МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет

АПАРАТНІ ТА ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

методичні вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання

Луцьк 2025

УДК 004.056(075.8)+681.518(075.8)
А76

Рекомендовано до видання вченою радою факультету комп'ютерних та інформаційних технологій ЛНТУ, протокол № ___ від _____ 2025 року.

Голова Вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № ___ від _____ 2025 року

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладачі: _____ Олег КАЙДИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Олена МАЦІБОРКО, директор ТОВ «ВОРРРК»

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

А76 Апаратні та програмні засоби захисту інформації: методичні вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 24 с.

Пропоноване видання спрямоване на самостійну та якісну підготовку здобувачів освіти з курсу «Апаратні та програмні засоби захисту інформації».

Наведено мету, завдання та необхідні інформаціні джерела для усвідомлення проблематики винесениз для опрацювання питань. Розв'язання тестових завдань дозволить провести самооцінювання, а перелік екзаменаційних питань дозволять якісно підготуватися до атестації.

ВСТУП

В умовах стрімкого розвитку інформаційних технологій та їх проникнення до усі сфер життєдіяльності суспільства питання захисту інформації набуває особливої актуальності. Зростання обсягів цифрових даних, розширення мережевих взаємодій та поява нових кіберзагроз зумовлюють необхідність глибокого розуміння принципів і методів забезпечення інформаційної безпеки.

Методичні вказівки з курсу «Апаратні та програмні засоби захисту інформації» розроблено у відповідності до робочої програми, а їх метою є надання здобувачам освіти необхідних знань та практичних навичок щодо застосування апаратних та програмних засобів для ефективного захисту інформаційних ресурсів.

Самостійна робота здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» спрямована на поглиблене вивчення теоретичних аспектів дисципліни та набуття ними практичних навичок у сфері захисту інформації. Опанування матеріалу майбутнім фахівцям дозволить ефективно розв’язувати завдання, які пов’язані із забезпеченням конфіденційності, цілісності та доступності інформації в різноманітних інформаційних системах.

ЗМІСТ

Сторінка

І. Мета та завдання курсу «Апаратні та програмні засоби захисту інформації»

Мета вивчення дисципліни. Надання здобувачам вищої освіти базових знань про загрози, небезпеку та ступеня ризику втрати інформації, а також нормативно-правові, організаційні та технічні підходи до збереження та захисту інформації.

Завдання вивчення дисципліни. Ознайомити здобувачів вищої освіти з нормативними документами, методами, засобами й технологіями у галузі захисту інформації та інформаційної безпеки.

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

– загальні компетентності:

КЗ 2. Здатність застосовувати знання у практичних ситуаціях;

КЗ 3. Здатність до розуміння предметної області та професійної діяльності;

КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел;

– спеціальні компетентності:

КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп'ютерно-інтегрованих систем та системної мережної структури, управління ними;

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків;

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

Результати навчання. Результати навчання вивчення дисципліни «Апаратні та програмні засоби захисту інформації» базуються на програмних результатах навчання:

ПРН 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та

інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій;

ПРН 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

II. Самостійна робота з курсу «Апаратні та програмні засоби захисту інформації»

САМОСТІЙНА РОБОТА №1

Тема. Основні поняття та структура інформаційної безпеки.
Мета: опанувати теоретичні основи та принципи інформаційної безпеки.
Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Інформаційна безпека.
2. Захист інформації.
3. Властивості інформації.
4. Законодавча класифікація видів інформації.
5. Чинники розвитку технічного захисту інформації.

Рекомендована література: [1-17].

САМОСТІЙНА РОБОТА №2

Тема. Концептуальні засади забезпечення інформаційної безпеки в Україні.
Мета: опанувати нормативно-правове забезпечення інформаційної безпеки.
Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Інформаційна сфера. єдиний інформаційний простір.
2. інформаційний ресурс.
3. Загроза інформаційній безпеці.
4. Несанкціоноване втручання.
5. Технічний захист інформації.

6. Які базові засади інформаційної безпеки викладено в нормативних документах України.

7. Що складає правову основу забезпечення технічного захисту інформації?

8. Основні напрями та першочергові заходи державної політики у сфері технічного захисту інформації.

Рекомендована література: [1-17].

САМОСТІЙНА РОБОТА №3

Тема. Методи та засоби захисту в інформаційній безпеці. Огляд безпеки системи.

Мета: опанувати основні завдання захисту інформації, класифікацію методів і засобів захисту інформації, структуру політики безпеки.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Політика безпеки: основні поняття та принципи.
2. Структура політики безпеки та її основні частини.
3. Життєвий цикл розробки систем безпеки.
4. Система безпеки: основні поняття про інформацію.
5. Критерії оцінки системи безпеки відповідно до нормативного документу НД ТЗІ.
6. Законодавча база України відповідно до систем безпеки.
7. Поняття про інформацію з обмеженим доступом.

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №4

Тема. Загрози інформаційної безпеки. Основні види атак, принципи криптоаналізу.

Мета: опанувати основні засади запобігання загрозам інформаційній безпеці та класифікацію атак на криптограми й мезанізми захисту від них.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Типи атак на інформаційні системи.
2. Основні поняття теорії криптоаналізу.

3. Класифікація можливих загроз інформаційної безпеки.
4. Атаки на симетричні та асиметричні криптоалгоритми.
5. Основи диференціального та лінійного криптоаналізу.

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №5

Тема. Механізми і політики розмежування прав доступу.

Мета: ознайомитись з нормативними документами, які спрямовано на безпеку інформаційної системи.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. «Помаранчева книга».
2. Основні положення системи безпеки за «Помаранчевою книгою».
3. Критерії європейського стандарту у галузі оцінки захищеності комп'ютерних систем.
4. Основні положення нормативного документу НД ТЗІ 2.5-004-99.
5. Основні рівні довіри за європейським стандартом.
6. Послуги та механізми безпеки інформаційних систем.
7. Вимоги довіри (гарантії безпеки) на різних етапах життєвого циклу системи безпеки.

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №6

Тема. Шифрування даних.

Мета: опанувати основні принципи теорії зв'язку в секретних системах.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Основні показники ефективності секретних систем.
2. Класифікація сучасних криптосистем та основні вимоги до них.
3. Класифікація симетричних та асиметричних криптосистем та основні вимоги щодо їх безпеки.
4. Переваги та недоліки комбінованих криптосистем.
5. Основні математичні операції щодо побудови криптосистем.

Рекомендована література: [1; 3; 4; 6; 10…17].

САМОСТІЙНА РОБОТА №7

Тема. Алгоритми з секретним та відкритим ключами.

Мета: ознайомитись з модифікаціями стандарту DES та опанувати його основні режими роботи.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Основні операції шифрування у DES.
2. Основні модифікації шифру DES.
3. Переваги та недоліки 3DES і DESX.
4. Операції шифрування алгоритму криптографічного перетворення.
5. Основні відмінності операцій шифрування у алгоритмі Rijndael.
6. Основні режими роботи блоково-симетричних шифрів на основі використання алгоритму DES.
7. Сучасні потокові шифри, їх переваги та недоліки.
8. Алгоритм асиметричного шифрування даних RSA.
9. Основні операції алгоритму Ель-Гамаля.
10. Протокол забезпечення автентичності та конфіденційності даних за допомогою асиметричного алгоритму RSA.
11. Основні вимоги щодо криптостійкості асиметричних криптосистем.

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №8

Тема: Протоколи автентифікації.

Мета: ознайомитись з алгоритмами гешувальння та способами застосування кодів цілісності даних в інформаційних системах.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Гешувальний алгоритм та його призначення.
2. Алгоритми формування кодів-гешування за допомогою безключових геш-функцій.
3. Коди цілісності даних (MDC-коди) та способи використання їх у сучасних інформаційних системах.
4. Коди автентичності даних (MAC-коди). Способи їх побудови.
5. Основні вимоги щодо алгоритмів гешування на міжнародних криптографічних конкурсах NESSIE та SHA-3.

6. Основні переваги алгоритмів-переможців міжнародних криптографічних конкурсів NESSIE та SHA-3.

7. Каскадні схеми гешування на основі використання геш-функцій на універсальних класах.

Література: [1-17].

САМОСТІЙНА РОБОТА №9

Тема. Технічні канали витоку інформації. Способи несанкціонова-ного зняття інформації з технічних каналів її витоку.

Мета: опанувати загальний підхід до технічного захисту інформації та ознайомитись із його організаційно-технічними заходами.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Основні джерела інформації, які входять до складу національних та міжнародних стандартів.
2. Технічний канал витоку інформації та його класифікація.
3. Небезпечний фізичний сигнал.
4. Природні та штучні технічні канали витоку інформації.
5. Що виступає основним об’єктом захисту інформації?
6. Фізична суть акустичного сигналу.
7. Що є частотою та періодом коливань?
8. Які частоти коливань відносяться до звукового, інфразвукового та ультразвукового діапазону частот?
9. Мікрофонний ефект та яка його фізична суть. Радіозв’язок.
10. Що відносять до комбінованих каналів витоку інформації?
11. Канали витоку акустичної інформації?
12. Види радіозакладних пристроїв.
13. Канали витоку електромагнітної та електронної інформації.
14. Способи та засобами зняття електромагнітної та електронної інформації.

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №10

Тема: Методи та засоби блокування технічних каналів витоку інформації.

Мета: ознайомитись із засобами та методами виявлення й блокування технічних каналів витоку інформації.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Об’єкт технічного захисту інформації.
2. Комплексний захист інформації.
3. Основні та допоміжні технічні засоби захисту інформації.
4. Активний та пасивний захист інформації.
5. Які фізичні явища покладено у методи та засоби захисту акустичної інформації від витоку по вібраційних каналах?
6. В чому полягає суть метод «завантаження мембрани», який використовують для придушення мікрофонів?
7. Які прилади використовують для захисту акустичної інформації, що циркулює у приміщенні, від зняття з телефону?
8. На що звертають увагу під час візуального пошуку радіозакладних пристроїв?
9. Які методи використовують для виявлення радіозакладних пристроїв?
10. Які функції виконують програми моніторингу ефіру, сканери та індикатори електромагнітного поля?
11. Який алгоритм виявлення радіозакладних пристроїв з використанням методу моніторингу ефіру?
12. Які функції виконують нелінійні локатори?
13. Які методи пошуку радіозакладних пристроїв, побудовано на використанні способу ВЧ-нав’язування?

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №11

Тема. Методи та пристрої забезпечення захисту і безпеки.

Мета: опанувати основні принципи захисту інформації при підключені до мережі Internet.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Основні принципи захисту інформації при підключенні до Internet.
2. Захист інформації в інформаційних системах за допомогою міжмережевих екранів.
3. Захист інформації на мережному рівні за допомогою протоколів TLS, SSL, IPSec.

4. Схема проходження IP-пакета даних з використанням протоколів безпеки AH і ESP в тунельному та транспортному режимі.

5. Забезпечення конфіденційності, цілісності та автентичності даних в IP-мережах з використанням протоколу ESP (IPSec).

6. Забезпечення безпеки даних в інформаційних системах за допомогою Log- та Proxy-сервера.

Рекомендована література: [2; 5-11; 14-17].

САМОСТІЙНА РОБОТА №12

Тема. Заходи щодо захисту інформації.

Мета: опанувати основні вимоги, які висуваються до системи захисту інформації та ознайомитись із організаційними й інженерно-технічними заходами її захисту.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Комплексна система захисту інформації.
2. Основні принципи та завдання, які висуваються до комплексної системи захисту інформації.
3. Визначення складу інформації, яку захищають.
4. Класифікація інформації із обмеженим доступом.
5. У чому полягає суть концепції інформаційної безпеки.
6. У чому суть організаційних та інженерно-технічних заходів щодо захисту інформації.
7. Суб'єкт та об'єкт комплексної системи захисту інформації.

Література: [1-17].

САМОСТІЙНА РОБОТА №13

Тема: Порядок здійснення захисту інформації на об'єктах інформаційної діяльності.

Мета: ознайомитись із етапами технічного захисту інформації та організацією розроблення системи її захисту.

Завдання: опрацювати матеріал та дати відповіді на запитання.

ЗАПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Технічний захист інформації та його етапи.

2. Поняття і структура загроз інформації, яку захищають.

3. Що варто віднести до явищ сутнісних проявів загрози?

4. За якими ознаками класифікуютьі захищувану інформацію?

5. На що звертають увагу під час обстеження об'єктів інформаційної діяльності?

6. Технічне завдання на розроблення системи захисту інформації.

Рекомендована література: [2; 5-11; 14-17].

III. Тестові завдання для самоконтролю опрацьованого матеріалу з курсу «Апаратні та програмні засоби захисту інформації»

1. У яких комп'ютерних системах лише уповноважені користувачі мають змогу читати та змінювати призначену для них інформацію?

A. Персональних.

B. Безпечних.

C. Мобільних

D. Мережевих.

E. Інформаційних.

2. Які принципи безпеки, за «Оранжевою книгою», задовольняє захищена система?

A. Політики та мітки безпеки.

B. Монітор звернень.

C. Відповідальність.

D. Ядро та гарантії безпеки.

E. Усі перераховані принципи безпеки.

3. Які елементарні сервіси безпеки визначає перша група функціональних вимог?

A. APE та ASE.

B. FAU; FIA та FRU.

C. ADV; ACM; ATE та ADO.

D. FCO; FPR; FDP та FPT.

E. FCS; FMT; FTA та FTP.

4. Який нормативний документ встановлює критерії оцінки захищеності інформації, яка обробляється комп'ютерними системами, від несанкціонованого доступу?

A. Evaluation criteria for IT security.

B. НД ТЗІ 2.5-004-99.

C. ДСТУ 3396.0-96.

D. Department of Defense Trusted Computer System Evaluation Criteria.

E. НД ТЗІ 3.6-001-2000.

5. Що являє собою потенційно можлива подія, дія/вплив, процес або явище, які можуть призвести до заподіяння шкоди будь-чиїм інтересам?

A. Атаку.

B. Криптоаналіз.

C. Загрозу.

D. Проникнення.

E. Самоствердження.

6. Як називають атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу?

A. Local penetration.

B. Password crackers.

C. Denial of service.

D. Man-in-the-Middle.

E. Remote penetration.

7. Якою буде криптографічна схема, коли зашифроване повідомлення не буде містити ніякої інформації про відкритий текст.

A. Захищена.

B. Персональна.

C. Мобільна.

D. Лояльна.

E. Безпечна.

8. Які засоби захисту базуються на використанні різних електронних пристроїв і спеціального програмного забезпечення, що входять до складу автоматизованої системи і виконують, самостійно або в комплексі з іншими засобами, функції захисту інформації?

A. Правові.

B. Морально-етичні.

C. Організаційні.

D. Фізичні.

E. Технічні.

9. Як називають спосіб захисту інформації, яка передбачає перетворення даних у форму, яка буде не придатною для сприйняття сторонніми особами?

A. Маскування.

B. Управління.

C. Примус.

D. Шифрування.

E. Обмеження доступу.

10. Яка кількість розділів, зазвичай, формує політику безпеки?

A. 4.

B. 6.

C. 7.

D. 9.

E. 10

11. Що відносять до основних видів загроз безпеки комп'ютерних систем та інформації?

A. Стихійні лиха та аварії.

B. Збої у роботі та аустаткування.

C. Наслідки помилок під час проектування/розробки компонентів та експлуатації комп'ютерних систем.

D. Навмисні дії порушників/зловмисників.

E. До основних видів загроз безпеки підходять усі зазначені варіанти відповідей.

12. Для яких блокових шифрів під час атаки застосовують лінійні наближення?

A. FEAL та DES.

B. REDOC та 3-WAY.

C. MMB та SKIPJACK.

D. CA-1.1 та CRAB.

E. NewDES та BLOWFISH.

13. Назвіть найбільш відомий алгоритмом симетричного шифрування:

A. RSA.

B. AES.

C. DES.

D. NIST.

E. FIPS.

14. Основною модифікацією DES прийнято вважати:

A. RSA EDE3.

B. 3DES.

C. AES EDE2.

D. FIPS PUB 46.

E. AES eXtended.

15. Який алгоритм являє собою 16-раундову сітку Фейстеля із довжиною блоку 64 біти та володіє ключем довжиною у 448 бітів?

A. ADE.

B. SAFER.

C. RSB-32.

D. IDEA.

E. Blowfish.

16. Що являє собою функція гешування?

