термін дії паролю – 56 днів; пароль повинен відповідати вимогам складності – включено; зберігати паролі, використовуючи зворотне шифрування – включено. Навести скріншоти виконання завдання.

11.	Провести налаштування політики облікових записів: мінімальна довжина паролю 7 символів; максимальний термін дії паролю – 25 днів; пароль повинен відповідати вимогам складності – включено; зберігати паролі, використовуючи зворотне шифрування – включено. Навести скріншоти виконання завдання.
12.	Провести налаштування політики блокування облікових засобів: порогове значення блокування 2 спроби на 5 хвилин. Навести скріншоти виконання завдання.
13.	Провести налаштування локальної політики безпеки: політика аудиту. Встановити: аудит входу в систему – успіх та відмова. Навести скріншоти виконання завдання.
14.	Провести налаштування локальної політики безпеки: політика аудиту. Встановити: аудит зміни політики – успіх та відмова. Навести скріншоти виконання завдання.
15.	Провести налаштування локальної політики безпеки: політика аудиту. Встановити: аудит подій входу в систему – успіх та відмова. Навести скріншоти виконання завдання.
16.	Провести налаштування локальної політики безпеки: призначення прав користувача. Встановити: доступ до комп’ютера з мережі . Навести скріншоти виконання завдання.
17.	Провести налаштування локальної політики безпеки: призначення прав користувача: локальний вхід в систему. Видалити «гість». Навести скріншоти виконання завдання.
18.	Провести налаштування локальної політики безпеки: параметри безпеки. Облікові записи: перейменування облікового запису адміністратора – вказати нове ім'я (прізвище студента). Навести скріншоти виконання завдання.
19.	Провести налаштування локальної політики безпеки: параметри безпеки. Облікові записи: перейменування облікового запису гостя – вказати нове ім'я (скорочене прізвище студента). Навести скріншоти виконання завдання.
20.	Провести налаштування локальної політики безпеки: параметри безпеки. Облікові записи: дозволити використання пустих паролів для входу тільки при консольному вході – Виключити. Навести скріншоти виконання завдання.
21.	Провести налаштування локальної політики безпеки: параметри безпеки. Мережева безпека: не зберігати хеш LAN Manager при наступній зміні пароля – Включено (увімкнуто). Навести скріншоти виконання завдання.
22.	Вибрати будь-який доступний документ, запустити процедуру архівування, встановити пароль на відкриття документу та перевірити його дію. Навести кріншоти виконання операції.

23.	Створити документ в Microsoft Word встановити пароль на відкриття документу, на дозвіл запису.
24.	Створити документ в Microsoft Excel встановити пароль на відкриття документу, на дозвіл запису. Провести налаштування параметрів захисту конфіденційності інформації та захисту від макросів.
25.	Створити документ в Microsoft PowerPoint встановити пароль на відкриття документу. Провести перевірку та навести скріншоти виконання завдання.
26.	Створити документ в Microsoft Access встановити пароль на відкриття документу, на дозвіл запису. Провести перевірку та навести скріншоти виконання завдання.
27.	Провести сканування ПК на наявність вірусів доступним програмним засобом та зробити аналіз результатів перевірки. Навести скріншоти виконання завдання.
28.	Вибрати будь-який доступний документ, запустити процедуру архівування, встановити пароль на відкриття документу та перевірити його дію. Навести кріншоти виконання операції.
29.	Створити документ MS Word, захистити документ за допомогою стеганографічних методів засобами колонтитулів. Провести перевірку та навести скріншоти виконання завдання.
30.	Створити документ в Microsoft Excel встановити пароль на відкриття документу, на дозвіл запису. Провести налаштування параметрів захисту конфіденційності інформації та захисту від макросів. Провести перевірку на навести скріншоти виконання завдання.
31.	Створити документ в Microsoft Word встановити пароль на відкриття документу, на дозвіл запису. Провести перевірку на навести скріншоти виконання завдання.
32.	Вибрати будь-який доступний документ, запустити процедуру архівування, встановити пароль на відкриття документу та перевірити його дію. Навести кріншоти виконання операції.
33.	Створити документ в Microsoft Word встановити пароль на відкриття документів, на дозвіл запису. Провести налаштування параметрів захисту конфіденційності інформації та захисту від макросів.
34.	Провести сканування ПК на наявність вірусів доступним програмним засобом та зробити аналіз результатів перевірки.
35.	Створити документ в Microsoft Excel встановити пароль на відкриття документів, на дозвіл запису. Провести налаштування параметрів захисту конфіденційності інформації та захисту від макросів.

