МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
"22" 09 2025 р.

ЗАТВЕРДЖУЮ
Директор навчально-наукового інституту інноваційних освітніх технологій
_____ Святослав ПИТЕЛЬ
"22" 09 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
"22" 09 2025 р.

РОБОЧА ПРОГРАМА
з дисципліни «Методи та засоби захисту програмного забезпечення»

ступінь вищої освіти: магістр
галузь знань – F «Інформаційні технології»
спеціальність – F2 «Інженерія програмного забезпечення»
освітньо-професійна програма – «Інженерія програмного забезпечення»

Кафедра комп'ютерних наук

Форма навчання	Курс	Семестр	Лекції (год.)	Прак. (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Екзамен (сем.)
денна	1	1	30	14	4	6	96	150	1
заочна	1	1	8	4	-	-	138	150	2

19.08.2025 р.

Тернопіль 2025

Робочу програму склав доцент кафедри комп'ютерних наук, к.т.н. Руслан ШЕВЧУК

Робоча програма затверджена на засіданні кафедри комп'ютерних наук, протокол №2 від «22» 09 2025 р.

Завідувач кафедри д.т.н, професор _____ Андрій ПУКАС

Гарант ОП
к.т.н., доцент

_____ Ірина СПІВАК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Методи та засоби захисту програмного забезпечення»

1. Опис дисципліни «Методи та засоби захисту програмного забезпечення»

Дисципліна «Методи та засоби захисту програмного забезпечення»	Галузь знань, спеціальність, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів : Денна - 5 Заочна - 5	Галузь знань - F «Інформаційні технології»	Статус дисципліни: вибіркова Мова навчання: українська
Кількість залікових модулів - 5	Спеціальність: F2 «Інженерія програмного забезпечення»	Рік підготовки: *Денна – 1* *Заочна - 1* Семестр: *Денна – 1* *Заочна – 1*
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції: *Денна* – 30 год, *Заочна* – 8 год. Практичні заняття: *Денна* – 14 год, *Заочна* – 4 год.
Загальна кількість годин: Денна – 150 Заочна – 150		Самостійна робота: *Денна* – 96 год, тренінг – 6 год., *Заочна* – 138 год. Індивідуальна робота: *Денна* – 4 год.
Тижневих годин: Денна форма навчання – 10 год., з них аудиторних 3 год. (лекційних – 2 год., практичних – 1 год.)		Вид підсумкового контролю – екзамен

2. Мета і завдання вивчення дисципліни «Методи та засоби захисту програмного забезпечення»

2.1. Мета вивчення дисципліни

Метою курсу „Методи та засоби захисту програмного забезпечення” є вивчення студентами методологічних та методичних питань щодо дослідження вразливостей та захисту програмного забезпечення, набуття спеціальних знань і практичних навиків застосування методів та засобів побудови ефективних систем захисту програмного забезпечення. Курс "Методи та засоби захисту ПЗ" охоплює теоретичні та практичні основи роботи з методами та засобами дослідження вразливостей та захисту програмного забезпечення. Названий курс повинен сприяти формуванню висококваліфікованих фахівців в галузі знань «Інформатика та обчислювальна техніка».

Оволодіння цим курсом повинне виробити у студентів навички практичного використання сучасних методів захисту програмного забезпечення.

Вивчення курсу "Методи та засоби захисту програмного забезпечення" передбачає наявність систематичних та ґрунтовних знань із суміжних курсів (безпека програм та даних, дискретна математика, основи програмування і алгоритмічні мови, основи програмування, організація комп'ютерних мереж, програмування інтернет, операційні системи, якість програмного забезпечення та тестування, технологія NET), цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях, практичних та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

2.2. Завдання вивчення дисципліни

У результаті вивчення курсу "Методи та засоби захисту програмного забезпечення" студенти повинні знати:

- сучасні методи захисту ПЗ;
- модель SSDLC;
- вимоги безпеки для програмного забезпечення;
- методи та засоби обмеження доступу до програмного забезпечення;
- класифікацію вразливостей ПЗ;
- особливості вразливостей у ПЗ;
- особливості конфігурування систем безпеки.

