**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ ТАРАСА ШЕВЧЕНКА**
**ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ**
**КАФЕДРА ІНТЕЛЕКТУАЛЬНИХ ПРОГРАМНИХ СИСТЕМ**

**«ЗАТВЕРДЖУЮ»**

Заступник декана
з навчальної роботи

_____ Кашпур О.Ф.

«____»_____2019 року

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# БЕЗПЕКА ТА АНОНІМНІСТЬ В ІНТЕРНЕТІ

**для студентів**

| | |
|---|---|
| галузь знань | **12 Інформаційні технології** |
| спеціальність | **121 Інженерія програмного забезпечення** |
| освітній рівень | **магістр** |
| освітня програма | **Програмне забезпечення систем** |
| вид дисципліни | **вибіркова** |

| | |
|---|---|
| Форма навчання | **денна** |
| Навчальний рік | **2021/2022** |
| Семестр | **4** |
| Кількість кредитів ECTS | **3** |
| Мова викладання, навчання та оцінювання | **українська** |
| Форма заключного контролю | **іспит** |

Викладач: **к. т. н., доцент Демківський Є.О.** (лекції).

Пролонговано: на 20__/20__ н. р. _____(_____) «__»___ 20__ р.

на 20__/20__ н. р. _____(_____) «__»___ 20__ р.

**КИЇВ – 2019**

Розробник: Демківський Євген Олександрович, к. т. н., доцент, доцент кафедри інтелектуальних програмних систем.

ЗАТВЕРДЖЕНО

Завідувач кафедри інтелектуальних програмних систем

_____ О.І. Провотар

Протокол № __ від «___» _____2019 р.

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики

Протокол від «____» _____ 2019 року №___

Голова науково-методичної комісії _____ Л.Л. Омельчук

«_____» _____ 2019 року

Затверджено вченою радою факультету комп'ютерних наук та кібернетики

Протокол від «____» _____ 2019 року №___

Голова вченої ради факультету _____ А.В. Анісімов

**1. Мета дисципліни** – вивчення засобів безпечної комунікації, зокрема, захисту комп'ютерних мереж від вторгнення зловмисників.

**2. Попередні вимоги до опанування або вибору навчальної дисципліни:** відсутні.

**3. Анотація навчальної дисципліни.** Навчальна дисципліна «Безпека та анонімність в Інтернеті» є складовою освітньо-наукової програми підготовки фахівців за другим (магістерським) рівнем вищої освіти у галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення в рамках освітньо-наукової програми «Програмне забезпечення систем».

Дана дисципліна належить до переліку № 2 дисциплін вільного вибору студента. Викладається у **4** семестрі в обсязі – **90 год.** (**3 кредити ECTS**), зокрема: лекції – 24 год., самостійна робота – 64 год., консультації – 2 год. У курсі передбачено 1 змістовна частина та 1 контрольна робота. Завершується дисципліна – **іспитом**.

Структура курсу. В рамках вивчення дисципліни розглядаються: основи криптографії; цілісність повідомлень і цифрові підписи; аутентифікація кінцевої точки; забезпечення безпеки електронної пошти; захист TCP-з'єднань за допомогою технології SSL; набір протоколів IPsec і віртуальні приватні мережі; захист бездротових локальних мереж; брандмауери та системи виявлення вторгнень.

**4. Завдання (навчальні цілі).** Основними завданнями дисципліни «Безпека та анонімність в Інтернеті» є набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень в області інформаційної безпеки в мережі Інтернет відповідно до освітньої кваліфікації магістр з інженерії програмного забезпечення.

Вивчити методи шифрування і дешифрування, методи аутентифікації співрозмовника, а також методи, що гарантують цілісність даних. Вивчити, як фундаментальні криптографічні принципи можуть використовуватися для створення безпечних мережевих протоколів. Познайомитись з основами операційної безпеки, тобто з'ясувати, як захистити від атак мережі організацій.

