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

Кафедра інженерії програмного забезпечення в енергетиці (ІПЗЕ)

Методи та засоби виявлення уразливостей та забезпечення безпеки Web-ресурсів

Робоча програма навчальної дисципліни

(Силабус)

Реквізитинавчальної дисципліни

Рівень вищої освіти	другий (магістерській)
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем в енергетиці*
Статус дисципліни	*вибіркова*
Форма навчання	*Очна(денна)*
Рік підготовки, семестр	*1 курс весняний семестр*
Обсяг дисципліни	*4 кредити, 120 годин, з яких 54 години аудиторних (36 год лекції, 18 год лабораторні), 66 години становить самостійна робота*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	http://rozklad.kpi.ua/
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: д.т.н., *професор Гаврилко Євген Володимирович, gev.1964@ukr.net, тел. 067-506-91-85* Лабораторні заняття: д.т.н., *професор Гаврилко Євген Володимирович, gev.1964@ukr.net, тел. 067-506-91-85*
Розміщення курсу	*Googleclassroom, Zoom, еКампус, Телеграмм*

Програма навчальної дисципліни

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

Захист інформації та кібербезпека формують окремі важливим напрями діяльності спеціалістів ІТ, інженерів з програмного забезпечення. Вивчення вибіркової дисципліни «Методи та засоби виявлення уразливостей та забезпечення безпеки Web-ресурсів» присвячене різним підходам захисту інформації та забезпечення безпеки Web-ресурсів від несанкціонованого впливу, внесенню змін, зникненню та крадіжкам.

Метою навчальної дисципліни є формування у студентів здатностей до використання законодавства України, організаційних, технічних, алгоритмічних та інших методів і засобів захисту програм і даних у цій області з метою забезпечувати захист Web-ресурсів.

Завдання. Основними завданнями вивчення дисципліни «Методи і засоби забезпечення безпеки Web-ресурсів» є отримання студентом компетенцій для того, щоб приймати участь у проектуванні інформаційних систем, розглянуті загальні питання криптоаналізу, зокрема типи криптоаналізу з точки зору інформації, яку має криптоаналітик; надана класифікація шифросистем стосовно

захищеності (стійкості до криптоаналізу). Наведені приклади зламування шифросистем. Значна увага приділяється електронному цифровому підпису, який підтверджує дійсність і цілісність документа та засвідчує авторствореалізації дискретних структур різних типів, створення складних процедур обробки.

В результаті вивчення дисципліни у студентів повинні сформуватися наступні компетентності:

загальні:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК1),
- Здатність спілкуватися іноземною мовою як усно, так і письмово (ЗК2),
- Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами інших галузей знань/видів економічної діяльності) (ЗК4).

фахові:

- Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення (ФК5);
- Здатність проектувати архітектуру програмного забезпечення, моделювати процеси функціонування окремих підсистем і модулів (ФК3);
- Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах (ФК7);

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні результати навчання:

- визначати вимоги політики безпеки та формувати свій профіль захисту відповідно до забезпечення послуг безпеки в інформаційній системі (ПРН1);
- ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в інформаційній системі (ПРН3);
- забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації (ПРН5);
- аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники інформаційних систем в цілому(ПРН7);
- проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів (ПРН7);
- забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій (ПРН12).

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

Пререквізити дисципліни. Знання та вміння, отримані при вивченні дисциплін: «Комп'ютерна дискретна математика», «Алгоритмізація та програмування», «Операційні системи», «Об'єктно-орієнтований аналіз та конструювання програмних систем», «Захист комп'ютерних програм».

***Постреквізити дисципліни*.** Отримані знання при вивченні дисципліни «Комп'ютерне моделювання та оптимізація» формує базові знання для вивчення дисциплін, пов'язаних з моделюванням, чисельним розв'язком обчислювальних задач, оптимізації та розробки програмного забезпечення для систем захисту Web-ресурсів.

3. Зміст навчальної дисципліни

Розділ 1. РОЗВИТОК ТЕОРІЇ І ПРАКТИКИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-РЕСУРСІВ.

Історія захисту Web-ресурсів. Короткий огляд історії безпеки програмного забезпечення за напрямом безпеки Web-ресурсів. Розглянути передісторію витоків хакерства. Короткий огляд головних подій у цій галузі за останні сто років дозволяє більш-менш уявити технологію, на якій ґрунтуються сучасні Web-додатки. електромеханічна роторна машина «Енігма». Автоматизований злом шифру «Енігми». Історія кібернетичних розробок Англійського математика Алана Т'юрінг та Діллі Нокса. Криптологічна бомба. Початок комп'ютерного злому. Історія всесвітньої павутини (the WorldWideWeb, WWW), що з'явилася у 1990-х, а її популярність почала стрімко зростати на початку 2000-х.

Підходи щодо захисту Web-ресурсів. основні поняття і аналіз загроз інформаційної безпеки. основні поняття захисту інформації і інформаційної безпеки. Політика безпеки Web-ресурсів. аналіз загроз інформаційної безпеки. основні методи реалізації загроз інформаційної безпеки. компоненти забезпечення безпеки інформаційної системи. способи забезпечення комп'ютерної безпеки. Огляд методів захисту Web-ресурсу. стандарти оцінки безпеки інформаційних систем. загальні методи забезпечення інформаційної безпеки. Класифікація захисту сучасних операційних систем.

Розділ 2. РОЗВИТОК ТЕОРІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-РЕСУРСІВ.

Оцінка вразливості Web-ресурсів. Методи попереднього вивчення, а саме оцінка вразливостей Web-ресурсів дозволяють розуміти технічні пристрої та структуру Web-додатку, а також служб, що забезпечують його роботу.

Оцінка програмних засобів, що забезпечують роботу Web-ресурсів. Оцінка структури web-ресурсів. Підходи Проведення Порівняння сучасних та ранніх версій додатків. Розгляд REST API. Підхід до Поділу функцій клієнта та сервера. Розгляд формат JSON. Ознайомлення з Програмним інтерфейсом DOM браузера та

Розгляд набору Фреймворка(ів) для SPA. Ознайомлення з системами аутентифікації та авторизації. Розгляд питань, шо стосуються WEB-серверів, програмного забезпечення Web-сервера, які працює в операційній системі зазвичай це якийсь дистрибутив Linux: Ubuntu, CentOS або RedHat.

Розгляд порядку зберігання даних на стороні клієнта. Зберігання та доступ до даних у вигляді пари «ключ-значення».

Оцінка програмних засобів для пошуку api Web-ресурсу. Аналіз API WEB-ресурсів. Виявлення кінцевої точки. Механізми аутентифікації. Різновиди кінцевих точок. Виявлення сторонніх залежностей Web-додатку.

Оцінка сторонніх залежностей Web-додатку. Клієнтські фреймворки, Фреймворки для односторінкових додатків, EmberJS, AngularJS, ReactVueJS, Бібліотеки JavaScript. Фреймворки на стороні сервера, Стандартні повідомлення про помилку та «Сторінки 404», Репозиторій CSS. Бази даних.

Розділ 3. МЕТОДИ ТА ЗАСОБИ ЗЛАМУ WEB-РЕСУРСІВ.

Використання результатів оцінок для зламу Web-ресурсів. Міжсайтовий скриптинг (XSS). Специфіка XSS атаки, виявлення XXS-вразливостей.

Методи підробки міжсайтових запитів (CSRF). Підхід для оцінки атаки CSRF, Приклади оцінки атаки CSRF.

атака на зовнішні сутності XML-документа. Аналіз атак на зовнішні сутності XML-документа, ExternalEntity, XXE). Непряма XXE-атака.

Розділ 4. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ WEB-РЕСУРСІВ.

Методи захисту архітектури Web-ресурсів. Проведення аналізу архітектури захищеного програмного забезпечення. Проведення глибокий аналіз коду ПЗ. Підходи до пошуку уразливост. Пошук вразливостей. Аналіз уразливості. Управління вразливістю. Регресивне тестування. Заходи щодо зниження ризику. Прикладні техніки розвідки та нападу. Методи зниження ризику.

Методи вибору безпечної архітектури Web-ресурсів. Аналіз вимог до ПЗ. Аутентифікація та авторизація. Протоколи SSL та TLS. Захист облікових даних: паролі, хешування, автентифікація.

МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-РЕСУРСУ. Автоматизована перевірка. Статичний аналіз. Регресійне тестування. Регресійне тестування. Процедури відповідального розкриття інформації.

МЕТОДИ УПРАВЛІННЯ ВИЯВЛЕНИХ ВРАЗЛИВІСТЕЙ У WEB-РЕСУРСАХ. Класифікація і відтворення вразливостей. Загальна система оцінки вразливостей.

Розділ 5. МЕТОДИ ТА СПОСОБИ ЗАХИСТУ WEB-РЕСУРСІВ.

Методи захисту захист Web-додатку від XSS атак. Атаки XSS і їх особливості.

Методи захисту Web-ресурсу від CSRF атак. Перевірка заголовків. CSRF-токени без збереження стану. Протидія CRSF на рівні коду. Зниження ризику CSRF на рівні програми. Проміжне програмне забезпечення для протидії CSRF-атакам.

Методи захисту Web-ресурсу від DOS атак. Протидія атакам ReDoS. ахист від логічних DoS-атак. Захист від DDoS. Пом'якшення DDoS-атак.

Заплановані види навчальної діяльності та методи навчання

Планується проведення навчальних занять у виді лекцій та лабораторних занять. Основний змістовний матеріал дисципліни викладається на лекціях. Лабораторні заняття проводяться з метою закріплення знань з основних тем дисципліни; формування у студентів навичок і вмінь з використання технологій захисту інформації Web-рисурсів.

4. Навчальні матеріали та ресурси

HTML5 Security Cheatsheet [Електронний ресурс]. – Режим доступу: https://html5sec.org.

Andrew Hoffman .Web Application Security: Exploitationand ountermeasuresfor Modern Web Applications, - :,2021.—336c.

Heiderich M., Nava E., Heyes G., Lindsay D. WebApplicationObfuscation. – ISBN-10: 1597496049.

McNab C. NetworkSecurityAssessment : KnowYourNetwork, secondedition. – ISBN-10:0-596-51030-6.

OWASP Foundation. OWASP TestingGuide v4.0 [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Web_Application_Penetration_ Testing.

Ristic I. Bulletproof SSL and TLS: Understandinganddeploying SSL/TLS and PKI tosecureserversand Webapplications. – ISBN-10: 1907117040.

Stuttard D., Pinto M. The Web Applicaion Hackers's Handbook: Findingand Exploiting Security Flaws. – ISBN-10: 1118026470.

Zalewski M. The Tangled Web: A GuidetoSecuring Modern Web Applications. – ISBN-10: 1593273886.

ДжоелСкембрей, Майк Шема. «Секретыхакеров/ Безопасность WEB-приложений - готовыерешения/ - пер з англ. – Днепр, 2003.- 384 с.

Джонсон Дэн Берг, Деоган Дэниел, Савано Дэниел /Безопаснobydesign/. — Днепр:, 2021. — 432 с.

Домарев В. В. Защитаинформации и безопасностькомпьютерных систем / В. В. Домарев. – К. : Диа-софт, 2009. – 234 с.

Защита в виртуальнойсреде: чеклистугроз [Електронний ресурс]. – Режим доступу: https://habr.com/company/croc/blog/140044.

Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД : навч. посіб. / М. В. Захарченко, В. Г. Кононович, В. Й. Кільдішев, Д. В. Голев; під ред. ак. МАІ М. В. Захарченка.– Одеса : ОНАЗ ім. О. С. Попова, 2011. – 168 с.

Інформаційна стійкість комп'ютерних технологій і мереж : навч. посіб. / А. В. Луговой, О. Г. Славко, П. П. Костенко, М. І. Гученко, М. М. Гузій. – Кременчук : Вид-во ПП Щербатих О. В., 2015. – 350 с.

Лисиченко М. Л. Методичні рекомендації щодо механізму перевірки письмових робіт на плагіат / М. Л. Лисиченко, В. І. Жила, А. В. Левкін. – Х.: ХНТУСГ, 2017. – 28 с.