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними відомостями щодо аналізу та дослідження вразливостей програмного забезпечення та використання сучасних методів та засобів для захисту програмного забезпечення від потенційних загроз.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних понять щодо захисту програмного забезпечення;
- сформувати у студентів цілісну систему теоретичних знань з курсу "Методи та засоби захисту програмного забезпечення".

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички розробки програмного забезпечення відповідно до моделі SSDLC.

Завдання проведення практичних занять:

- ознайомити з найбільш поширеними вразливостями програмного забезпечення відповідно до TOP 10 OWASP;
- отримати навики аналізу та дослідження вразливостей програмного забезпечення за допомогою сучасних програних засобів;
- отримати практичні навики розробки захищеного програмного забезпечення відповідно до моделі SSDLC.
- ознайомитись з сучасними методами та засобами захисту програм;
- глибше засвоїти та закріпити теоретичні знання, одержані на лекціях.

3. Програма навчальної дисципліни «МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»

Змістовний модуль 1. Особливості захисту програмного забезпечення

Тема 1. ЗАГАЛЬНИЙ ОГЛЯД МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ПЗ

Мета і доцільність використання систем захисту ПЗ. Класифікація систем захисту ПЗ. Основні методи захисту ПЗ. Критерії оцінювання та основні вимоги до розробки СЗПЗ.

Література: 9-15

ТЕМА 2. МОДЕЛЬ SSDLC.

Вимоги безпеки для розробки ПЗ. Особливості дизайну захищеного ПЗ. Реалізація захищеного ПЗ. Особливості тестування безпеки ПЗ. Експлуатація захищеного ПЗ.

Література: 1-6, 13,14

ТЕМА 3. НЕФУНКЦІОНАЛЬНІ ВИМОГИ БЕЗПЕКИ ДЛЯ РОЗРОБКИ ПЗ

Вимоги автентифікації. Вимоги до паролів. Вимоги до авторизації Вимоги до Cookies та Timeouts. Вимоги до сесій користувачів. Вимоги до введення \ виведення. Вимоги до логування

Література: 6, 9-12

Тема 4. ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО ДОСЛІДЖЕННЯ

Методи дослідження програмного коду. Засоби дослідження програмного коду. Принципи та підходи щодо захисту програмного коду від несанкціонованого дослідження.

Література: 13,14

Змістовний модуль 2. Особливості аналізу та дослідження вразливостей програмного забезпечення.

Тема 5. КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

OWASP TOP 10. Web Application Security Consortium Threat Classification. OWASP Top 10 Mobile Risks. Common Vulnerabilities Scoring System.

Література: 2,3

Тема 6. ЗАСОБИ АУДИТУ БЕЗПЕКИ ТА АНАЛІЗУ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Засоби аудиту безпеки web-додатків. Засоби виявлення вразливостей програмного забезпечення. Особливості конфігурування систем безпеки web-додатків.

Література: 2-7

4. Структура залікового кредиту дисципліни „Методи та засоби захисту програмного забезпечення”

денна форма навчання \ заочна форма навчання	Кількість годин				
	Лекції	Практичні роботи	Самостійна робота	Індивідуальна робота	Контрольні заходи
Змістовий модуль 1. Особливості захисту програмного забезпечення					
Тема 1. Загальний огляд методів та засобів захисту ПЗ	4 \ 1	3	16 \ 23	-	Усне опитування та тестування
Тема 2. Модель SSDLC	6 \ 2	3 \ 2	18 \ 23	2	Усне опитування та тестування
Тема 3. Нефункціональні вимоги безпеки для розробки ПЗ	4 \ 2	2 \ 2	16 \ 23	-	Усне опитування та тестування
Тема 4. Захист програмного забезпечення від несанкціонованого дослідження	4 \1	2	16 \ 23	-	Усне опитування та тестування
Змістовий модуль 2. Особливості аналізу та дослідження вразливостей програмного забезпечення.					
Тема 5. Класифікація вразливостей програмного забезпечення	6 \ 1	2	16 \ 23	-	Усне опитування та тестування
Тема 6. Засоби аудиту безпеки та аналізу захищеності програмного забезпечення	6 \ 1	2	14 \ 23	2	Усне опитування та тестування
Разом	30 \ 8	14 \ 4	96 \ 138	4	

5. Тематика практичних занять

Практичне заняття № 1

Тема: Вразливості та вектори атак на веб-застосунки відповідного до TOP 10 OWASP.

Мета: Отримати практичний досвід експлуатації вразливостей веб-застосунків у середовищі bWAPP.

Контрольні запитання:

1. Яку вразливість із OWASP Top 10 ви виявили в bWAPP і як її експлуатували?
2. Які кроки захисту потрібно застосувати, щоб запобігти цій вразливості?
3. Який вектор атаки використовувався та які наслідки експлуатації?

Практичне заняття № 2
Тема: Аналіз захищеності веб-базованого програмного забезпечення
Мета: Вивчення методів та засобів збору інформації про захист веб – ресурсів.
Контрольні запитання:
1. Які інструменти збору інформації про веб-ресурс ви використали?
2. Які потенційні вразливості або витоки інформації були виявлені?
3. Які заходи можна застосувати для зменшення виявлених ризиків?

Практичне заняття №3
Тема: Автоматичний аналіз вразливостей програмного забезпечення.
Мета: Формування вмінь і практичних навиків оцінки вразливостей ПЗ відповідно до CVSS з допомогою сканера OpenVAS.
Контрольні запитання:
1. Які основні вразливості були виявлені за допомогою OpenVAS?
2. Як визначається рівень критичності вразливостей за CVSS?
3. Які дії потрібно виконати для усунення найкритичніших вразливостей?

Практичне заняття №4
Тема: Формування вимог до захищеного програмного забезпечення відповідно до SSDLC.
Мета: Отримати практичний досвід формування нефункціональних вимог безпеки до програмного забезпечення.
Контрольні запитання:
1. Які нефункціональні вимоги безпеки потрібно враховувати при розробці ПЗ?
2. Як вимоги безпеки впливають на архітектуру програмного забезпечення?
3. Які критерії перевірки виконання вимог безпеки ви можете запропонувати?

Практичне заняття №5
Тема: Розробка прототипу захищеного програмного забезпечення відповідно до SSDLC.
Мета: Розробити архітектуру програмне забезпечення відповідно до SSDLC.
Контрольні запитання:
1. Які архітектурні рішення забезпечують безпеку прототипу ПЗ?
2. Які компоненти відповідають за автентифікацію, авторизацію та аудит дій користувачів?
3. Які загрози враховано під час проектування та які заходи протидії застосовано?

Практичне заняття №6
Тема: Реалізація захищеного програмного забезпечення відповідно до SSDLC.
Мета: Реалізувати програмне забезпечення відповідно до SSDLC.
Контрольні запитання:

1. Які механізми реалізовано для забезпечення захисту програмного забезпечення?
2. Як проводилась перевірка виконання вимог безпеки під час реалізації?
3. Які недоліки залишились після впровадження та як їх планується усунути?

6. Самостійна робота

Мета самостійної роботи - поглибити знання з аналізу захищеності програмного забезпечення, сформувати практичні навички використання інструментів тестування безпеки та розробки рекомендацій щодо усунення вразливостей.

Результатом виконання кожного завдання є підготовка короткої презентації (7–10 слайдів), у якій студент демонструє теоретичне обґрунтування теми, інструменти та методи, приклади практичного застосування, висновки й пропозиції.

№ п/п	Тематика	К-сть годин (денна)	К-сть годин (заочна)
1	Тестування захищеності механізму управління сесіями	8	12
2	Тестування захищеності транспортного рівня	8	10
3	Аналіз протекторів	8	12
4	Пошук вразливостей до атак CSRF	8	12
5	Пошук вразливостей до атак XSS	8	12
6	Пошук вразливостей до атак RCE	8	10
7	Аналіз Metasploit Framework	8	12
8	Середовище тестування захищеності веб-додатків Burp Suite	8	12
9	Аналіз спеціалізованих сканерів вразливостей веб- застосунків	10	12
10	Особливості програмної реалізація криптографічних алгоритмів	8	10
11	Методи безпечної реалізації ПЗ	8	12
12	Безпечна конфігурація БД	6	12
Разом:		**96**	**138**

7. Тренінг з дисципліни

Тематика: Проведення CTF (Capture The Flag) на тематику захисту/атаки на програмного забезпечення.

Завдання та структура: У контексті на атаку/захист (Attack-Defence, атака-захист, напад-захист) кожна команда отримує власну мережу (або лише один хост) з vulnarable services. Зазвичай команди мають час для патчення своїх сервісів та розробки експлойтів. А тоді викладач з'єднує учасників змагань — і починається бойова гра! Необхідно захистити власні сервіси у точках захисту (пунктах оборони) та хакнути опонентів у точках атаки. Залежно від характеру конкретної гри команди можуть намагатися захопити прапор суперника або підсадити свій прапор на машину супротивника.

8. Засоби оцінювання та методи демонстрування результатів навчання

В процесі вивчення дисципліни «Безпека інформаційних систем» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування та тестування;
- презентації результатів виконання лабораторних завдань;
- оцінювання результатів модульних контрольних робіт;
- оцінювання результатів роботи під час проведення тренінгів;
- оцінювання результатів самостійної роботи студентів;
- підсумковий екзамен.

9. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об’єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальної шкалою) з дисципліни «Безпека інформаційних систем» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10 %	10%	5 %	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінг	Самостійна робота	Екзамен
Виконання практичних робіт 1-3 (середня арифметична оцінка, 60 балів)	Тестування в системі Moodle, 40 балів	Виконання практичних робіт 4-6 (середня арифметична оцінка, 60 балів)	Тестування в системі Moodle, 40 балів	Виконання завдань під час тренінгу – 100 балів	Підготовка презентації, 100 балів	Завдання по теорії (2 теоретичних питання по 30 балів – 60 балів) Практичний кейс (40 балів)

Виконання практичних робіт (поточне оцінювання)

90–100 балів: Здобувач глибоко розуміє принципи та методи захисту програмного забезпечення, самостійно виконує практичні завдання (№1–6), демонструючи знання з виявлення та експлуатації вразливостей OWASP Top 10, аналізу безпеки веб-додатків, використання сканерів OpenVAS, формування вимог SSDLC, проєктування та реалізації захищеного ПЗ. Аргументовано обирає методи і засоби захисту, створює чіткий, логічно структурований і технічно грамотний звіт із практичними рекомендаціями. Повністю дотримується академічної доброчесності, етичних норм і вимог до оформлення.

75–89 балів: Здобувач загалом правильно виконує практичні роботи, застосовує методи та засоби захисту ПЗ з незначними неточностями або частковими недоліками у звіті. Демонструє достатній рівень розуміння принципів безпеки, але потребує уточнень у деяких аспектах реалізації. Етичних норм дотримано.

60–74 бали: Здобувач володіє базовими підходами до захисту ПЗ, виконує практичні роботи переважно за інструкцією, проявляє обмежену самостійність. Звіт мінімально достатній, містить загальні висновки без глибокого аналізу. Етичних норм дотримано загалом.

1–59 балів: Здобувач має фрагментарне розуміння основ захисту ПЗ, виконав практичну роботу частково або з грубими помилками, звіт неповний або формальний. Можливі порушення етичних норм.

Модульний контроль 1 (тестування)

Модульний контроль проводиться у формі тестування з теоретичних і практичних аспектів захисту інформації з матеріалу з 1-4 теми. Тест містить 25 запитань, кожна правильна відповідь оцінюється у 4 бали. Максимальна кількість балів — 100.

Модульний контроль 2 (тестування)

Другий модульний контроль проводиться у форматі тестування з матеріалу 5-6 теми. Тест містить 25 запитань, кожна правильна відповідь оцінюється у 4 бали. Максимальна кількість балів — 100.

Тренінг

90–100 балів: Здобувач самостійно і без помилок виконав усі завдання тренінгу відповідно до ролі в команді, продемонстрував уміння практично застосовувати методи безпечної розробки, аналізу вразливостей і тестування захищеності програмних систем. Пропонує власні ідеї щодо покращення безпеки, грамотно документує результати; етичних норм дотримано повністю.