Пояснити важливість і необхідність забезпечення якості в процесі розробки ПЗ, а також надати достатні знання для оволодіння і застосування на практиці ефективних прийомів побудови процесу тестування і забезпечення здатність застосовувати знання у практичних ситуаціях. Зокрема, розвивати:

- Здатність проведення теоретичних та прикладних до-сліджень на відповідному рівні (ЗК03).
- Здатність удосконалювати свої навички на основі аналізу попереднього досвіду (ЗК06).
- Здатність приймати обґрунтовані рішення (ЗК08).
- Здатність аналізувати предметні області, формувати, аналізувати та моделювати вимоги до програмного забезпечення (СК01).
- Здатність ідентифікувати, класифікувати та описувати проектні завдання, знаходити раціональні методи й підходи до їх розв'язання (СК02).
- Здатність оцінювати ступінь обґрунтованості застосування специфікацій, стандартів, правил і рекомендацій в професійній галузі та дотримуватися їх при реалізації процесів життєвого циклу програмного забезпечення (СК05).
- Здатність ефективно керувати фінансовими, людськими, технічними та іншими проектними ресурсами (СК06).

– Здатність систематизувати професійні знання щодо створення і супроводження програмного забезпечення (СК07).

**5. Результати навчання за дисципліною.**

| **Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)** | | **Форми (та/або методи і технології) викладання і навчання** | **Методи оцінювання та пороговий критерій оцінювання (за необхідності)** | **Відсоток у підсумковій оцінці з дисципліни** |
|---|---|---|---|---|
| **Код** | **Результат навчання** | | | |
| РН1.1 | Знати методи шифрування і дешифрування | Лекції, самостійна робота. | Іспит. | 10% |
| РН1.2 | Знати методи аутентифікації співрозмовника | Лекції, самостійна робота. | Іспит. | 10% |
| РН1.3 | Знати методи гарантування цілісності даних | Лекції, самостійна робота. | Іспит. | 10% |
| РН1.4 | Знати як фундаментальні криптографічні принципи можуть використовуватися для створення безпечних мережевих протоколів | Лекції, самостійна робота. | Іспит. | 10% |
| РН2.1 | Вміти захищати від атак мережі організацій | Лекції, самостійна робота. | Контрольна робота (тест), 60% правильних відповідей. | 10% |
| РН2.2 | Вміти забезпечувати безпеку мережі за допомогою брандмауерів і систем виявлення вторгнень | Лекції, самостійна робота. | Тест, 60% правильних відповідей. | 10% |
| РН2.3 | Вміти захищати передачу електронної пошти та TCP-з’єднання | Лекції, самостійна робота. | Тест, 60% правильних відповідей. | 10% |
| РН2.4 | Вміти забезпечувати комплексну безпеку на мережевому рівні | Лекції, самостійна робота. | Тест, 60% правильних відповідей. | 10% |
| РН2.5 | Вміти захищати свою бездротову локальну мережу | Лекції, самостійна робота. | Тест, 60% правильних відповідей. | 10% |
| РН3.1 | Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань тестування та розробки тестів, складати | Самостійна робота. | Тест, 60% правильних відповідей. | 3% |

| | | | | |
|---|---|---|---|---|
| | письмові звіти | | | |
| РН4.1 | Організовувати свою самостійну роботу для досягнення результату | Самостійна робота. | Тест, 60% правильних відповідей. | 3% |
| РН4.2 | Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість | Самостійна робота. | Тест, 60% правильних відповідей. | 4% |

**6. Співвідношення результатів навчання дисципліни із програмними результатами навчання.**

| **Результати навчання дисципліни** / **Програмні результати навчання** | **РН1.1** | **РН1.2** | **РН1.3** | **РН1.4** | **РН2.1** | **РН2.2** | **РН2.3** | **РН2.4** | **РН2.5** | **РН3.1** | **РН4.1** | **РН4.2** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПРН03.** Знати і застосовувати базові концепції і методології моделювання інформаційних процесів. | + | + | + | + | | | | | | | | |
| **ПРН06.** Аналізувати, оцінювати і обирати методи, сучасні програмно-апаратні інструментальні та обчислювальні засоби, технології, алгоритмічні та програмні рішення для ефективного виконання конкретних виробничих задач з програмної інженерії. | | | | | + | + | + | + | + | + | + | + |
| **ПРН09.** Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення. | | + | | + | | | | | | + | + | + |

**7. Схема формування оцінки.**

**7.1 Форми оцінювання студентів.**

**Семестрове оцінювання:**

1. Контрольна робота (тест): РН2.1 – РН2.5, РН 3.1., РН4.1, РН4.2 – **60 балів/36 балів**.