Тарасюк О. М. Безопасность и устойчивостьWeb- и облачных систем. Практикум / О. М. Тарасюк, А. В. Горбенко; под ред. В. С. Харченко. – Министерствообразования и науки Украины, Национальныйаэрокосмическийуниверситетим. Н. Е. Жуковского «ХАИ», 2017. – 40 с.

Троян С. О. Захист інформаційних ресурсів: навчально-методичний посібник до курсу «Захист інформаційних ресурсів» / С. О. Троян. – Умань: [б. в.], 2012. – 120 с.

Навчальний контент

5. Методика опанування навчальної дисципліни(освітнього компонента)

РОЗДІЛ 1. РОЗВИТОК ТЕОРІЇ І ПРАКТИКИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-РЕСУРСІВ.

Лекція 1.1. Історія захисту Web-ресурсів.

Короткий огляд історії безпеки програмного забезпечення за напрямом безпеки Web-ресурсів. Розглянути передісторію витоків хакерства. Короткий огляд головних подій у цій галузі за останні сто

років дозволяє більш-менш уявити технологію, на якій ґрунтуються сучасні Web-додатки. Електромеханічна роторна машина «Енігма». Автоматизований злом шифру «Енігми».

Лекція 1.2. Підходи щодо захисту Web-ресурсів.

Основні поняття і аналіз загроз інформаційної безпеки. Основні поняття захисту інформації і інформаційної безпеки. Огляд методів захисту Web-ресурсу. Стандарти оцінки безпеки інформаційних систем. Загальні методи забезпечення інформаційної безпеки. Класифікація захисту сучасних операційних систем.

Розділ 2. РОЗВИТОК ТЕОРІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-РЕСУРСІВ.

Лекція 2.1. Оцінка вразливості Web-ресурсів.

Методи попереднього вивчення, а саме оцінка вразливостей Web-ресурсів дозволяють розуміти технічні пристрої та структуру Web-додатку, а також служб, що забезпечують його роботу.

Лекція 2.2. Оцінка програмних засобів, що забезпечують роботу Web-ресурсів.

Оцінка структури web-ресурсів. Підходи Проведення Порівняння сучасних та ранніх версій додатків. Розгляд REST API.

Лекція 2.3. Оцінка програмних засобів для пошуку api Web-ресурсу. Аналіз API WEB-ресурсів. Виявлення кінцевої точки. Механізми аутентифікації. Різновиди кінцевих точок. Виявлення сторонніх залежностей Web-додатку.

Лекція 2.4. Оцінка сторонніх залежностей Web-додатку. Клієнтські фреймворки, Фреймворки для односторінкових додатків, EmberJS, AngularJS, ReactVueJS, Бібліотеки JavaScript. Фреймворки на стороні сервера, Стандартні повідомлення про помилку та «Сторінки 404», Репозиторій CSS. Бази даних.

Розділ 3. МЕТОДИ ТА ЗАСОБИ ЗЛАМУ WEB-РЕСУРСІВ.

Лекція 3.1. Використання результатів оцінок для зламу Web-ресурсів.

Міжсайтовий скриптинг (XSS). Специфіка XSS атаки, виявлення XXS-вразливостей.

Лекція 3.2. Методи підробки міжсайтових запитів (CSRF).

Підхід для оцінки атаки CSRF, Приклади оцінки атаки CSRF.

Лекція 3.3. Атака на зовнішні сутності XML-документа.

Аналіз атак на зовнішні сутності XML-документа, ExternalEntity, XXE). Непряма XXE-атака.

Розділ 4. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ WEB-РЕСУРСІВ.

Лекція 4.1. Методи захисту архітектури Web-ресурсів.

Проведення аналізу архітектури захищеного програмного забезпечення. Проведення глибокий аналіз коду ПЗ. Підходи до пошуку уразливост. Пошук вразливостей. Аналіз уразливості. Управління вразливістю. Регресивне тестування. Заходи щодо зниження ризику. Прикладні техніки розвідки та нападу. Методи зниження ризику.

Лекція 4.2. Методи вибору безпечної архітектури Web-ресурсів.

Аналіз вимог до ПЗ. Аутентифікація та авторизація. Протоколи SSL та TLS. Захист облікових даних: паролі, хешування, автентифікація.