75–89 балів: Здобувач виконав завдання тренінгу з кількома незначними помилками, які не вплинули на кінцевий результат. Продемонстрував розуміння процесів захисту ПЗ, але потребував консультацій. Етичних норм дотримано.

60–74 бали: Здобувач виконав завдання частково або з помітними помилками, не завжди правильно інтерпретував поставлені завдання, продемонстрував поверхневе розуміння процесів безпечної розробки. Етичних норм дотримано загалом.

1–59 балів: Здобувач не виконав завдання або результати некоректні. Не продемонстрував базових навичок використання засобів захисту ПЗ. Можливі порушення етичних норм.

Самостійна робота

90–100 балів: Здобувач самостійно виконав усі завдання, продемонстрував креативний підхід до реалізації захисних механізмів, правильно задокументував результати, вільно користується інструментами інформаційної безпеки. Етичних норм дотримано повністю.

75–89 балів: Завдання виконано в цілому правильно, допущено незначні помилки або неточності, що не вплинули на результат (наприклад, нечіткість у схемі чи звіті). Під час виконання виникали питання; етичних норм дотримано.

60–74 бали: Завдання виконані частково або з суттєвими помилками, розуміння матеріалу поверхневе. Демонструється базовий рівень володіння інструментами безпеки. Етичних норм дотримано загалом.

1–59 балів: Здобувач не виконав завдання або результати повністю невірні; відсутні базові навички роботи з програмними засобами захисту; можливі порушення етичних норм.

Екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу. Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитання, за кожне з яких можна отримати від 0 до 30 балів, що в підсумку дає максимально 60 балів. За відповідь на питання здобувач отримує 16–30 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на

питання білету і 1–15 балів – якщо володіє навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить практичне завдання за виконання якого можна отримати від 0 до 40 балів. За виконання та відповідь здобувач отримує 16–40 балів, якщо самостійно і у повному обсязі виконав практичний кейс та аргументовано відповідає на питання і 0–15 балів – якщо практичне завдання виконав не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Шкала оцінювання:

За шкалою Університету	За національною шкалою	За шкалою ECTS
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Електронний варіант лекцій	1-6
2.	Вихідні дані для виконання практичних занять.	1-6
3.	Програмне забезпечення • bWAPP - навчальне середовище з вразливостями; • Burp Suite Community Edition - для перехоплення та модифікації HTTP-запитів; • OWASP ZAP Proxy - для аналізу вразливостей веб-додатків; • Firefox / Chrome із розширенням FoxyProxy - для зручного перемикання між проксі;	1-6

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Baker, M. (2022). *Secure Web Application Development: A hands-on guide with Python and Django*. Apress.
2. Fisher, D. (2022). *Application Security Program Handbook*.
3. Sahu, S. K. (2024). *Building Secure PHP Applications: A comprehensive guide to protecting your web applications from threats*.

4. Saikali, A., & Spilcă, L. (2025). *Software Security for Developers*.
5. Hoffman, A. (2023). *Web Application Security, 2nd Ed.: Exploitation and countermeasures for modern web applications*.
6. Закон України від 15 грудня 2005 року № 3200-IV "Про основи національної безпеки України".
7. Закон України "Про інформацію". Із змінами, внесеними згідно із Законом від 07.02.2002 № 3047-III-ВР.
8. Закон України "Про Національну програму інформатизації" Із змінами, внесеними згідно із Законом від 13.09.2001 № 2684-III-ВР.
9. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» від 31.05.2005 № 2594-IV. 5. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IX.
10. Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 № 851-IV.
11. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.
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 спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50).
13. ДСТУ ETSI TS 101 456:2015 Електронні підписи та інфраструктура (ESI). Вимоги до політики органів сертифікації, які видають кваліфіковані сертифікати (ETSI TS 101 456:2007, IDT). 10. ДСТУ ISO/IEC 13888-1:2015 Інформаційні технології. Методи захисту. Неспростовність. Частина 1: Загальні положення (ISO/IEC 13888 1:2009, IDT). 11. ДСТУ ISO/IEC 13888-3:2015 Інформаційні технології. Методи захисту. Неспростовність. Частина
14. ДСТУ ISO/IEC 18033-2:2015 Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри (ISO/IEC 18033-2:2006, IDT).