



# ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ПРОНИКНЕННЯ

## Робоча програма навчальної дисципліни (Силабус)

### Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (бакалаврський)</i>
Галузь знань	<i>Інформаційні технології</i>
Спеціальність	<i>121 Інженерія програмного забезпечення</i>
Освітня програма	<i>Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Заочна</i>
Рік підготовки, семестр	<i>4-й курс, 1-й семестр</i>
Обсяг дисципліни	<i>4 кред. /120 год. (заочна форма: лекцій 6 год., лаб. 4 год., СРС 110 год.)</i>
Семестровий контроль/ контрольні заходи	<i>Залік, модульна контрольна робота</i>
Розклад занять	<i><a href="http://schedule.kpi.ua/">http://schedule.kpi.ua/</a></i>
Мова викладання	<i>Українська/Англійська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: д. е. н., професор Сігайов Андрій Олександрович Практичні / Семінарські: Лабораторні: Сігайов А. О.</i>
Розміщення курсу	<i>GitHub Classroom, eCampus</i>

### Програма навчальної дисципліни

#### 1 Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

##### **Чому майбутньому фахівцю варто вчити саме цю дисципліну?**

*З переважанням постійного підключення до Internet і досягнень в технологіях, які доступні на сьогодні, кіберзагрози швидко розвиваються для експлуатації різних аспектів цих технологій. Будь-який пристрій є вразливим для атаки, а з появою концепції “інтернету речей” (IoT) це стало реальністю.*

*За минулі роки інвестиції у сферу забезпечення безпеки перейшли з розряду “nice to have” в розряд “must have”, і тепер організації по всьому світу розуміють, наскільки важливо постійно інвестувати в безпеку. Ці інвестиції забезпечать конкурентоспроможність компанії на ринку. Нездатність належним чином захистити свої ресурси може призвести до непоправних збитків, а в деяких випадках — до банкрутства. За нинішнього ландшафту кіберзагроз недостатньо інвестувати тільки в захист. Компанії повинні покращувати загальну стратегію безпеки, а це означає, що інвестиції в захист, виявлення і реагування повинні бути узгоджені.*

**Мета дисципліни.** *Ознайомити студентів з сучасним станом інформаційної безпеки у кібер-енергетичних системах.*

**Предмет дисципліни.** *Огляд інформаційної безпеки, включаючи поточний ландшафт кіберзагроз, виклики простору кібербезпеки, як поліпшити свою стратегію безпеки, ролі Синьої та Червоної команд в установі.*

## **Очікувані результати навчання.**

### **Фахові компетентності.**

ФК 6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

### **Програмні результати навчання.**

ПРН 30. Аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

ПРН 31. Реалізовувати застосунки корпоративних систем з інформаційної безпеки програм і даних, зокрема, в кібер-фізичних та енергетичних системах.

## **2 Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)**

Дисципліна вивчається у сьомому семестрі. Пререквізитів у даного курсу на бакалаврському рівні немає. Постреквізитів у даного курсу на бакалаврському рівні немає.

## **3 Зміст навчальної дисципліни**

1. Як зламати вебсайт.
2. Як працює Інтернет.
3. Як працюють браузерери.
4. Як працюють вебсервери.
5. Як працюють програмісти.
6. Ін'єкційні атаки.
7. Атаки міжсайтового скриптингу.
8. Атаки міжсайтової підробки запиту.
9. Компрометація аутентифікації.
10. Перехоплення сесій.
11. Дозволи.
12. Витоки інформації.
13. Шифрування.
14. Сторонній код.
15. Атаки XML.
16. Не будьте інструментом в чужих руках.
17. Атаки відмови у обслуговування.
18. Підсумкові роздуми.

## **4 Навчальні матеріали та ресурси**

### **Базова література:**

McDonald, M. *Web Security for Developers: San Francisco, CA: No Starch Press, 2020. 216 с. URL: <http://gen.lib.rus.ec/book/index.php?md5=C07B7DD841D0F7180C06E08A8AF9D553>*

### **Додаткова література:**

1. Clark, B. *RTFM: Red Team Field Manual: CreateSpace Independent Publishing Platform, 2014. 96 с. URL: <http://libgen.rs/book/index.php?md5=4e34290b25a81c1132b46be57d181ad4>*