**Підсумкове оцінювання (у формі іспиту):**

1. Максимальна кількість балів які можуть бути отримані студентом: 40 балів.
2. Результати навчання які будуть оцінюватись: РН1.1, РН1.2, РН1.3, РН1.4.
3. Форма проведення і види завдань: письмова робота.
4. Види завдань: 3 письмових завдання.

**Критерії оцінювання на іспиті.**

| **Завдання** | **Тема завдання** | **Вага складових у відсотках** |
|---|---|---|

| | | |
|---|---|---|
| Завдання 1 | Основи криптографії, цілісність повідомлень і цифрові підписи. | 33% |
| Завдання 2 | Автентифікація кінцевої точки, забезпечення безпеки електронної пошти, захист TCP-з'єднань за допомогою технології SSL. | 33% |
| Завдання 3 | Безпека на мережевому рівні, захист бездротових локальних мереж, експлуатаційна безпека. | 34% |
| | | **100%** |

**Запитання для підготовки до іспиту.**

1. У чому відмінність між конфіденційністю повідомлень і цілісністю повідомлень? Чи можливо одне без іншого? Аргументуйте свою відповідь.
2. У чому відмінність між активним і пасивним зловмисниками?
3. У чому принципова відмінність системи з симетричними ключами від системи з відкритим ключем?
4. Припустимо, що зловмисник зумів отримати зашифроване повідомлення, а також те ж саме повідомлення у вигляді відкритого тексту. Який різновид атаки зможе зробити в цьому випадку зловмисник?
5. Припустимо, N людей хочуть спілкуватися по мережі з кожною з решти N-1 людиною, використовуючи шифрування з симетричними ключами. Всі дані, якими обмінюється будь-яка пара з групи, видимі всім іншим членам групи. Передбачається, що ніхто з групи, крім двох учасників обміну даними, не повинен мати можливості розшифрувати ці дані. Скільки всього ключів потрібно для такої системи? Далі припустимо, що використовується шифрування з відкритим ключем. Скільки ключів знадобиться в цьому випадку?
6. Назвіть і поясніть суть найбільш популярної техніки перевірки цілісності повідомлень, що застосовується в багатьох безпечних мережевих протоколах.
7. Які властивості повинна мати криптографічна хеш-функція?
8. Чому проста контрольна сума, на зразок тієї, що застосовується в Інтернет-протоколах, погано підходить для обчислення хеш-значення?
9. Опишіть суть алгоритму обчислення хеш-значення повідомлення MD5.
10. Як можна перевірити цілісність повідомлення?
11. Дайте визначення поняттю «розділений секрет».
12. Як за допомогою розділеного секрету можна підтвердити цілісність повідомлення?
13. Навіщо потрібен і де використовується цифровий підпис?
14. Як створюється цифровий підпис для документа?
15. Яким чином відбувається перевірка підписаного цифровим підписом повідомлення?
16. Навіщо проводиться сертифікація із застосуванням відкритого ключа?
17. В яких мережевих протоколах застосовується сертифікація з відкритим ключем?
18. Дайте визначення поняттю «автентифікація кінцевої точки».
19. Перелічіть основні підходи до автентифікації, які застосовуються в Інтернеті.
20. Назвіть переваги та недоліки сучасних підходів до автентифікації, які застосовуються в Інтернеті.
21. Дайте визначення поняттю «одноразовий номер (nonce)».
22. Наведіть приклад використання одноразового номеру.
23. Які функції безпеки необхідно реалізувати в рамках системи обміну електронними листами, щоб гарантувати безпечність цієї процедури?

