**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ**

**"ЗАТВЕРДЖУЮ"**
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
М. В. Афанасьєв

# ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ

**робоча програма навчальної дисципліни**

| | |
|---|---|
| Галузь знань | **12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"** |
| Спеціальність | **125 "КІБЕРБЕЗПЕКА"** |
| Освітній рівень | **перший (бакалаврський)** |
| Освітня програма | **"КІБЕРБЕЗПЕКА"** |

| | |
|---|---|
| Вид дисципліни | **базова** |
| Мова викладання, навчання та оцінювання | **українська** |

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

**Харків**
**ХНЕУ ім. С. Кузнеця**
**2019**

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 1 від 26.08.2019 р.

Розробник(-и):
Євсеєв С.П, д.т.н., с.н.с., завідувач кафедри КІТ
Алексієв В. О., д. т. н., проф. кафедри КІТ
Мілов О.В., к.т.н., доц. кафедри КІТ

**Лист оновлення та перезатвердження**
**робочої програми навчальної дисципліни**

| Навчальний рік | Дата засідання кафедри – розробника РПНД | Номер протоколу | Підпис завідувача кафедри |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 1. Вступ

**Анотація навчальної дисципліни:**

«Основи криптографічного захисту» є забезпечення підготовки бакалаврів відповідно до вимог і навчального плану спеціальності «кібербезпека», ознайомлення студентів з основами теорії двійкового кодування, алгоритмами стиснення, завадостійкого кодування. Дисципліна «Основи криптографічного захисту» розглядається як теоретична і прикладна дисципліна, що дає уявлення про основні математичні підрахунки і алгоритмічних підходах, що застосовуються для зберігання, передачі, виправлення інформації, представленої в довічних кодах. Дисципліна присвячена вивченню основ криптографії та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах, яких навчають, знайомляться з поняттям шифрів, симетричною і асиметричною криптографії, електронним підписом, гешуванням і іншими математичними об'єктами криптографії. Вивчаються відповідні криптографічні стандарти, що застосовуються сьогодні в захисті інформації в Росії і за кордоном. Докладно розглядаються: стандарти RSA. DES. GOST1989. та інші. Також приділено увагу перспективним напрямам в криптографії: криптографічні протоколи з розголошенням і без розголошення, теорія алгоритмічної складності і односторонніх функцій, схеми поділу секрету і деякі їх застосування в задачах ідентифікації і аутентифікації

**Мета навчальної дисципліни:**

- ознайомлення з основами математичної теорії криптології:
- придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації:
- розуміння суті інформаційних процесів в криптографічних системах;
- застосування комп'ютерів для вирішення завдань шифрування і дешифрування:
- розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

| | | |
|---|---|---|
| Курс | **3** | |
| Семестр | **1** | |
| Кількість кредитів ECTS | **5** | |
| Аудиторні навчальні заняття | **лекції** | **32** |
| | **лабораторні** | **32** |
| Самостійна робота | | **86** |
| Форма підсумкового контролю | **іспит** | |

**Структурно-логічна схема вивчення навчальної дисципліни:**

| Попередні дисципліни | Наступні дисципліни |
|---|---|
| Математичний аналіз<br>Лінійна алгебра<br>Математичне моделювання<br>Теорія ризику<br>Теорія ймовірностей і математична статистика<br>Дискретна математика<br>Основи теорії систем та системний аналіз;<br>Теорія інформації та кодування<br>Інформатика<br>Програмування<br>Менеджмент інформаційної безпеки | Основи інформаційної безпеки<br>Теорія прийняття рішень;<br>Проектування захищених телекомунікаційних систем<br>Програмно-апаратні засоби забезпечення інформаційної безпеки<br>Системи аналізу захищеності<br>Технічний захист інформації<br>Забезпечення інформаційної безпеки |

