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	4кредити, 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*

Програманавчальної дисципліни

1. Описнавчальної 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 інформації 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. Історія безпеки 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 АланаТ'юрінг та ДіллиНокса.Криптологічна бомба. Початок комп'ютерного злому. Історія всесвітньої павутини (theWorldWideWeb, WWW), що з'явилася у 1990-х, а її популярність почала стрімко зростати на початку 2000-х.

Основні поняття і аналіз загроз інформаційної безпеки. Основні поняття захисту інформації і інформаційної безпеки. Аналіз загроз інформаційної безпеки. Основні методи реалізації загроз інформаційної безпеки. Компоненти забезпечення безпеки інформаційної системи. Способи забезпечення комп'ютерної безпеки. Стандарти оцінки безпеки інформаційних систем. Загальні методи забезпечення інформаційної безпеки. Класифікація захисту сучасних операційних систем.

Розділ 2. 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 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». Аналіз API WEB-ресурсів. Виявлення сторонніх залежностейWeb-додатку. 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.

Аналіз кінцеві точки API і визначення вразливостей. Огляд коректності кодів на стороні клієнта (браузера). Захищеність процес керування структурою документа. Аналіз атак на зовнішні сутності XML-документа, ExternalEntity, XXE). Непряма XXE-атака. Атаки типу DoS,RDoS,DeDos.

Розділ 4. Захист Web-ресурсів.

Захист сучасних Web-додатків. Архітектура захищеного ПЗ. Глибокий аналіз коду. Пошук вразливостей. Аналіз уразливості. Управління вразливістю. Регресивне тестування. Заходи щодо зниження ризику. Прикладні техніки розвідки та нападу.

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 SecurityCheatsheet [Електронний ресурс]. – Режим доступу: https://html5sec.org.

AndrewHoffman .Web Application Security: Exploitationan dountermeasures for Modern WebApplications - :,2021.—336c.

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

McNab C. NetworkSecurityAssessment : Know Your Network, 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 tosecureserversandWebapplications. – ISBN-10: 1907117040.

Stuttard D., Pinto M. TheWebApplicaionHackers'sHandbook: FindingandExploitingSecurityFlaws. – ISBN-10: 1118026470.

Zalewski M. TheTangledWeb: A GuidetoSecuringModernWebApplications. – ISBN-10: 1593273886.

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. Безпека і стійкість Web- и охмарних систем. Практикум / О. М. Тарасюк, А. В. Горбенко; под ред. В. С. Харченко. – МОНУ, НАКУ. Н. Е. Жуковского «ХАІ», 2017. – 40 с.

Троян С. О. Захист інформаційних ресурсів: навчально-методичний посібник до курсу «Захист інформаційних ресурсів» / С. О. Троян. – Умань: [б. в.], 2022. – 120 с.

Навчальний контент

5. *Методика опанування навчальної дисципліни(освітнього компонента)*

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

Лекція 1.Історія безпеки Web-ресурсів.

Витоки хакерства. «Енігма», 1930-ті. Автоматизований злом шифру «Енігми», 1940-ті. Поява «бомби». Фрікінг, 1950-ті. Метод боротьби з фрикінгом, 1960-ті. Початок комп'ютерного злому, 1980-ті.

Лекція2.Методи захисту інформації Web-ресурсів.

Політика безпеки Web-ресурсів та серверів. 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.

Лекція 3. Оцінка вразливості Web-ресурсів.

Карта Web-ресурсів. Оцінка вразливості архітектури Web-ресурсів.

Лекція 4. Оцінка структури 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.

Лекція 5. Пошук субдоменів, що забезпечують роботу Web -ресурсу.

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

Лекція 6. Аналіз API Web- ресурсу

Виявлення кінцевої точки. Механізми аутентифікації. Різновиди кінцевих точок. Основні різновиди Спеціалізовані різновиди.

***Лекція 7. Виявлення сторонніх залежностейWeb -ресурсу**.*

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.

Лекція 8. Злам Web -ресурсу.

Синтез і аналіз мислення хакера. Застосування даних, отриманих у процесі розвідки.

Лекція 9. Підробка міжсайтових запитів (CSRF).

Підробка параметрів запиту. Зміна вмісту запиту GET. CSRF-атака на кінцеві точки POST

Лекція 10. Атака безпосередньо на об'єкт XML.

Непряма XXE-атака .Пряма XXE-атака опосередкована XXE-атака.

Лекція 11. Відмова в обслуговуванні (DoS).

ReDoS-атака. Розподілена DDoS-атака.

Розділ 4. ЗАХИСТ WEB-РЕСУРСІВ.

Лекція 12. Архітектура захищеного ПЗ.

Глибокий аналіз коду. Пошук уразливості. Аналіз уразливості. Управління вразливістю. Регресивне тестування. Заходи щодо зниження ризику. Прикладні техніки розвідки та нападу.

Лекція 13. Безпечна архітектура додатків.

Аналіз вимог до ПЗ. Аутентифікація та авторизація Протоколи SSL та TLS Захист облікових даних Хешування облікових даних. BCrypt PBKDF2 Двофакторна автентифікація Особисті дані та фінансова інформація. Пошукові системи

***Лекція 14. Виявлення вразливостей WEB додатку**.*

Автоматизована перевірка. Статичний аналіз. Динамічний аналіз. Регресійне тестування. Програми відповідального розкриття інформації. Програми BugBounty. Сторонні пентестери.

Лекція 15. Управління вразливістю виявлених у WEB додатках.

Відтворення вразливостей. Класифікація вразливостей. Загальна система оцінки вразливостей. CVSS: Базова метрика. Вектор атаки. Складність доступу. Взаємодія з користувачем. Вплив на конфіденційність. Вплив на цілісність. Вплив на цілісність. CVSS: Тимчасова метрика. CVSS: Контекстна метрика. Удосконалена класифікація вразливостей.

Лекція 16. Захист від CSRF.

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.

Лекція 17. Протидія DoS-атакам.

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

Лекція 18. Захист ресурсів шляхом застосування блокчен технологій.

Шифрування SHA256 (384, 512)Secure Hashing Algorithm. Геш із файлу з ключем. Типове значення системи, ASCII, Unicode, Big-endian Unicode, UTF-8. Винятки. Підведення підсумків

Лабораторні роботи

№ з/п	Назва практичної роботи	Кількість ауд. годин
1	Розділ 2 Лабораторна №1. Методи та засоби виявлення уразливостей та забезпечення безпеки Web-ресурсів	6

2	*Розділ 3:* *Лабораторна 2. Пошук вразливості Web-ресурсу*	*6*
3	*Розділ 4:* *Лабораторна 3. Особливості криптографії у віртуальних системах*	*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.Підробкаміжсайтових запитів (CSRF). Підробка параметрів запиту. Зміна вмісту запиту GET. CSRF-атака на кінцеві точки POST. Відмова в обслуговуванні (DoS). ReDoS-атака. РаспределеннаяDDoS-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

6. Політика навчальної дисципліни (освітнього компонента)

Для успішного проходження курсу та складання контрольних заходів необхідним є вивчення навчального матеріалу за кожною темою. Специфіка курсу передбачає акцент на розумінні підходів і принципів, отримання практичних навичок, а не просто запам'ятовування визначень. Кожен студент повинен ознайомитися і слідувати Положенню про академічну доброчесність, Статуту і розпорядку дня університету. Для успішного засвоєння програмного матеріалу студент зобов'язаний:

– не запізнюватися на заняття;

– не пропускати заняття, а в разі пропуску відновити за допомогою консультування з викладачем та з використанням конспекту на платформі дистанційного навчання «Сікорський», самостійно вивчити матеріал пропущеного заняття та скласти відповідні контрольні заходи в індивідуальному порядку;

– конструктивно підтримувати зворотній зв'язок на всіх заняттях;
– брати активну участь у освітньому процесі;
– своєчасно і старанно виконувати завдання для самостійної роботи;
– бути доброзичливим до однокурсників та викладачів;
– брати участь у контрольних заходах;
– за об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись індивідуально (в дистанційній online формі за погодженням із деканом факультету);
– будь-яке копіювання або відтворення результатів чужої праці (у тому числі списування), якщо тільки робота не має груповий формат, використання чужих завантажених з Інтернету матеріалів кваліфікується як порушення норм і правил академічної доброчесності та передбачає притягнення винного до відповідальності, у порядку, визначеному чинним законодавством та Положенням про академічну доброчесність університету. Результатом невиконання та/або недотримання правил може бути оцінка «не зараховано» за курс.
Система вимог, які викладач ставить перед студентом:
- Кодекс честі: http://kpi.ua/code;
- Правила внутрішнього розпорядку: http://kpi.ua/admin-rule;
- Положення про організацію освітнього процесу в КПІ ім. Ігоря Сікорського: https://kpi.ua/regulations.

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

***Поточний контроль**: тестування або експрес опитування, МКР, виконання завдань до практичних занять.*
***Календарний контроль**: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.*
***Семестровий контроль:** залік.*
***Умови допуску до семестрового контролю**: семестровий рейтинг більше 40 балів.*
Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше 60	Незадовільно
Менше 30	Не допущено

Загальна рейтингова оцінка студента після завершення семестру складається з балів, отриманих за:
- *тестування або експрес опитування полекційним заняттям;*
- *виконання завдань до практичних занять;*
- *виконання модульної контрольної роботи (МКР);*
- *виконання і захист індивідуального домашнього завдання;*
- *виконання додатковий завдань.*

Тестування (або експрес опитування)по лекціям	Практичні заняття	МКР	Захист індивідуального домашнього завдання	Додаткові бали

18	27	15	40	10

Тестування (або експрес опитування) по матеріалам лекційних занять

Ваговий бал - 1. *Максимальна кількість балів за тестування – 1 бал * 18 лекцій = 18 балів.*

Тестування може проводиться за допомогою систем дистанційного навчання, наприклад Moodle, яке доступне протягом 2 робочих днів після завершення поточної лекції. У деяких випадках термін проходження тестування може бути продовжений лектором. Тривалість проходження одного тестування – 10 хвилин. Кількість спроб – одна. У деяких випадках, що пов'язані з технічними проблемами студентів, може надатися повторна спроба на окремі тестування.

Кожне тестування містить 10 запитань різного формату (вибір правильного варіанту з переліку; вірно/невірно; визначити відповідність; чисельна відповідь; вибір пропущених слів; перетаскування на зображення тощо).

Критерії оцінювання

- запитання типу «вибір правильного варіанту з переліку», «вірно/невірно», «чисельна відповідь» оцінюються однозначно: вірна відповідь – 0,1 бал, невірна відповідь – 0 балів;

- запитання, на які немає однієї конкретної відповіді, типу «визначити відповідність», «вибір пропущених слів», «перетаскування на зображення» оцінюються у відповідності до кількості елементів у тесті (наприклад, якщо треба вставити 4 слова у текст, то студент отримає по 0,025 балів за одне правильне вставлене слово, а за всі 4 правильно вставлені слова отримає відповідно 0,1 бал) – невірна відповідь – 0 балів, частково вірна відповідь – 0,01-0,09 балів, вірна відповідь 0,1 бал.

Практичні заняття

Ваговий бал –3*. Максимальна кількість балів за всі практичні заняття – 3 бали * 9 занять= 27балів.*

На практичних занять студенти разом із викладачем розв'язують завдання за тематикою практичного заняття. Після кожного практичного заняття студенти отримують домашнє завдання, яке необхідно вирішити та надати на перевірку викладачу до початку наступного заняття (зазвичай це 2 тижні, однак іноді цей час може бути змінений викладачем у деяких конкретних випадках).

Перше практичне заняття, зазвичай, поводиться коли лекційний матеріал ще не начитаний, тому його тематика не пов'язана з конкретними темами дисципліни, а направлена на перевірку логічного мислення студентів та можливості інтуїтивно, без знать методів синтезу, складати схеми для простих логічних задач.

Критерії оцінювання

- домашнє завдання вирішено вірно та здано протягом 2-х тижнів після практичного заняття – 3 бали;

- домашнє завдання вирішено вірно, але здано протягом більш ніж 2-х тижнів після практичного заняття – 2,5 бал;

- домашнє завдання вирішено із незначними помилками та здано протягом 2-х тижнів після практичного заняття – 2 бали;

- домашнє завдання вирішено із незначними помилками та здано протягом більш ніж 2-х тижнів після практичного заняття – 1,5 балів;

- домашнє завдання вирішено із значними помилками – повертається на доопрацювання.

Модульна контрольна робота

Ваговий бал МКР – 15*. Максимальний бал за МКР складає 15 балів.*

На модульній контрольній роботі студент має виконати 3 завдання. Завдання оцінюються від 0 до 5 балів в залежності від правильності вирішення.

Критерії оцінювання

- завдання вирішено вірно та здано протягом 2-х тижнів після практичного заняття – 5 бали;

- завдання вирішено вірно, але здано протягом більш ніж 2-х тижнів після практичного заняття – 4 бал;

- завдання вирішено із незначними помилками та здано протягом 2-х тижнів після практичного заняття – 3 бали;

- завдання вирішено із незначними помилками та здано протягом більш ніж 2-х тижнів після практичного заняття – 2 балів;

- домашнє завдання вирішено із значними помилками – повертається на доопрацювання.

Захист індивідуального домашнього завдання (презентація).

Ваговий бал – 40*. Максимальний бал за захист індивідуального домашнього завдання (презентація) складає 40 балів.*

Студент представляє презентацію проєкту політики системи управління якістю по своїй магістерській дисертації.

Критерії оцінювання

1. Рейтинг захисту Rз = 35 - 40 балів – повністю виконані всі завдання, своєчасно оформлено та представлено супровідну пояснювальну записку. При захисті грамотно та логічно послідовно викладено основні положення роботи у вигляді доповіді, в процесі відповідей на питання продемонстрував наявність глибоких вичерпних знань, або твердих та достатньо повних знань.

2. Рейтинг захисту Rз = 30 - 35 балів – відповідаючи на питання під час презентаціївласної роботи, здобувач припускається окремих помилок, але може їх виправити за допомогою викладача, знає визначення основних понять і величин, впевнено орієнтується в своїй роботі.

3. Рейтинг захисту Rз = 25 - 30 балів – здобувач відповідає майже на всі питання під час презентаціївласної роботи. Відповіді іноді непослідовні та нечіткі. Своєчасно оформив та представив презентацію власного проєкту.

4. Рейтинг захисту Rз = 20 - 25 балів – здобувач частково відповідає на всі питання під час презентаціївласної роботи, показує знання, але не впевнено орієнтується в своїй роботі. Відповіді непослідовні та нечіткі. Не своєчасно оформив та представив презентацію власного проєкту.

5. Рейтинг захисту Rз = 15 – 20 балів – здобуваччастково відповідає на деякі питання під час презентаціївласної роботи, показує незадовільні знання. Відповіді непослідовні та нечіткі. Не своєчасно оформив та представив презентацію власного проєкту.

6. Рейтинг захисту Rз< 20 балів – у відповіді здобувач припускається суттєвих помилок, не може виправити помилки за допомогою викладача. Відповіді некоректні, а в деяких випадках не відповідають суті поставленого питання. Не своєчасно оформив та представив презентацію власного проєкту.

Додаткові (бонусні) бали

Рейтинговою системою оцінювання передбачені додаткові бали за виконання додаткових завдань. Один студент не може отримати більше ніж 10 бонусних балів у семестрі. При отриманні більш ніж 10 балів, вони обмежуються на рівні 10. Бонусні бали можуть бути отримані за такі види робіт: «Івенти», «Додаткові лекції» та «Завдання до лекцій».

Івенти. *Івенти - це спеціальні події для студентів, які хочуть отримати додаткові бали за вирішення ускладнених завдань. Івенти активуються у визначений час і активні обмежений час. Додаткові бали отримують тільки ті студенти, які надали правильну відповідь вчасно її завантажили. Кількість балів за додаткові завдання визначає кожен івент окремо. Один студент не може отримати більш ніж 10 балів за івенти.*

Додаткові лекції*. Самостійна робота студентів передбачає до 10 додаткових лекцій, які студенти повинні опрацювати та законспектувати. За опрацювання однієї лекції вигляді у конспекту нараховується 1 бал. Максимальна кількість балів, що можна отримати за опрацювання додаткових лекції складає 5 балів.*

Завдання до лекцій. *Студенти, за бажанням, можуть виконувати додаткові завдання за матеріалами лекцій (розв'язати приклад, зробити доповідь тощо). За одне додаткове завдання нараховується 0,5 бали. Максимальна кількість балів, що можна отримати за завдання до лекцій складає 5 балів.*

Форма семестрового контролю – залік

Максимальна сума балів складає 100. Необхідною умовою допуску до заліку є зарахування всіх домашніх робіт та робота на практичних заняттях.Для отримання заліку з кредитного модулю «автоматом» потрібно мати рейтинг не менше 60 балів, а також виконані умови допуску до заліку.

Здобувачі, які наприкінці семестру мають рейтинг менше 60 балів, а також ті, хто хоче підвищити свою оцінку в системі ECTS, виконують залікову контрольну роботу. При цьому набрані бали студентом анулюються, а оцінка за залікову контрольну роботу є остаточною.

Залікова робота. *Залікова робота проводиться на останньому лекційному занятті. Здобувач проходить тестування очного або у середовищі дистанційного навчання, наприклад Moodle. На тестування пропонується 100 тестових, кожне з яких оцінюється в 1 бал. Для отримання позитивної оцінки необхідно набрати 60 балів і вище. