

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра програмної інженерії та інформаційних технологій управління
(назва)

ПАКЕТ КОМПЛЕКСНИХ КОНТРОЛЬНИХ РОБІТ (ККР) ДЛЯ
ПЕРЕВІРКИ ЗНАНЬ З ДИСЦИПЛІНИ

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

(назва навчальної дисципліни)

рівень вищої освіти перший (бакалаврський)
перший (бакалаврський) / другий (магістерський)

галузь знань 12 Інформаційні технології
(шифр і назва)

спеціальність 126 Інформаційні системи та технології
(шифр і назва)

вид дисципліни професійна підготовка
(загальна підготовка / професійна підготовка)

форма навчання денна
(денна / заочна)

Укладач Євсєєв Сергій Петрович, доцент
(прізвище, посада)

Харків – 2017 рік

ПОЯСНЮВАЛЬНА ЗАПИСКА

Мета контрольних завдань - перевірити ступінь сформованості у майбутніх фахівців принципів побудови комплексних систем захисту інформації, дослідження та використання сучасних процедур забезпечення надання основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Контрольні завдання вимагають від студента творчого підходу, креативності, спонукають до пошукової діяльності. Вони орієнтовані на те, що слухачі повинні продемонструвати:

- Здатність застосовувати знання у практичних ситуаціях.
- Знання та розуміння предметної області та розуміння професійної діяльності.
- Здатність вчитися і оволодівати сучасними знаннями.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

Перелік контрольних питань для перевірки теоретичних знань, умінь та навичок додається. Вони складені на підставі навчальної програми професійної дисципліни «БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ» та робочого навчального плану підготовки фахівців освітньо-кваліфікаційного рівня „бакалавр” за спеціальністю 126 Інформаційні системи та технології у галузі знань 12 «Інформаційні технології».

Тривалість виконання контрольних завдань - 2 години

НАВЧАЛЬНА ПРОГРАМА НОРМАТИВНОЇ ДИСЦИПЛІНИ

Модуль 1. Безпека та захист даних

Тема 1. Категорії інформаційної безпеки. Основні визначення і поняття теорії захисту інформації. Технічний та програмний захист інформації. Історія розвитку. Сфера застосування. Термінологія.

Тема 2. Визначення політики безпеки. Абстрактні моделі захисту інформації. Абстрактні моделі та формальні моделі захисту інформації. Особливості моделей Белла-Ла Падую та Біба.

Тема 3. Законодавча база в галузі захисту інформації Закони України “Про інформацію”, “Про захист інформації в автоматизованих системах”. Вимоги вітчизняних стандартів захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах. Зарубіжна нормативна база в галузі технічного захисту інформації. “Оранжева книга” безпеки. Критерії, вимоги та категорії систем безпеки “Оранжевої книги”.

Література: основна [1 – 4]; додаткова [5 – 10].

Модуль 2. Основи побудови систем захисту інформації в ПЗ

Тема 4. Класи безпеки. Критерії інформаційної безпеки. Канали витоку інформації. Класи безпеки інформації та інформаційних систем. Класифікація систем за критеріями інформаційної безпеки. Вимоги стосовно роботи з конфіденційною інформацією. Створення політики інформаційної безпеки. Електромагнітні та електричні канали витоку інформації. Параметричні канали витоку інформації.

Тема 5. Класифікація криптоалгоритмів Тайнопис, криптографія з ключем. Симетричні та асиметричні криптоалгоритми.

Тема 6. Системи шифрування даних, які передаються в мережах Канальне шифрування. Абонементне шифрування

Література: основна [1 – 4]; додаткова [5 – 10].

КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ ТА ВМІНЬ СТУДЕНТІВ

Рівень досягнень/Marks			Критерії оцінювання/Evaluation criteria		
Національна оцінка National grad		Бали Local grad	Оцінка за шкалою ЄКТС ECTS grad	позитивні/positiv	негативні/negativ
<u>Відмінно</u> Excelient	5	95-100	A	Глибоке знання навчального матеріалу, що містяться в основних і додаткових літературних; Вміння аналізувати явища, які вивчаються в їхньому взаємозв'язку і розвитку; Вміння проводити теоретичні розрахунки; Відповіді на запитання чіткі, лаконічні, логічно послідовні; Вміння застосовувати теоретичні положення під час розв'язання складних практичних задач.	
<u>Відмінно</u> Excelient	5	90-94	B	Глибокий рівень знань в обсязі обов'язкового матеріалу, що передбачений модулем; Вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; Вміння вирішувати складні практичні задачі.	Відповіді на запитання містять незначні неточності.
<u>Добре</u> Good	4	85-89	B	Глибокий рівень знань в обсязі обов'язкового матеріалу, що передбачений модулем; Вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; Вміння вирішувати складні практичні задачі.	Відповіді на запитання містять певні неточності.
<u>Добре</u> Good	4	75-84	C	Міцні знання матеріалу, що вивчається, та його практичного застосування; Вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; Вміння вирішувати практичні задачі.	Невміння використовувати теоритичні знання для вирішення складних практичних задач.
<u>Задовільно</u> Satisfactory	3	65-74	D	Знання основних фундаментальних положень матеріалу, що вивчається, та їх практичного застосування; Вміння вирішувати прості практичні задачі.	Невміння давати аргументовані відповіді на запитання; Невміння аналізувати викладений матеріал і виконувати розрахунки; Невміння вирішувати складні практичні задачі.