**2. Компетентності та результати навчання за дисципліною:**

| Компетентності | Результати навчання |
|---|---|
| здатністю застосовувати відповідний математичний апарат для вирішення професійних завдань | Знати: моделі шифрів і математичні методи їх дослідження<br>Вміти: застосовувати математичні методи опису і дослідження криптографічних систем<br>Володіти: навичками математичного моделювання в криптографії. |
| здатністю здійснювати раціональний вибір засобів забезпечення інформаційної безпеки телекомунікаційних систем з урахуванням пред'явлених до них вимог якості обслуговування і якості функціонування | Знати:<br>основні завдання та поняття криптографічних методів захисту інформації;<br>основні криптографічні методи захисту інформації;<br>вимоги до шифрів і основні характеристики шифрів<br>вміти:<br>здійснювати раціональний вибір криптографічних методів і засобів захисту інформації в телекомунікаційних системах;<br>реалізовувати типові криптографічні перетворення;<br>володіти:<br>навичками використання типових криптографічних перетворень;<br>навичками застосування інженерно-криптографічних механізмів для виявлення несправностей криптографічних засобів захисту інформації |

**3. Програма навчальної дисципліни**

**Змістовий модуль 1. Традиційне шифрування**

**Тема 1.** Вступ до криптографічних методів захисту. Порушення, механізми і служби захисту (пасивні та активні порушення). Сервісні служби захисту. Приватна

власність, аутентифікація, цілісність, управління доступом, доступність. Модель захисту мережі.

**Тема 2.** Традиційне шифрування: класичні методи. Криптографія, криптоаналіз, стеганографія. Класична техніка шифрування. Застосування підстановок. Застосування перестановок. Барабанні шифрувальні машини.

**Тема 3.** Традиційне шифрування: сучасні методи. Спрощений DES. Принципи блочного шифрування. Потокові і блокові шифри. Передумови створення шифру Файстеля. Шифр Файстеля. Стандарт шифрування даних (DES). Шифрування DES. Дешифрування DES. Надійність DES.

**Тема 4.** Диференціальний і лінійний криптоаналіз. Принципи побудови блокових шифрів. Критерії, що лежать в основі конструкції DES. Число раундів шифрування. Алгоритм обчислення ключів. Режими роботи блокових шифрів. Режим електронної шифрувальної книги. Режим зчеплення шифрованих блоків. Режим шифрованого зворотного зв'язку. Режим зворотного зв'язку по виходу

**Тема 5.** Традиційне шифрування: алгоритми. "Потрійний" DES. "Подвійний" DES. "Потрійний" DES з двома ключами. "Потрійний" DES із трьома ключами. Міжнародний алгоритм шифрування даних (IDEA). Внутрішня структура алгоритму. Шифрування IDEA. Дешифрування IDEA. Blowfish. Обчислення подключей і S-матриць. Шифрування і дешифрування. RC5. Параметри RC5. Розгортання ключа. Шифрування. Дешифрування. CAST-128. Шифрування.

**Тема 6.** Традиційне шифрування і конфіденційність. Розміщення функції шифрування. Потенційні можливості для порушень захисту. Канальне шифрування і наскрізне шифрування. Конфіденційна передача даних. Використання канального шифрування. Використання наскрізного шифрування

**Тема 7.** Розподіл ключів. Сценарій розподілу ключів. Управління ієрархією ключів. Тривалість використання сеансового ключа. Прозора схема управління ключами. Децентралізоване управління ключами. Управління використанням ключів.

**Тема 8.** Генерування випадкових чисел. Використання випадкових чисел. Джерела випадкових чисел. Генератори псевдовипадкових чисел. Криптографічно генеруються випадкові числа. Генератор BBS.

**Змістовий модуль 2. Сучасні методи шифрування**

**Тема 9.** Криптографія з відкритим ключем. Принципи побудови криптосистем з відкритим ключем. Криптосистеми з відкритим ключем. Застосування криптосистем з відкритим ключем. Умови застосування методів криптографії з відкритим ключем. Криптоаналіз схем шифрування з відкритим ключем.