2. White, A. J., Clark, B. *Blue Team Field Manual: CreateSpace Independent Publishing Platform*, 2017. 134 c. URL: <http://libgen.rs/book/index.php?md5=51e0448ce4f9757f6939d74508bfee6d>
3. *Hack The Box :: Penetration Testing Labs*: URL: <https://www.hackthebox.com>
4. *The Enigma Group*: URL: <https://www.enigmagroup.org/>
5. *HackThisSite*: URL: <https://www.hackthissite.org/>
6. *Vulnerable By Design ~ VulnHub*: URL: <https://www.vulnhub.com/>
7. Raienko, N. *enaqx/awesome-pentest*: 2021. URL: <https://github.com/enaqx/awesome-pentest>
8. *vitalysim/Awesome-Hacking-Resources*: 2021. URL: <https://github.com/vitalysim/Awesome-Hacking-Resources>
9. *OlivierLaflamme/Cheatsheet-God*: 2021. URL: <https://github.com/OlivierLaflamme/Cheatsheet-God>
10. *Pwn Adventure 3: Pwnie Island*: URL: <http://www.pwnadventure.com/>
11. *PentesterLab: Learn Web Penetration Testing: The Right Way*: URL: <https://pentesterlab.com/>
12. Seitz, J., Arnold, T. *Black Hat Python: Python Programming for Hackers and Pentesters*: San Francisco, CA: No Starch Press, 2021. 216 c. URL: <http://libgen.rs/book/index.php?md5=FA5CF2BDA4AFD01B888D2FD8BD04888B>
13. Davis, R. *The Art of Network Penetration Testing: How to take over any company in the world*: Shelter Island, NY: Manning Publications, 2020. 304 c. URL: <http://libgen.rs/book/index.php?md5=1F7DE7879D5686BD9F91B22530EE485F>
14. Pruteanu, A. *Becoming the Hacker: The Playbook for Getting Inside the Mind of the Attacker*: Birmingham, UK: Packt Publishing, 2019. 404 c. URL: <http://libgen.rs/book/index.php?md5=6A6D404D4403C482D68AF38A92BB9AC4>
15. Yaworski, P. *Real-World Bug Hunting: A Field Guide to Web Hacking*: San Francisco, CA: No Starch Press, 2019. 264 c. URL: <http://libgen.rs/book/index.php?md5=9BDA3D95334A08FCB5F73B17E69DDE05>
16. Grimes, R. A. *Hacking the Hacker: Learn From the Experts Who Take Down Hackers*: Indianapolis, IN: Wiley, 2017. 320 c. URL: <http://libgen.rs/book/index.php?md5=2361f3ae95017aacaf02d0f94d1dded5>
17. Parasram, S. V. N., Samm, A., Boodoo, D., *ма ин. Kali Linux 2018: Assuring Security by Penetration Testing: Unleash the full potential of Kali Linux 2018, now with updated tools*: Birmingham, UK: Packt Publishing, 2018. 528 c. URL: <http://libgen.rs/book/index.php?md5=516C794F3B3563E35559261430DA642A>
18. Davis, R. *The Art of Network Penetration Testing: How to take over any company in the world*: Shelter Island, NY: Manning Publications, 2020. 304 c. URL: <http://libgen.rs/book/index.php?md5=1F7DE7879D5686BD9F91B22530EE485F>
19. Sikorski, M., Honig, A. *Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software*: San Francisco, CA: No Starch Press, 2012. 800 c. URL: <http://libgen.rs/book/index.php?md5=21F9FDBD90744C6AE0189B9CCDC26BF9>
20. Eagle, C., Nance, K. *The Ghidra Book: The Definitive Guide*: San Francisco, CA: No Starch Press, 2020. 608 c. URL: <http://libgen.rs/book/index.php?md5=69A5AC5AFB0F64EEBB918468238DF733>

## 5 Методика опанування навчальної дисципліни (освітнього компонента)

1. *Злам вебсайтів.*
  - 1.1. *Програмні експойти.*
  - 1.2. *Як зламати вебсайт.*
2. *Як працює Інтернет.*
  - 2.1. *Інтернет-протокол.*
    - 2.1.1. *Адреси мережі Інтернет.*
    - 2.1.2. *Система доменних імен.*
  - 2.2. *Протоколи рівня застосунку.*
    - 2.2.1. *Гіпертекстовий протокол.*
  - 2.3. *З'єднання з підтримкою стану.*
  - 2.4. *Шифрування.*
  - 2.5. *Підсумки.*
3. *Як працюють браузер.*
  - 3.1. *Рендерінг вебсторінки.*
    - 3.1.1. *Конвеєр рендерінгу.*
    - 3.1.2. *Документна об'єктна модель.*
    - 3.1.3. *Стилі відображення інформації.*
  - 3.2. *JavaScript.*
  - 3.3. *До та після рендерінгу: що ще робить браузер.*
  - 3.4. *Підсумки.*
4. *Як працюють вебсервери.*
  - 4.1. *Статичні та динамічні ресурси.*
  - 4.2. *Статичні ресурси.*
    - 4.2.1. *Резолюція URL.*
    - 4.2.2. *Мережі доставлення контенту.*
    - 4.2.3. *Системи управління контентом.*
  - 4.3. *Динамічні ресурси.*
    - 4.3.1. *Шаблони.*
    - 4.3.2. *Бази даних.*
    - 4.3.3. *Розподілені кеші.*
    - 4.3.4. *Мови програмування вебу.*
  - 4.4. *Підсумки.*
5. *Як працюють програмісти.*
  - 5.1. *Фаза 1: дизайн і аналіз.*
  - 5.2. *Фаза 2: написання коду.*

- 5.2.1. *Розподілений або централізований контроль версій.*
- 5.2.2. *Гілкування та злиття коду.*
- 5.3. *Фаза 3: тестування перед релізом.*
  - 5.3.1. *Покриття та неперервна інтеграція.*
  - 5.3.2. *Тестові середовища.*
- 5.4. *Фаза 4: процес релізу.*
  - 5.4.1. *Опції стандартизованого розгортання під час релізу.*
  - 5.4.2. *Процес збирання.*
  - 5.4.3. *Скрипти міграції баз даних.*
- 5.5. *Фаза 5: тестування після релізу.*
  - 5.5.1. *Тестування на проникнення.*
  - 5.5.2. *Моніторинг, ведення логів та повідомлення про помилки.*
- 5.6. *Менеджмент залежностей.*
- 5.7. *Підсумки.*
- 6. *Ін'єкційні атаки.*
  - 6.1. *Ін'єкції SQL.*
    - 6.1.1. *Що таке SQL?*
    - 6.1.2. *Анатомія атаки з ін'єкцією SQL.*
    - 6.1.3. *Нейтралізація наслідків 1: використання параметризованих тверджень.*
    - 6.1.4. *Нейтралізація наслідків 2: використання об'єктно-реляційного відбивання.*
    - 6.1.5. *Бонусна нейтралізація наслідків: застосуйте глибокий захист.*
  - 6.2. *Ін'єкції команд.*
    - 6.2.1. *Анатомія атаки з ін'єкцією команд.*
    - 6.2.2. *Нейтралізація наслідків: використання Escape Control Characters.*
  - 6.3. *Віддалене виконання коду.*
    - 6.3.1. *Анатомія атаки з віддаленим виконанням коду.*
    - 6.3.2. *Нейтралізація наслідків: заборона виконання коду під час десеріалізації.*
  - 6.4. *Вразливості завантаження файлів.*
    - 6.4.1. *Анатомія атаки із завантаженням файлів.*
    - 6.4.2. *Нейтралізація наслідків.*
  - 6.5. *Підсумки.*
- 7. *Атаки міжсайтового скриптингу.*
  - 7.1. *Збережені атаки міжсайтового скриптингу.*
    - 7.1.1. *Нейтралізація наслідків 1: екранування HTML-символів.*
    - 7.1.2. *Нейтралізація наслідків 2: запровадження політики безпеки контенту.*
  - 7.2. *Відображені атаки міжсайтового скриптингу.*