<u>Задовільно</u> Satisfactory	3	60-64	E	Знання основних фундаментальних положень матеріалу модуля; Вміння вирішувати найпростіші практичні задачі.	Незнання окремих (непринципових) питань з матеріалу модуля; Невміння послідовно і аргументовано висловлювати думку; Невміння застосовувати теоретичні положення при розв'язанні практичних задач.
<u>Незадовільно</u> Fail	2	35-59	FX	Додаткове вивчення матеріалу модуля може бути виконане в терміни, що передбачені навчальним планом.	Незнання основних фундаментальних положень навчального матеріалу модуля; Істотні помилки у відповідях на запитання; Невміння розв'язувати прості практичні задачі.
<u>Незадовільно</u> Fail	2	<35	F		Повна відсутність знань значної частини навчального матеріалу модуля; Істотні помилки у відповідях на запитання; Незнання основних фундаментальних положень; Невміння орієнтуватися під час розв'язання простих практичних задач.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 1.

1. Поняття інформаційної безпеки. Основні складові.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 7$, $q = 11$, $e = 43$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 2.

1. Основні визначення та класифікація загроз.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 5$, $q = 19$, $e = 29$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 3.

1. Екранування, аналіз захищеності.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 7$, $q = 11$, $e = 37$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 4.

1. Стандарти та специфікації в області інформаційної безпеки.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 5$, $q = 19$, $e=23$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 5.

1. Адміністративний рівень інформаційної безпеки.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 13$, $q = 11$, $e = 37$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 6.

1. Управління ризиками в інформаційній безпеці.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 5$, $q = 19$, $e=13$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 7.

1. Процедурний рівень інформаційної безпеки.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 5$, $q = 19$, $e = 7$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 8.

1. Основні поняття програмно-технічного рівня інформаційної безпеки.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 7$, $q = 13$, $e = 5$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 9.

1. Ідентифікація та автентифікація. Управління доступом.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 5$, $q = 17$, $e=7$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

рівень вищої освіти перший (бакалаврський)

галузь знань 12 Інформаційні технології

спеціальність 126 Інформаційні системи та технології

Навчальна дисципліна БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

КОМПЛЕКСНА КОНТРОЛЬНА РОБОТА № 10.

1. Протоколювання та аудит, шифрування, контроль цілісності.
2. Симетричні криптосистеми. Алгоритм DES. Необхідно зашифрувати перші вісім літер прізвища, імені та по батькові студента в латинській транслітерації за допомогою алгоритму DES. В якості пароля взяти слово «password». Для зменшення кількості обчислень в алгоритмі DES слід обмежитись лише одним раундом.
3. Асиметричні криптосистеми. Алгоритм RSA. Необхідно зашифрувати перші чотири літери прізвища, імені та по батькові студента (латиницею) за допомогою алгоритму RSA для передачі абоненту В. Параметри алгоритму RSA: $p = 7$, $q = 13$, $e = 23$. Необхідно також обчислити закритий ключ і розшифрувати шифротекст.

Затверджено на засіданні Кафедри програмної інженерії та інформаційних технологій управління

Протокол № _____ від „_____” _____ 20____ року

Завідувач кафедри _____ Годлевський М.Д.

Укладач _____ Євсєєв С.П.

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Євсєєв С.П. Лабораторний практикум з дисципліни “Технології захисту інформації” [Електронний ресурс]. – Режим доступу: ntumoodle.com

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.
2. Кузнецов О. О. Захист інформації в інформаційних систе-мах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.
3. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
4. Хорошко В. А. Методы и средства защиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Допоміжна література

5. Ленков С.В. Методы и средства защиты информации. В 2-х томах/ С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.– К.: Арий, 2008. – Т.ІІ. Информационная безопасность. – 344 с.
6. Мао Венбо Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2005. – 768 с.
7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. / А. А. Петров– М.: ДМК, 2000. – 448 с.
8. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМІТ”, 2006. – Т.1. – 292 с.
9. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМІТ”, 2006. – Т.2. – 252 с.
10. Чмора А.Л. Современная прикладная криптография. / А. Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

11. <http://bezopasnost.biz>.

12. <http://dstszi.gov.ua>.
13. [http:// securitylab.ru](http://securitylab.ru)
14. [http:// pgpi.org](http://pgpi.org)
15. [http:// citmgu.ru](http://citmgu.ru)