A. Алгоритм стиснення інформаційного ресурсу.

B. Односторонню функцію стійкості інформаційного ресурсу.

C. Механізм забезпечення цілісності та автентичності інформаційного ресурсу.

D. Модифікований блоковий шифр.

E. Механізм автентифікації повідомлень із єдиним ключем

17. Вкажіть на ту вимогу, за якої геш-функція вважається криптографічно стійкою:

A. Незворотність або стійкість до відновлення прообразу.

B. Стійкість за прообразом, але нестійка за другим прообразом.

C. Відсутність кореляції.

D. Не захищеність відносно підбору до такого ж самого повідомлення з однаковим гешем.

E. Специфічна мета автентифікації повідомлення.

18. Для якого алгоритму притаманним є паралельне виконання однієї і тієї ж геш-функції із різними векторами ініціалізації?

A. HMACWhirlpool.

B. CBC MAC-Shacal.

C. TTMAC.

D. HMAC-SHA-0.

E. MD4.

19. Який алгоритм використовується протоколом автентифікації MSCHAP?

A. Message Digest 4.

B. Modification Detection Code.

C. Unique Block Iteration.

D. Keccak.

E. JH.

20. Як називають алгоритм стиснення, функція якого заснована на використанні ключової підстановки в конструкції Davies-Meyer?

A. BLAKE.

B. Gröstl.

C. JH.

D. Keccak.

E. Skein.

21. Як називають технічні канали витоку інформації, в основу яких покладено фізичні властивості джерел виникнення небезпечних сигналів?

A. Виявлені.

B. Прогнозовані.

C. Природні.

D. Штучні.

E. Тимчасові.

22. Як прийнято називати сигнал, у якому відбуваються механічні коливання часточок пружнього середовища?

A. Акустичний.

B. Гармонійним коливанням.

C. Паразитним.

D. Високочастотним.

E. Механічний.

23. Як називають технічні засоби, які застосовують для оброблення, зберігання та передавання закритої інформації?

A. Апаратними.

B. Програмними.

C. Спеціальними.

D. Основними.

E. Допомідними.

24. За допомогою чого реалізовують набір правил, які визначають умови проходження пакетів даних з відкритої комп'ютерної мережі в захищену?

A. Ethernet-портів.

B. Міжмережеві екрани.

C. Log-сервера.

D. Proxy-сервера.

E. Протоколом ESP (IPSec).

IV. Перелік питань, які виносяться на іспит з курсу «Апаратні та програмні засоби захисту інформації»

1. Основні поняття та структура інформаційної безпеки.
2. Нормативно-правове забезпечення інформаційної безпеки.
3. Класифікація методів і засобів захисту інформації.
4. Лінійний криптоаналіз.
5. Механізми і політики розмежування прав доступу.
6. Основні вимоги, які висуваються до сучасних криптосистем.
7. Блокові та потокові шифри.
8. Алгоритми сімейства SHA.
9. Фізичні основи утворення технічних каналів витоку інформації.
10. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами.
11. Захист інформації на мережному рівні.
12. Суб'єкт та об'єкт захисту інформації.
13. Етапи технічного захисту інформації.
14. Теоретичні основи інформаційної безпеки.
15. Інформаційна безпека як складова національної безпеки.
16. Методи та засоби захисту в інформаційній безпеці.
17. Механізми захисту від атак.
18. TCSEC. Common Criteria. НД ТЗІ 2.5-004-99.
19. Шифрування даних.
20. Стандарт DES. Основні модифікації DES та його основні режими роботи.
21. Гешувальні алгоритми: призначення та вимоги до них.
22. Загальний підхід до технічного захисту інформації.
23. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації.
24. Основні вимоги, які висуваються до системи захисту інформації.

25. Основні принципи захисту інформації при підключені до мережі Internet.

26. Реалізація первинних та основних технічних заходів захисту.

27. Принципи безпеки.

28. Концептуальні засади забезпечення інформаційної безпеки в Україні.

29. Захист інформації та його основні завдання.

30. Загрози інформаційної безпеки, основні види атак та принципи криптоаналізу.

31. Теорія зв'язку в секретних системах.

32. Алгоритми з секретним та відкритим ключами.

33. Алгоритми сімейства MD.

34. Основи несанкціонованого зняття інформації способом та засобами високочастотного нав'язування.

35. Захист інформації від несанкціонованого запису звукозаписувальними пристроями.

36. Захист інформації за допомогою міжмережних екранів.

37. Концептуальні підходи до проектування систем захисту.

38. Порядок здійснення захисту інформації на об'єктах інформаційної діяльності.

39. Структура політики безпеки та її основні частини.

40. Атаки на інформаційні системи.

41. Симетричні, асиметричні та комбіновані криптосистеми.

42. Алгоритм RSA.

43. Протоколи автентифікації.

44. Організаційно-технічні заходи щодо технічного захисту інформації на об'єкті.

45. Методи пошуку радіозакладних пристроїв. Захист електронної інформації.

46. Організація розроблення системи захисту інформації.

47. Методи та пристрої забезпечення захисту і безпеки.

48. Організаційні та інженерно-технічні заходи захисту інформації.

49. Інформація з обмеженим доступом.

50. Класифікація атак на симетричні та асиметричні криптоалгоритми.

51. Алгоритми криптографічних перетворень.

52. Технічний канал витоку інформації.

53. Методи та пристрої забезпечення захисту і безпеки.

54. Методика визначення складу інформації, яку захищають.

55. Способи несанкціонованого зняття інформації з технічних каналів її витоку.
56. Методи проведення атак на інформацію.
57. Диференціальний криптоаналіз.
58. Загальні положення технічного захисту інформації.
59. Застосування протоколів AH, ESP, SSL та TLS.
60. Захист акустичної інформації від зняття радіозакладними пристроями.
61. Життєвий цикл розробки систем безпеки.
62. Загрози інформаційної безпеки.
63. Алгоритм Ель-Гамаля.
64. Класифікація каналів витоку інформації.
65. Методи та засоби блокування технічних каналів витоку інформації.
66. Методи та пристрої забезпечення захисту і безпеки.
67. Реалізація організаційних заходів захисту.
68. Технічні канали витоку інформації.
69. Захист письмової інформації від оптичного зняття.
70. Заходи щодо захисту інформації.

V. Ключ відповідей для перевірки тестових завдань опрацьованого матеріалу з курсу «Апаратні та програмні засоби захисту інформації»

№ з/п	Вірна відповідь	№ з/п	Вірна відповідь	№ з/п	Вірна відповідь	№ з/п	Вірна відповідь
1	**B**	7	**E**	13	**C**	19	**A**
2	**E**	8	**E**	14	**B**	20	**A**
3	**B**	9	**A**	15	**E**	21	**C**
4	**B**	10	**D**	16	**C**	22	**A**
5	**C**	11	**E**	17	**A**	23	**D**
6	**E**	12	**A**	18	**E**	24	**B**

VI. Комплексне практичне індивідуальне завдання з курсу «Апаратні та програмні засоби захисту інформації»

Робочим навчальним планом освітньої програми «Інформаційні системи та технології охорони і безпеки» передбачено виконання здобувачами вищої освіти комплексного практичного індивідуального завдання (КПІЗ).

КПІЗ з курсу «Апаратні та програмні засоби захисту інформації» виконується упродовж семестру. Його виконання є обов'язковою умовою для успішного вивчення курсу та отримання позитивної оцінки.

Метою виконання індивідуального завдання є закріплення здобувачами вищої освіти необхідних знань, які пов'язані із забезпеченням єдності вимірювань, технічним регулюванням та якістю продукції.

Індивідуальне завдання захищається в кінці семестру. Під час виконання та оформленні індивідуального завдання студенту дозволено використовувати наявну базу службової документації, законодавчу базу та інтернет-ресурси.

Метою виконання КПІЗ є розвиток навичок самостійної роботи; систематизація знань; закріплення теоретичних знань та практичне застосування знань студента із навчального курсу; підготовлення логічно-структурної схеми його атестаційної роботи. У ході виконання КПІЗ та його оформленні здобувач використовує комп'ютерну техніку.

КПІЗ оцінюється максимальною кількістю балів та визначається, як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту.

Тематика КПІЗ із курсу «Апаратні та програмні засоби захисту інформації» є комплексною (одне завдання видається на групу з чотирьох здобувачів освіти) та визначається за номером першого з них по списку в групі. КПІЗ являє собою структуровану презентацію, яка виконують на 10 слайдах (перший слайд є титульним, а останній – завершальним).