Лекція 4.3. Методи виявлення вразливостей Web-ресурсу.

Автоматизована перевірка. Статичний аналіз. Регресійне тестування. Регресійне тестування. Процедури відповідального розкриття інформації.

Лекція 4.4. Методи управління виявлених вразливістей у Web-ресурсах.

Класифікація і відтворення вразливостей. Загальна система оцінки вразливостей.

Розділ 5. МЕТОДИ ТА СПОСОБИ ЗАХИСТУ WEB-РЕСУРСІВ.

Лекція 5.1. Методи захисту захист Web-додатку від XSS атак.

Атаки XSS і їх особливості.

Лекція 5.2. Методи захисту Web-ресурсу від CSRF атак.

Перевірка заголовків. CSRF-токени без збереження стану. Протидія CRSF на рівні коду. Зниження ризику CSRF на рівні програми. Проміжне програмне забезпечення для протидії CSRF-атакам.

Лекція 5.3. Методи захисту Web-ресурсу від DOS атак.

Протидія атакам ReDoS. ахист від логічних DoS-атак. Захист від DDoS. Пом'якшення DDoS-атак.

6. Самостійна робота студента

Розділ 1. ІСТОРІЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ І WEB-РЕСУРСІВ.

Початок комп'ютерного злому, хакери, білі хакери.

Методи захисту інформації Web-ресурсів. Огляд методів захисту Web-ресурсів. Підсистема розмежування доступу. Підсистема антивірусного захисту Підсистема контролю цілісності. Підсистема виявлення вторгнень. Підсистема криптографічного захисту.

Розділ 2. ОЦІНКА ВРАЗЛИВОСТІ WEB-РЕСУРСІВ.

Оцінка вразливості архітектури Web-ресурсів.

Підходи проведення порівняння сучасних та ранніх версій додатків. REST API. Поділ функцій клієнта та сервера. Розгляд формат JSON. Ознайомлення з Програмним інтерфейсом DOM браузера.

Пошук безлічі додатків в рамках домена. Вбудовані в браузер інструменти аналізу. Соціальні профілі. Груба сила для пошуку субдоменів

Механізми аутентифікації. Різновиди кінцевих точок. Клієнтські фреймворки. Фреймворки для односторінкових додатків, EmberJS, AngularJS, ReactVueJS, Бібліотеки JavaScript. Фреймворки на стороні сервера, Стандартні повідомлення про помилку та «Сторінки 404», Бази даних.

Розділ 3. МЕТОДИ ЗЛАМУ WEB-РЕСУРСІВ.

Синтез і аналіз мислення хакера. Застосування даних, отриманих у процесі розвідки.Підробка міжсайтових запитів (CSRF). Підробка параметрів запиту. Зміна вмісту запиту GET. CSRF-атака на кінцеві точки POST. Відмова в обслуговуванні (DoS). ReDoS-атака. Распределенная DDoS-атака.

Розділ 4. ЗАХИСТ WEB-РЕСУРСІВ.

Перевірка заголовків. CSRF-токен. CSRF-токени без збереження стану. Протидія CRSF на рівні коду. Запити GET без збереження стану. Зниження ризику CSRF на рівні програми. Проміжне програмне забезпечення для протидії CSRF-атакам.

Протидія DoS-атакам.

Протидія атакам ReDoS. Захист від логічних DoS-атак. Захист від DDoS. Пом'якшення DDoS-атак

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування лекційних та практичних занять є обов’язковим за винятком поважних причин (хвороби, форс-мажорних обставин).

В разі пропущення занять з поважних причин викладач надає можливість студенту виконати усі або деякі лабораторні завдання (винятком є виконання деяких завдань у зв’язку із закінченням навчального процесу).

В разі пропущення занять без поважних причин, а також через порушення граничноготерміну виконання завдання (deadline)студент може отримати зменшену кількість балів від максимальної оцінки за відповідне завдання.

Протягом семестру студенти:

- виконують та захищають лабораторні роботи у відповідні терміни,
- пишутьмодульнуконтрольну роботу,
- повинні позитивно закрити дві атестації (в кінці березня та в серединітравня),
- по закінченні навчального процесу складають залік.