**Тема 10.** Алгоритм RSA. Опис алгоритму. Обчислювальні аспекти. Захищеність алгоритму RSA.

**Тема 11.** Управління ключами. Розподіл відкритих ключів. Розподіл секретних ключів за допомогою системи з відкритим ключем. Обмін ключами за схемою Діффі-Хеллмана

**Тема 12.** Криптографія з використанням еліптичних кривих. Еліптичні криві. Еліптичні криві над кінцевими полями. Еліптичні криві і криптографія. Безпека криптографії з використанням еліптичних кривих

**Тема 13.** Введення в теорію чисел. Прості і взаємно прості числа. Арифметика в класах відрахувань. Властивості арифметики в класах відрахувань. Теореми Ферма і

Ейлера. Алгоритм Евкліда. Пошук найбільшого загального дільника. Обчислення мультиплікативного зворотного. Китайська теорема про залишки. Дискретні логарифми. Ступінь цілого числа по модулю п. індекси

**Тема 14.** Функції хешування. Вимоги, що пред'являються до функції хешування. Прості функції хешування. Атаки, в основі яких лежить парадокс завдання про дні народження. Метод зчеплення блоків. Захист функцій хешування. Атаки з перебором всіх варіантів. Криптоаналіз. Математичне обгрунтування атак

**Тема 15.** Алгоритми хешування. Алгоритм MD5 обчислення профілю повідомлення. Логіка MD5. Функція стиснення MD5. Стійкість MD5. Захищений алгоритм хешування (SHA). Логіка SHA-1. Функція стиснення SHA-1. Порівняльний аналіз SHA-1 і MD5. RIPEMD-160. Логіка RIPEMD-160. Функція стиснення RIPEMD-160. Конструктивні рішення RIPEMD-160. Порівняння з MD5 і SHA-1. HMAC. Цілі розробки HMAC. Алгоритм HMAC. захищеність HMAC

**Тема 16.** Цифрові підписи і протоколи аутентифікації. Цифрові підписи, обґрунтування алгоритму цифрового підпису, вимоги, безпосередня цифровий підпис, арбітражна цифровий підпис. Стандарт цифрового підпису, підхід DSS, алгоритм цифрового підпису. Протоколи аутентифікації, взаємна аутентифікація, одностороння аутентифікація

**Теми лабораторних робіт**

Лабораторна робота 1. Традиційні методи шифрування.

Лабораторна робота 2. Принципи блочного шифрування. Потокові і блокові шифри.

Лабораторна робота 3. Шифр Файстеля.

Лабораторна робота 4. Шифрування DES. Дешифрування DES. Надійність DES.

Лабораторна робота 5. Алгоритм RSA.

Лабораторна робота 6. Генерування випадкових чисел.

Лабораторна робота 7. Функції хешування. Алгоритми хешування.

## 4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, практичних, семінарських, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі колоквіуму як проміжний міні-екзамен з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті інтегровану оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

розуміння, ступінь засвоєння теорії та методології проблем, що розглядаються; ступінь засвоєння фактичного матеріалу навчальної дисципліни; ознайомлення з рекомендованою літературою, а також із сучасною літературою з питань, що розглядаються; вміння поєднувати теорію з практикою при розгляді виробничих ситуацій, розв'язанні задач, проведенні розрахунків у процесі виконання індивідуальних завдань та завдань, винесених на розгляд в аудиторії; логіка, структура, стиль викладу матеріалу в письмових роботах і при виступах в аудиторії, вміння обґрунтовувати свою позицію, здійснювати узагальнення інформації та робити висновки; арифметична правильність виконання індивідуального та комплексного розрахункового завдання; здатність проводити критичну та незалежну оцінку певних проблемних питань; вміння пояснювати альтернативні погляди та наявність власної точки зору, позиції на певне проблемне питання; застосування аналітичних підходів; якість і чіткість викладення міркувань; логіка, структуризація та обґрунтованість висновків щодо конкретної проблеми; самостійність виконання роботи; грамотність подачі матеріалу; використання методів порівняння, узагальнення понять та явищ; оформлення роботи.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є: глибина і міцність знань, рівень мислення, вміння систематизувати знання за окремими темами, вміння робити обґрунтовані висновки, володіння категорійним апаратом, навички і прийоми виконання практичних завдань, вміння знаходити необхідну інформацію, здійснювати її систематизацію та обробку, самореалізація на лабораторних заняттях.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 5 практичних ситуацій (два стереотипних, два діагностичних та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