8. Методи навчання

На лекційних заняттях: розповідь, пояснення, демонстрація, бесіда, дискусія. На лабораторних роботах: пояснення, дослідження, розв`язування ситуаційних задач, виконання індивідуального варіанту завдання. Самостійна робота студента: реферати, повідомлення, науково-пошукові, дослідницькі проекти, виконання он-лайн курсів.

За джерелами знань використовуються такі методи навчання: словесні – розповідь, пояснення, лекція, інструктаж; наочні – демонстрація, ілюстрація; практичні – лабораторна робота, практична робота, вправи. За характером логіки пізнання використовуються такі методи: аналітичний, синтетичний, аналітико-синтетичний, індуктивний, дедуктивний. За рівнем самостійної розумової діяльності використовуються методи: проблемний, частково-пошуковий, дослідницький.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль в тому числі у вигляді комп’ютерних тестів, виконання практичних робіт.

Поточний контроль здійснюється під час проведення практичних (лабораторних) занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль, комп’ютерне тестування, виконання практичного завдання. Оцінюється вхідний, проміжний, кінцевий рівень знань студента.

Підсумковий контроль проводиться у вигляді комп’ютерних тестів.

10. Розподіл балів

Поточне тестування та самостійна робота								Сума
Змістовий модуль №1			Змістовий модуль № 2		Змістовий модуль № 3			
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	100
7	8	7	11	23	11	20	13	

В межах ОК на освітньому порталі розміщено рейтинг лист, де детально можна ознайомитись з бали по кожному виду занять, поточному та підсумковому контролю.

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Лобанчикова Н.М. Захист інформації в АСУ: навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.
2. Конституція України.
3. Закон України «Про захист інформації в автоматизованих системах»
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 № 80/94-ВР (Зі змінами, внесеними згідно із Законом № 1703-IV від 11.05.2004, в редакції Закону № 2594-IV від 31.05.2005, ВВР, 2005, № 26, ст. 347).
5. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
6. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визна¬чення.
7. ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
8. ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
9. ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.
10. Інформаційні технології. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:1995): ДСТУ 3918–1999. – [Чинний від 2000–01–01]. – К.: Держстандарт України, 2000. – 50 с. – (Національний стандарт України).
11. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

12. НД ТЗІ 2.5-004-99: Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

13. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.

14. НД ТЗІ 1.4-001-2000: Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.

15. Закон України «Про інформацію» № 2657-ХИ від 02.10.1992. - ВВР, 1992, № 48, ст. 650.

16. Закон України «Про державну таємницю» № 3855-ХП від 21.01.1994, ВВР, 1994, № 16, ст. 93 (остання редакція № 1519-IV від 19.02.2004).

17. Закон України «Про електронні документи і електронний документообіг», № 851-IV від 22.05.2003, ВВР, 2003, № 36, ст. 275 (зі змінами, внесеними згідно із Законом № 2599-IV від 31.05.2005, ВВР, 2005, № 26, ст. 349).

18. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

19. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

20. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

21. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

22. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

23. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.

24. ДБН 2.2-3-2004 Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.

25. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 № 84.

26. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

27. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ЕОТ-95). Затверджені наказом ДСТЗІ від 09.06.1995 № 25.

28. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія /Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. Житомир : ЖНАЕУ, 2016 – 636 с.

30. Белов Е.Б. Основы информационной безопасности. Учебное пособие для студентов вузов. /Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.– М.: Горячая линия – Телеком, 2006. – 544 с.

31. Бобунов А.І. Захист інформації в автоматизованих системах / Бобунов А.І., Шестаков В.І. Захист інформації в автоматизованих системах: Навчальний посібник. – Житомир: ЖВІРЕ, 2004. - 172 с.

32. Kevin Mitnick. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big./ Kevin Mitnick.– New York, Boston, London: Little, Brown and Company, 2017 – 320 с.

