Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

НН Фізико технічний інститут
Кафедра математичного моделювання та аналізу даних

БЕЗПЕКА ІНТЕРНЕТ РЕСУРСІВ

Робоча програма навчальної дисципліни (Силабус)

- Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*вибіркова (цикл професійної підготовки)*
Форма навчання	*очна (денна)*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*4 кредити 120 годин, 36 лекц., 36 лабораторних, 48 - срс*
Семестровий контроль/ контрольні заходи	*Залік, МКР*
Розклад занять	*http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*к.т.н., доцент Барановський Олексій Миколайович* *o.baranovskyi@kpi.ua*
Розміщення курсу	*https://do.ipo.kpi.ua/*

- Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Мета навчальної дисципліни “Безпека інтернет ресурсів” є формування теоретичних знань та практичних умінь у сфері забезпечення безпеки веб-додатків, їх інформаційної та кібернетичної безпеки. Забезпечення комплексного захисту бізнес-процесів компанії чи підприємства на рівні веб-додатків. Розглядаються основи програмування захищених веб-сайтів та засоби серверної безпеки рівня веб-серверу, бази даних, засобів авторизації та аутентифікації користувачів.

Дана дисципліна вивчається один семестр. В процесі вивчення дисципліни розглядаються основи безпеки рівня веб-серверу, засоби безпеки рівня серверної інфраструктури, особливості застосування технології виконання скриптових мов програмування. При вивченні архітектури веб-систем та взаємодії між веб-сервісами, особлива увага звертається на об’єкти захисту/атаки, аутентифікацію та авторизацію, забезпечення безпеки даних, особливості застосування баз даних для побудови захищених веб-рішень, відкриті проекти по забезпеченню безпеки веб-додатків та перспективи організації та виконання тестування рівня безпеки для певного веб-додатку.

Силабус навчальної дисципліни “Безпека інтернет ресурсів” розроблений на основі принципу конструктивного вирівнювання (constructive alignment), що дозволяє передбачити необхідні навчальні завдання та активності, які потрібні студентам для досягнення очікуваних результатів навчання, а потім спроектувати навчальний досвід таким чином, щоб максимально збільшити можливості студентів досягти бажаних результатів.

Метою навчальної дисципліни є формування у студентів компетентностей:

ЗДАТНІСТЬ:

Здатність застосовувати знання у практичних ситуаціях.

Знання та розуміння предметної області та розуміння професії.

Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Здатність до пошуку, оброблення та аналізу інформації.

Спеціальні (фахові, предметні) компетентності:

Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання

Знання:

аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

розробляти моделі загроз та порушника;

аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

вирішувати задачі аналізу програмного коду на наявність можливих загроз.

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

Дисципліна «БЕЗПЕКА ІНТЕРНЕТ РЕСУРСІВ» базується на навичках, отриманих студентами при вивченні таких дисциплін як «Програмування», «Програмне забезпечення обчислювальних систем». Опанування таких дисциплін як «Операційні системи» та «Web-програмування» спростить опанування даної дисципліни.

Отримані практичні навички та засвоєні під час вивчення теоретичні знання в подальшому можна використовувати у професійній діяльності.

3. Зміст навчальної дисципліни

- Тема 1. Вступ і технології
- Тема 2. Вразливості веб-серверів.
- Тема 3. Ін'єкції:
- Тема 3. Безпека сесій.
- Тема 4. Скриптові атаки XSS і CSRF.
- Тема 5. Проблеми автентифікації та авторизації в веб-додатках.
- Тема 6. Проект OWASP:
- Тема 7. Стандарти безпеки веб-додатків: серії ISO 27000, PCI-DSS, HIPPA, SOC2, SOX тощо).

4. Навчальні матеріали та ресурси

Базова література

1. Web Security Testing Cookbook. Paco Hope, Ben Walther. O'Reilly Media, Inc., ISBN 9780596514839
2. Mastering Modern Web Penetration Testing. Prakhar Prasad. Packt Publishing. ISBN 9781785284588
3. Hacking Exposed Web Applications. Joel Scambray, Mike Shema. ISBN 007222438X

Допоміжна література

1. http://pentestmonkey.net/category/cheat-sheet/sql-injection
2. https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SQL%20Injection
3. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection
4. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
5. https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_Cheat_Sheet.html
6. https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
7. https://owasp.org/www-community/vulnerabilities/PHP_File_Inclusion
8. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/01-Testing_Directory_Traversal_File_Include
9. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

10. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.2-Testing_for_Remote_File_Inclusion
11. https://owasp.org/www-community/attacks/Server_Side_Request_Forgery
12. https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html
13. https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html
14. https://owasp.org/www-community/attacks/Session_hijacking_attack
15. https://owasp.org/www-community/attacks/Session_fixation
16. https://github.com/Coalfire-Research/java-deserialization-exploits
17. https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Insecure%20Deserialization/Java.md
18. http://www.phpinternalsbook.com/php5/classes_objects/serialization.html
19. https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A8-Insecure_Deserialization
https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html
20. https://www.geeksforgeeks.org/php-serializing-data/
21. https://nickbloor.co.uk/2017/08/13/attacking-java-deserialization/
22. https://www.nccgroup.com/uk/about-us/newsroom-and-events/blogs/2019/march/finding-and-exploiting-.net-remoting-over-http-using-deserialisation/

- Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять:
- лекційні заняття;
- лабораторні заняття.