- 7.2.1. *Нейтралізація наслідків: екранування динамічного контенту від HTTP-запитів.*
    - 7.3. *Атаки міжсайтового скриптингу на основі DOM.*
      - 7.3.1. *Нейтралізація наслідків: екранування динамічного контенту від фрагментів URI.*
    - 7.4. *Підсумки.*
  - 8. *Атаки міжсайтової підробки запиту.*
    - 8.1. *Анатомія атаки CSRF.*
      - 8.1.1. *Нейтралізація наслідків 1: дотримуйтесь принципів REST.*
      - 8.1.2. *Нейтралізація наслідків 2: запроваджуйте Anti-CSRF Cookies.*
      - 8.1.3. *Нейтралізація наслідків 3: використовуйте атрибут SameSite Cookie.*
      - 8.1.4. *Бонусна нейтралізація наслідків: вимагайте повторної аутентифікації.*
      - 8.1.5. *Підсумки.*
  - 9. *Компрометація аутентифікації.*
    - 9.1. *Запровадження аутентифікації.*
      - 9.1.1. *HTTP-нативна аутентифікація.*
      - 9.1.2. *Ненативна аутентифікація.*
      - 9.1.3. *Атаки перебору.*
    - 9.2. *Нейтралізація наслідків 1: використання сторонньої аутентифікації.*
    - 9.3. *Нейтралізація наслідків 2: інтеграція з єдиним входом.*
    - 9.4. *Нейтралізація наслідків 3: підвищення безпеки власної системи аутентифікації.*
      - 9.4.1. *Вимагати імена користувачів, адреси електронної пошти або те й інше разом.*
      - 9.4.2. *Вимагати складні паролі.*
      - 9.4.3. *Безпечно зберігання паролів.*
      - 9.4.4. *Вимагати мультифакторну аутентифікацію.*
      - 9.4.5. *Запровадити та убезпечити функцію вихода з системи.*
      - 9.4.6. *Запобігати перебору користувачів.*
    - 9.5. *Підсумки.*
  - 10. *Перехоплення сесій.*
    - 10.1. *Як працюють сесії.*
      - 10.1.1. *Сесії на стороні сервера.*
      - 10.1.2. *Сесії на стороні клієнта.*
    - 10.2. *Як атакувальники перехоплюють сесії.*
      - 10.2.1. *Крадіжка Cookie.*
      - 10.2.2. *Фіксація сесії.*
      - 10.2.3. *Використання слабких ідентифікаторів сесій.*
    - 10.3. *Підсумки.*

## 11. Дозволи.

11.1. Ескалація привилеїв.

11.2. Управління доступом.

11.2.1. Робзробка моделі авторизації.

11.2.2. Запровадження управління доступом.

11.2.3. Тестування управління доступом.

11.2.4. Додавання аудиту слідів.

11.2.5. Запобігання поширеним помилкам.

11.3. Прочісування директорій.

11.3.1. Маршрути та відносні маршрути до файлів.

11.3.2. Анатомія Directory Traversal Attack.

11.3.3. Нейтралізація наслідків 1: довіряйте вашому вебсерверу.

11.3.4. Нейтралізація наслідків 2: використовуйте хостинг-сервіс.

11.3.5. Нейтралізація наслідків 3: застосовуйте непрямі посилання на файли.

11.3.6. Нейтралізація наслідків 1: очищайте посилання на файли.

11.4. Підсумки.

## 12. Витоки інформації.

12.1. Нейтралізація наслідків 1: вимкніть красномовні серверні заголовки.

12.2. Нейтралізація наслідків 2: використовуйте очищені URL.

12.3. Нейтралізація наслідків 3: використовуйте узагальнені параметри Cookie.

12.4. Нейтралізація наслідків 4: вимкніть повідомлення про помилки на сторінці клієнта.

12.5. Нейтралізація наслідків 5: мінімізуйте та обфускуйте ваші файли JavaScript.

12.6. Нейтралізація наслідків 6: очищайте файли на стороні клієнта.

12.7. Намагайтеся йти в ногу з супротивниками у галузі кібербезпеки.

12.8. Підсумки.

## 13. Шифрування.

13.1. Шифрування у протоколі Інтернет.

13.1.1. Алгоритми шифрування, хешування та коди аутентифікації повідомлень.

13.1.2. Рукостискання TLS.

13.2. Увімкнення HTTPS.

13.2.1. Цифрові сертифікати.

13.2.2. Отримання цифрового сертифіката.

13.2.3. Встановлення цифрового сертифіката.

13.3. Атаки на HTTP (і на HTTPS).

13.3.1. Бездротові маршрутизатори.

13.3.2. Точки роздачі Wi-Fi.

13.3.3. Провайдери Інтернет.



13.3.4. Урядові установи.

13.4. Підсумки.

14. Сторонній код.

14.1. Убезпечення залежностей.

14.1.1. Знайте, який код ви запускаєте.

14.1.2. Будьте здатні швидко розгортати нові версії.

14.1.3. Пильнуйте проблеми безпеки.

14.1.4. Знайте, коли треба оновлювати програмне забезпечення.

14.2. Убезпечення конфігурації.

14.2.1. Вимкнення вхідних екаунтів за умовчанням.

14.2.2. Вимкнення виведення списків директорій.

14.2.3. Захист вашої конфігураційної інформації.

14.2.4. Гартування тестових середовищ.

14.2.5. Убезпечення адміністративних панелей управління.

14.3. Убезпечення використаних сервісів.

14.3.1. Захист ваших ключів API.

14.3.2. Захист ваших вебхуків.

14.3.3. Убезпечення контенту, який надається третіми сторонами.

14.4. Сервіси як вектор атаки.

14.4.1. Будьте уважними до несумлінної реклами.

14.4.2. Уникайте доставляння malware.

14.4.3. Використовуйте поважні рекламні платформи.

14.4.4. Використовуйте SafeFrame.

14.4.5. Ретельно налаштовуйте Ad Preferences.

14.4.6. Проглядайте та блокуйте підозрілу рекламу.

14.5. Підсумки.

15. Атаки XML.

15.1. Використання XML.

15.2. Валідація XML.

15.2.1. Визначення типів документів.

15.3. XML-бомби.

15.4. Атаки на зовнішні сутності XML.

15.4.1. Як хакери експлуатують зовнішні сутності.

15.5. Убезпечення вашого XML-парсера.

15.5.1. Python.

15.5.2. Ruby.

15.5.3. Node .js.



- 15.5.4. *Java.*
- 15.5.5. *.NET.*
- 15.6. *Інші міркування.*
- 15.7. *Підсумки.*
- 16. *Не будьте інструментом в чужих руках.*
  - 16.1. *Шахрайство з Email.*
    - 16.1.1. *Використовуйте Sender Policy Framework.*
    - 16.1.2. *Використовуйте DomainKeys Identified Mail.*
    - 16.1.3. *Убезпечення вашої Email: практичні кроки.*
  - 16.2. *Приховування зловмисних посилань у листах.*
    - 16.2.1. *Open Redirect.*
    - 16.2.2. *Запобігання Open Redirect.*
    - 16.2.3. *Інші міркування.*
  - 16.3. *Clickjacking.*
    - 16.3.1. *Запобігання Clickjacking.*
  - 16.4. *Підробка запитів на стороні сервера.*
    - 16.4.1. *Захист від Server-Side Request Forgery.*
  - 16.5. *Ботнети.*
  - 16.6. *Захист від інфікування зловмисним програмним забезпеченням.*
  - 16.7. *Підсумки.*
- 17. *Атаки відмови в обслуговуванні (DoS).*
  - 17.1. *Типи Denial-of-Service Attacks.*
    - 17.1.1. *Атаки на Internet Control Message Protocol (ICMP).*
    - 17.1.2. *Атаки на Transmission Control Protocol (TCP).*
    - 17.1.3. *Атаки на Application Layer (HTTP).*
    - 17.1.4. *Відображені та підсилені атаки.*
    - 17.1.5. *Атаки Distributed Denial-of-Service (DDoS).*
    - 17.1.6. *Ненавмисні атаки DoS.*
  - 17.2. *Нейтралізація наслідків атаки відмови у обслуговуванні.*
    - 17.2.1. *Файерволи та системи запобігання вторгненню.*
    - 17.2.2. *Сервіси захисту від DDoS.*
    - 17.2.3. *Масштабування.*
- 18. *Прикінцеві роздуми.*

## **6 Самостійна робота студента/аспіранта**

*Студент витратить 4 години на тиждень на самостійну роботу з матеріалом курсу.*

## 7 Політика навчальної дисципліни (освітнього компонента)

Студенти отримують бали за правильне та вчасне виконання лабораторних робіт. Загальний рейтинг (кількість балів) складається з: 1) лабораторних робіт (у формі практичних завдань з програмування) та МКР 60%, 2) заліку 40%.

Наразі в курсі наявні три лабораторні роботи, кожне оцінюється до 20 балів. Студент повинен здати правильно виконану лабораторну роботу протягом двох тижнів з дня видачі завдання для отримання повної кількості балів, в іншому випадку застосовуються штрафні бали не більше 40% від загальної кількості за лабораторну роботу.

## 8 Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Поточний контроль: МКР, лабораторні роботи

Календарний контроль: заочною формою навчання не передбачений.

Семестровий контроль: залік

Умови допуску до семестрового контролю: зарахування усіх лабораторних робіт, семестровий рейтинг не менше 40 балів.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	Оцінка
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менш як 60	Незадовільно
Не виконані умови допуску	Не допущено

## 9 Додаткова інформація з дисципліни (освітнього компонента)

- перелік питань, які виносяться на семестровий контроль (див. додаток до силабусу).

### Робочу програму навчальної дисципліни (силабус):

**Складено** Професор кафедри інженерії програмного забезпечення в енергетиці, д.е.н., професор А. О. Сігайов

**Ухвалено** кафедрою інженерії програмного забезпечення в енергетиці (протокол № 28 від 15 травня 2023 р.)

**Погоджено** Методичною комісією Навчально-наукового інституту атомної і теплової енергетики КПІ ім. Ігоря Сікорського (протокол № 9 від 26 травня 2023 р.)