33. Грайворонський М.В. Безпека інформаційно-комунікаційних систем/ М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009.– 608с.

34. Поповский В.В. Зашита информации в телекоммуникационных системах: Учебник: В 2 т./ В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМИТ», 2006. – Т.1.– 286 с.

35. Поповский В.В. Зашита информации в телекоммуникационных системах: Учебник: В 2 т./ В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМИТ», 2006. – Т.2.– 292с.

36. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. / А.А. Малюк. – М.: «Горячая линия» – Телеком, 2004. – 280 с

37. Joseph Menn. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World/ Joseph Menn.– New York: PublicAffairs, 2019.– 270.

38. Kevin Mitnick. Ghost In The Wires: My Adventures as the World's Most Wanted Hacker/ Kevin Mitnick.– New York, Boston, London: Little, Brown and Company, Back Bay Books, 2012 – 448 с.

39. Лобанчикова Н.М., Пірог О.В. Основи кібербезпеки. Методичні рекомендації до виконання лабораторних робіт. Ч. 1. – Житомир, Житомирська політехніка, 2021. – 56 с.

40. Лобанчикова Н.М., Пірог О.В. Основи кібербезпеки. Методичні рекомендації до виконання лабораторних робіт. Ч. 2. – Житомир, Житомирська політехніка, 2021. – 36 с.

Допоміжна література

41. Кукацкий А.В. Обнаружение атак / А.В. Кукацкий СПб.: БХВ – Петербург, 2001. - 624 с.

42. Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности / В.Ю. Скиба, В.А. Курбатов – СПб: Питер, 2008.– 320 с.

43. Купер М. Анализ типовых нарушений безопасности в сетях.: Пер. с англ. / С.Норткат, М.Купер, М.Фирноу, К.Фредерик – М.: «Вильямс», 2001. – 464 с.

44. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов– СПб: Наука и техника, 2004. – 384 с.

45. Коваленко М.М. Комп’ютерні віруси і захист інформації / М.М. Коваленко – К.: Наукова думка, 1999. – 267 с.

46. Хоффман Л. Современные методы защиты информации / Хоффман Л. пер. с англ. / Под ред. В.А. Герасименко. – М.: Сов. Радио, 1980. – 264 с.

47. Мельников В.В. Защита информации в компьютерных системах / В.В.Мельников – М.: Финансы и статистика. Электроинформ, 1997. – 368 с.

48. Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник./М. Мамаев, С. Петренко – СПб.: Питер, 2002.– 848 с.: ил.

49. Защита информации в компьютерных системах и сетях / [Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.]; под ред. В. Ф. Шаньгина.-2-е изд., перераб. и доп.-М.: Радио и связь, 2001.-376 с: ил.

50. Фергюсон Н. Практическая криптография. : Пер. с англ./ Н. Фергюсон, Б. Шнайер – М.: Издательский дом "Вильямс", 2005. – 424 с. : ил.

12. Інформаційні ресурси в Інтернеті

51. Стандарти інформаційної безпеки: http://www.is-standard.com

52. Інформаційна безпеки: науковий журнал: http://www.nbuv.gov.ua/portal/natural/Ibez/index.html

53. Семенов Ю.А. Telecommunication technologies – телекоммуникационные технологии. Интернет-публикации сайта http://book.itep.ru.

54. Тематические курсы Интернет-университета информационных технологий. Интернет-публикации сайта http://www.intuit.ru.

55. Центр інформаційної безпеки: http://www.bezpeka.com

56. Журнал «Інформаційні технології. Аналітичні матеріали»: http://it.ridne.net/taxonomy/term/14

57. Интернет-публикации сайта-каталога http://www.all-ebooks.com.

58. Введение в криптографию под ред. В. В. Ященко // http://nature.web.ru/db/msg.html?mid=1157083&uri=node1.html

59. Казарин О. В. Безопасность программного обеспечения компьютерных систем // http://citforum.ru/security/articles/kazarin

60. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров//http://www.ssl.stu.neva.ru/psw/crypto/rostovtsev/cryptoanalysis.html

61. Федотов Н. Н. Защита информации (Учебный курс) // http://www.college.ru/UDP/texts/index.html.