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

Система рейтингових (вагових) балів та критерії оцінювання

Максимальна кількість балів з кредитного модуля дорівнює 100.

Рейтинг студента з дисципліни складається з балів, що він отримує за:

- виконання та захист лабораторних робіт,
- модульну контрольну роботу (МКР) тривалістю 1 акад. година.

1. <u>Виконання завдань лабораторних робіт</u>

Завдання лабораторної роботи являє собою індивідуальне виконання робіт, що пов'язані з рішенням на ЕОМ заданої задачі комп’ютерного моделювання.

Вагові бали завдань наведено у таблиці.

Види завдань	*Внесок до семестрового рейтингу балів*
Завдання №1. Аналіз безпеки і захищеності Web-ресурсів	10
Завдання №2. Пошук вразливості Web-ресурсу	10
Завдання №3. Особливості криптографії систем захисту Web-ресурсу у віртуальних системах	10

Максимальна кількість балів за всі завдання дорівнює 30 балів.

Критерії оцінювання

Підготовка до роботи (у відсотках від максимальної кількості балів за відповідну роботу):

- протокол відповідає вимогам, охайний – 20 %;
- протокол відповідає вимогам, але є чисельні виправлення – 10 %;

Виконання завдання лабораторної роботи:

- робота виконана повністю і вірно протягом відведеного часу – 50 %;
- робота виконана пізніше зазначеного терміну – 20 %;

Якість захисту роботи:

- студент вірно і повністю відповів на запитання – 30 %;
- студент при відповіді допустив несуттєві неточності – 20 %;
- студент при відповіді на запитання допустив суттєві неточності, але самостійно виправив їх – 10 %.

2. Модульний контроль

Ваговий бал – 10.

Контрольна робота складається з 10 тестових завдань. За кожну вірну відповідь на запитання надається 1 бал.

Сума вагових балів контрольних заходів протягом семестру складає:

R= 60 + 40 = 100 балів.

Необхідною умовою допуску до заліку є зарахування усіх лабораторних робіт, а також стартовий рейтинг (r_c) не менше 40% від R, тобто 40 балів.

Сума балів переводиться до залікової оцінки згідно з таблицею:

Бали (RD)	Традиційна оцінка
95..100	Відмінно
85…94	Дуже добре
75…84	Добре
65…74	Задовільно
60…64	Достатньо
RD<=60	Незадовільно
RD < 40 або не виконані інші умови допуску до заліку	Не допущений

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль

1. *Істрія захисту інформації у Web-ресурсах. Методи захисту інформації Web-ресурсів.*
2. *Підсистема розмежування доступу. Підсистема антивірусного захисту Підсистема контролю цілісності. Підсистема виявлення вторгнень. Підсистема криптографічного захисту.*
3. *Оцінка вразливості архітектури Web-ресурсів.*
4. *Підходи проведення порівняння сучасних та ранніх версій додатків. REST API.*
5. *Поділ функцій клієнта та сервера.*
6. *Вбудовані в браузер інструменти аналізу.*
7. *Механізми аутентифікації.*
8. *Різновиди кінцевих точок. Клієнтські фреймворки. Фреймворки для односторінкових додатків,*
9. *Підробка міжсайтових запитів (CSRF).*
10. *Підробка параметрів запиту. CSRF-атака на кінцеві точки POST.*
11. *Відмова в обслуговуванні (DoS). ReDoS-атака. Распределенная DDoS-атака.*
12. *Протидія CRSF на рівні коду.*
13. *Протидія DoS-атакам.*
14. *Протидія атакам ReDoS.*
15. *Захист від логічних DoS-атак.*
16. *Захист від DDoS.*
17. *Пом'якшення DDoS-атак.*

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри ІПЗЕ, д.т.н., професор Гаврилком Є.В.

Ухвалено кафедрою ІПЗЕ (протокол № 1 від 2.07.2022 р.)

Погоджено Методичною комісією ННІАТЕ КПІ ім. Ігоря Сікорського [1] (протокол № ___ від _____.2022 р.)

1 Методичною радою університету – для загальноуніверситетських дисциплін.