Теми дисципліни взаємозв’язані, матеріал вивчається в логічній послідовності. На лекційних заняттях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити студентам можливість глибокого самостійного вивчення всього програмного матеріалу. Теми та порядок виконання лабораторних занять сформовано в логічній послідовності і повністю узгоджуються з метою дисципліни. Теоретичні і лабораторні знання поглиблюються шляхом самостійної роботи з використанням рекомендованої літератури та глобальної мережі Internet.

На заняттях використовуються презентації лекцій. Велика частина методичних матеріалів міститься у вищевказаній методичній літературі.

- Тема 1. Вступ і технології
  - Сучасні та застарілі технології створення веб-додатків
  - Збір інформації про веб-додатки. Використання пошуковика Google.
  - Enumeration веб-додатків/серверів
- Тема 2. Вразливості веб-серверів.
  - Неправильна конфігурація, shrink wrap
  - Path traversal
  - Heartbleed, Poodle, Bashbug (shellshock)
- Тема 3. Ін'єкції:
  - SQL-ін’єкції: error-based, blind, double blind (на основі часу). Захист від SQL-ін’єкцій.
  - Ін’єкції функцій, коду, ін’єкції команд тощо, підключення файлів, проблеми завантаження файлів у веб-додатках. Захист від ін’єкцій коду та команд.
  - Небезпечна десеріалізація. Ін'єкції XML.
- Тема 3. Безпека сесій.
  - Загальний опис сесій. Стани в HTTP, HTTPS. Сховища сеансів.
  - Атаки на сесії: фіксація сеансів, прогнозування сеансів, захоплення та перехоплення сеансу. Захист сесій.

- Тема 4. Скриптові атаки XSS і CSRF.
    - Клікджекінг. Захист від скриптових атак: заголовки безпеки.
- Тема 5. Проблеми автентифікації та авторизації в веб-додатках.
    - Загальні вразливості автентифікації: перерахування, атаки на паролі. Захист: captcha, відстеження та блокування, перенаправлення.
    - Загальні помилки авторизації: доступ до функцій/об'єктів. Маніпулювання параметрами.
- Тема 6. Проект OWASP:
    - Керівництво з тестування безпеки веб-додатків OWASP
    - Стандарт перевірки безпеки додатків OWASP (ASVS 4.0)
    - Модель зрілості Software Assurance
- Тема 7. Стандарти безпеки веб-додатків: серії ISO 27000, PCI-DSS, HIPPA, SOC2, SOX тощо).

5.1 Лабораторні заняття

Безпека інтернет ресурсів

№ з/п	**Назва теми та перелік основних питань** *(перелік дидактичних засобів, завдання на СРС з посиланням на літературу)*
1	**Information Gathering**
2	**Web Server Vulnerabilities**
3	**SQL Injections**
4	**CCF Injections**
5	**Session Attacks**
6	**XSS and CSRF**
7	**Password Attacks and enumeration**
8	**Parameter tampering and authorization errors.**
9	**XML attacks**
10	**Insecure Deserialization**

6. Самостійна робота студента (СРС)

Безпека інтернет ресурсів

№ з/п	Назви тем і питань, що виноситься на самостійне опрацювання та посилання на навчальну літературу
1	Методики удосконалення конфігурації веб-серверів
2	Порядок проведення робіт по тестуванню безпеки веб-додатків
3	Протидія несанкціонованому доступу до ресурсів веб-серверів
4	Засоби автоматизації тестування безпеки веб-додатків
5	Інструментальні засоби проведення аудиту безпеки веб-додатків
6	Підготовка до заліку

-

- **Політика та контроль**

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати заняття. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, які здатні розвинути практичні уміння та навички.

Порушення термінів виконання завдань та заохочувальні бали

Заохочувальні бали

Критерій	Ваговий бал
Участь у міжнародних, всеукраїнських та/або інших заходах та/або конкурсах, підготовка наукової статті (за тематикою навчальної дисципліни)	10 балів

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.
Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Семестровий контроль: залік

1. **Розрахунок шкали рейтингу:**

№ з/п	Контрольний захід	%	Кіл-ть	Всього
1.	Лабораторні роботи	5	10	50
2.	Модульна контрольна робота (МКР)	50	1	50
	Всього			100

На останньому за розкладом занятті викладач проводить семестрову атестацію у вигляді співбесіди зі студентами, які не змогли отримати за рейтингом позитивну оцінку (набрали протягом семестру менше ніж 60 балів (RD < 60)), але були допущені до семестрової атестації. Ці студенти зобов'язані проходити співбесіду. У даному випадку рейтингова оцінка студента буде складатись з результатів роботи в семестрі (RD) та результатів співбесіди, але не вище 60 балів.

Студенти, які протягом семестру отримали більш ніж 60 балів, можуть пройти співбесіду з метою підвищення оцінки. У даному випадку семестровий рейтинг студента анулюється, і студент отримує оцінку за результатами співбесіди.

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
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (Силабус):

Складено:

к.т.н, доцентом Барановським Олексієм Миколайовичем.

Ухвалено кафедрою інформаційної безпеки (протокол № 6/ 2022_від 22.06.2022р.)

Погоджено Методичною комісією ФТІ (протокол № 7 /2022_ від 30.06.2022р.)