Тематика КПІЗ:

1. Розроблення криптосистеми на основі шифру Цезаря.

   Розроблення алгоритму виявлення витоку інформації з обмеженим доступом технічними каналами за допомогою багатофункціональних пошукових приладів.

2. Розроблення криптосистеми на основі шифру Тритеміуса.

   Розроблення алгоритму виявлення витоку інформації через радіозакладні пристрої за допомогою багатофункціональних пошукових приладів та систем.

3. Розроблення криптосистеми на основі шифру гамування.

   Виявлення витоку інформації через телефонні радіоретранслятори за допомогою багатофункціональних пошукових приладів та систем.

4. Розроблення криптосистеми на основі шифру DES.

   Розроблення алгоритму локалізації витоку інформації через інфрачервоне випромінювання за допомогою багатофункціональних пошукових приладів та систем.

5. Розроблення асиметричної криптосистеми на основі задачі рюкзака з відкритим ключем.

   Розроблення алгоритму локалізації витоку інформації через

низькочастотні магнітні поля за допомогою багатофункціональних пошукових приладів та систем.

6. Розроблення асиметричної криптосистеми на основі алгоритму RSA з відкритим ключем.

Розроблення засобу ідентифікації користувачів в комп'ютерних системах.

ІНФОРМАЦІЙНІ ДЖЕРЕЛА

1. Вакалюк Т. А. Захист інформації в комп'ютерних системах. URL: http://eprints.zu.edu.ua/9650/1/1.pdf (дата звернення: 28.04.2025).
2. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Гапак О. М. Криптоаналіз. Криптографічні протоколи : навч. посіб. Ужгород : Вид-во ПП «АУТДОР-ШАРК», 2021.
4. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах : підруч. Ужгород : ДВНЗ «УжНУ», 2021. 184 с.
5. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
6. Гуз А. М. Організація захисту інформації з обмеженим доступом. URL: http://za.inf.ua/bo/oziod18.pdf (дата звернення: 28.04.2025).
7. Заплотинський Б. А. Основи інформаційної безпеки. URL: http://surl.li/pfkpnk (дата звернення: 28.04.2025).
8. Інформаційна безпека / за ред. Ю. Я. Бобала та І. В. Горбатого. URL: http://surl.li/iglfxk (дата звернення: 28.04.2025).
9. Інформаційна безпека : підруч. / за ред. В. Остроухова. К. : Вид-во Ліра-К, 2021. 412 с.
10. Інформаційна безпека в комп'ютерних мережах : навч. посіб. / за ред. О. А. Смірнов. Кропивницький : Видавець Лисенко В. Ф., 2020. 295 с.
11. Кавун С. В. Носов В. В. Манжай О. В. Інформаційна безпека : навч. посіб. URL: http://surl.li/ikprgx (дата звернення: 28.04.2025).
12. Комплексні системи захисту інформації. URL: http://surl.li/yptezr (дата звернення: 28.04.2025).
13. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO : навч. посіб. Львів : Вид-во Львівська політехніка, 2021. 232 с.
14. Лісовська Ю. Кібербезпека. Ризики та заходи. URL: http://surl.li/hrqcoh (дата звернення: 28.04.2025).
15. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека : сучасні технології захисту : навч. посіб. Львів : «Новий Світ-2000», 2020. 678 с.

16. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf (дата звернення: 28.04.2025).
17. Пількевич І. А., Лобанчикова Н. М., Молодецька К. В. Захист інформації в автоматизованих системах управління. URL: http://surl.li/znnide (дата звернення: 28.04.2025).

ДЛЯ НОТАТОК

Апаратні та програмні засоби захисту інформації: методичні вказівки до самостійної роботи для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький. Луцьк : ЛНТУ, 2025. 24 с.

Комп'ютерний набір та верстка: О. Л. Кайдик.

Редактор: в авторській редакції.

Підп. до друку «__» _____ 2025 р.
Формат 60х84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. 1,5. Обл. – вид. арк. 1,4.
Тираж _50_ прим. Зам. _____.

Луцький національний технічний університет
43018 м. Луцьк, вул. Львівська, 75