**Розподіл балів за тижнями**

| Теми змістового модуля | | | Лекційні заняття | Практичні заняття | Лабораторні заняття | Семінарські заняття | Перевірка есе | Презентація | Експрес-опитування | Тестування | Письмова контрольна робота | Колоквіум | Усього |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Змістовий модуль 1. | **Тема 1** | 1 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 2** | 2 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 3** | 3 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 4** | 4 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 5** | 5 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 6** | 6 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 7** | 7 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 8** | 8 тиждень | 0,5 | | 2 | | | | | | 10 | | 12,5 |
| Змістовий модуль 2. | **Тема 9** | 9 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 10** | 10 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 11** | 11 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 12** | 12 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 13** | 13 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 14** | 14 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 15** | 15 тиждень | 0,5 | | 2 | | | | | | | | 2,5 |
| | **Тема 16** | 16 тиждень | 0,5 | | 2 | | | | | | 10 | | 12,5 |
| | Іспит | | | | | | | | | | | | 40 |
| **Усього** | | | | | | | | | | | | | 100 |

**Шкала оцінювання: національна та ЄКТС**

| Сума балів за всі види навчальної діяльності | Оцінка ЄКТС | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, курсового проекту (роботи), практики | для заліку |
| 90 – 100 | A | відмінно | зараховано |
| 82 – 89 | B | добре | |

| | | | |
|---|---|---|---|
| 74 – 81 | C | | |
| 64 – 73 | D | задовільно | |
| 60 – 63 | E | | |
| 35 – 59 | FX | незадовільно | не зараховано |
| 1 – 34 | F | | |

## 5. Рекомендована література

### 5.1 Основна


1. В. Мао. Современная криптография: теория и практика. - СПб.: Вильямс, 2005,Д 85с.
2. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование - М.: СОЛОН-ПРЕСС, 2009
3. Бирюков А. А. Информационная безопасность: защита и нападение - М.: ДМК Пресс, 2012
4. Виега Д., Лебланк Д., Ховард М. 19 смертных грехов, угрожающих безопасности программ : Как не допустить типичных ошибок - М.: ДМК Пресс, 2009 v


### 5.2 Додаткова


5. Вернет, Пэйн. Криптография. Официальное руководство RSA Security. - М.: Бином, 2002,342с.
6. Грэм, Кнут, Паташник. Конкретная математика. - М.: Мир, 1998, 145с.
7. П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. Программно-аппаратные средства обеспечения информационной безопасности. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000, 176с.
8. А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Введение в защиту информации в автоматизированных системах. - М.: Горячая Линия - Телеком, 2001, 126с.
9. А.А. Молдовян, Н.А. Молдовян, Гуц, Изотов. - Криптография: скоростные шифры. - СПб.: БХВ, 2002, 222 с.
10. Ноден, Ките. Алгебраическая алгоритмика. - М.: Мир, 1999, 192с.


### 5.3 Інформаційні ресурси в мережі Інтернет

11. www.cyberpol.ru Комп'ютерна злочинність і способи боротьби.
12. www.iso27000.ru Інформаційний портал, присвячений питанням управління інформаційною безпекою.
13. www.itsec.ru Інтернет-журнал «Інформаційна безпека».
14. www.inside-zi.ru Інформаційно-методичний журнал «Захист інформації. Інсайд».www.kaspersky.ru Лаборатория Касперского.
15. www.comss.ru.
16. www.drweb.com.
17. www.esethod32.ru.
18. www.kaspersky.ru.
19. http://free.avg.com
20. www.kaspersky.ru/removaltools
21. www.freedrweb.com/cureit/
22. www.computerologia.ru
23. www.free-av.com
24. www.mcafee.com
25. http://www.viruslab.ru/
26. www.bitdefender.com.