24. Поясніть принцип дії програми PGP (Pretty Good Privacy).
25. Чим відрізняється протокол TCP від SSL (Secure Socket Layer)?
26. Якими можливостями доповнює протокол TCP технологія SSL?
27. Назвіть основні етапи роботи протоколу SSL.
28. Перелічіть і охарактеризуйте поля SSL-запису.
29. Перелічіть етапи, з яких складається рукостискання по протоколу SSL.
30. Для чого в SSL застосовуються одноразові номери?
31. Які з основних криптографічних принципів використовує протокол SSL?
32. Які сервіси надаються протоколом IPsec?
33. Для вирішення яких задач створюють віртуальні приватні мережі (VPN)?
34. Яку роль відіграє протокол IPsec при створенні віртуальних приватних мереж?
35. Назвіть два найбільш важливих протоколи з набору протоколів IPsec.
36. Чим відрізняється протокол AH (Authentication Header) від протоколу ESP (Encapsulation Security Payload).
37. Дайте визначення поняттю «безпечна асоціація (security association)».
38. Яку інформацію про стан безпечної асоціації буде зберігати маршрутизатор, який знаходиться у віртуальній приватній мережі?
39. Назвіть види пакетів, що застосовуються в IPsec.
40. Перелічіть і охарактеризуйте поля, з яких складається IPsec-дейтаграма.
41. Які задачі вирішуються за допомогою протоколу обміну ключами в Інтернеті (Internet Key Exchange, IKE)?
42. Назвіть основні відмінності протоколу IKE від протоколу SSL.
43. Яка технологія покликана забезпечити в бездротових мережах рівень безпеки, який можна порівняти з тим, що досягається в звичайних стаціонарних мережах?
44. Перелічіть недоліків в області безпеки, характерних для WEP.
45. Чим стандарт 802.11i відрізняється від 802.11?
46. Опишіть процес автентифікації за протоколом WEP стандарту 802.11.
47. Перелічіть основні параметри алгоритму шифрування даних, що застосовується в технології WEP.
48. З яких етапів складеться робота 802.11i?
49. Дайте визначення поняттю «брандмауер»
50. Які практичні задачі вирішує брандмауер?
51. Назвіть і охарактеризуйте категорії брандмауерів.
52. Яким чином здійснюється поглиблена перевірка пакетів?
53. До основних функцій якого пристрою відноситься генерація повідомлень про потенційно небезпечний трафік?
54. До основних функцій якого пристрою відноситься відфільтровування підозрілого трафіку?
55. Які типи атак дозволяє виявляти система IDS (intrusion detection system).
56. Назвіть категорії систем виявлення вторгнень.

**Студенти не допускаються до іспиту, якщо під час семестру вони набрали менше ніж 36 балів.**

### 7.2 Організація оцінювання.

**Терміни проведення форм оцінювання:**

1. Контрольна робота (тест): до 4-го тижня семестру.

Студенти мають право на одне перескладання контрольної роботи із можливістю отримання максимально 80% початково визначених за цю контрольну роботу балів. Термін перескладання визначається викладачем.

У випадку відсутності студентів з поважних причин відпрацювання та перездачі контрольних робіт здійснюються у відповідності до «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу» від 1 жовтня 2010 року.

У разі неякісного виконання визначених вище робіт, викладач має право не зарахувати роботу, або знизити за неї бали.

Студенти мають право здавати роботи після закінчення визначеного для них терміну, але з втратою 20% від максимальної оцінки за кожен тиждень, який пройшов з моменту закінчення терміну її здачі.

### 7.3 Шкала відповідності оцінок.

| | |
|---|---|
| **Відмінно** / Excellent | 90-100 |
| **Добре** / Good | 75-89 |
| **Задовільно** / Satisfactory | 60-74 |
| **Незадовільно** / Fail | 0-59 |

### 8. Структура навчальної дисципліни. Тематичний план лекцій.

| № лекції | Назва лекції | Кількість годин | |
|---|---|---|---|
| | | Лекції | Самостійна робота |
| 1 | **Тема 1.** Основи криптографії. | 4 | 10 |
| 2 | | | |
| 3 | **Тема 2.** Цілісність повідомлень і цифрові підписи. | 4 | 10 |
| 4 | | | |
| 5 | **Тема 3.** Автентифікація кінцевої точки. | 2 | 6 |
| 6 | **Тема 4.** Забезпечення безпеки електронної пошти. | 2 | 6 |
| 7 | **Тема 5.** Захист TCP-з'єднань за допомогою технології SSL. | 4 | 9 |
| 8 | | | |
| 9 | **Тема 6.** Безпека на мережевому рівні. | 4 | 9 |
| 10 | | | |
| 11 | **Тема 7.** Захист бездротових локальних мереж. | 2 | 6 |
| 12 | **Тема 8.** Експлуатаційна безпека. | 2 | 6 |
| Консультація | | | 2 |
| **ВСЬОГО** | | **24** | **64** |

Загальний обсяг **– 90** год., в тому числі:
Лекцій **– 24** год.
Консультації – **2** год.
Самостійна робота – **64** год.

**9. Рекомендовані джерела.**

**Основні:**


1. Джеймс Куроуз, Кит Росс. Компьютерные сети: Нисходящий подход. 6-е изд. – М.: Издательство «Э», 2016. – 912 с. – ISBN 978-5-699-78090-7.
2. C. Kaufman, R. Perlman, M. Speciner, Network Security, Private Communication in a Public World, Prentice Hall, Englewood Cliffs, NJ, 1995.
3. R. Rivest, The MD5 Message-Digest Algorithm, RFC 1321, Apr. 1992.
4. R. Rivest, The MD4 Message-Digest Algorithm, RFC 1320, Apr. 1992.
5. C. Kaufman, R. Perlman, M. Speciner, Network Security, Private Communication in a Public World, Prentice Hall, Englewood Cliffs, NJ, 1995.
6. H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, RFC 2104, Feb. 1997.
7. International Telecommunication Union, ITU-T X.509, The Directory: Publickey and attribute certificate frameworks (August 2005).
8. S. Kent, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, RFC 1422.
9. P. Ferguson, D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing, RFC 2827, May 2000.
10. The International PGP Home Page, www.pgpi.org.
11. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, Apr. 2006.
12. E. Rescorla, SSL and TLS: Designing and Building Secure Systems, Addison-Wesley, Boston, 2001. 416.
13. S. Crocker, Host Software TechOnLine, Protected Wireless Networks, online webcast tutorial, http://techonline.com/community/tech_topic/internet/21752.
14. C. Rigney, S. Willens, A. Rubens, W. Simpson, Remote Authentication Dial in User Service (RADIUS), RFC 2865, June 2000.
15. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, Diameter Base Protocol, RFC 3588, Sept. 2003.
16. D. Simon, B. Aboba, R. Hurst, The EAP-TLS Authentication Protocol, RFC 5216, Mar. 2008.


**Додаткові:**


1. W. Diffie, M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol IT-22 (1976), pp. 644–654.
2. R. Rivest, A. Shamir, L. Adelman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM, Vol. 21, No. 2 (Feb. 1978), pp. 120–126.

3. Federal Information Processing Standard, Secure Hash Standard, FIPS Publication 180-1. www.itl.nist.gov/fipspubs/fip180-1.htm.
4. D. Jimenez, Outside Hackers Infiltrate MIT Network, Compromise Security, The Tech, Vol. 117, No 49 (Oct. 1997), p. 1, www.tech.mit.edu/V117/N49/hackers.49n.html.
5. P. Zimmermann, Why do you need PGP? www.pgpi.org/doc/whypgp/en/
6. J. Edney and W. A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley Professional, 2003.
7. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley and Sons, 1995.
8. Stubblefield, J. Ioannidis, A. Rubin, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, Proceedings of 2002 Network and Distributed Systems Security Symposium (2002), pp. 17–22.
9. J. Walker, IEEE P802.11 Wireless LANs, Unsafe at Any Key Size; An Analysis of the WEP Encapsulation, Oct. 2000, www.drizzle.com/%7Eaboba/IEEE/0-362.zip.
10. S. Weatherspoon, Overview of IEEE 802.11b Security, Intel Technology Journal (2nd Quarter 2000), http://download.intel.com/technology/itj/q22000/pdf/art_5.pdf.
11. IEEE Std 802.1X-2001 Port-Based Network Access Control, http://standards.ieee.org/reading/ieee/std_public/description/lanman/802.1x-2001_desc.html.
12. Sourcefire Inc., Snort homepage, www.snort.org.
13. J. Koziol, Intrusion Detection with Snort, Sams Publishing, 2003.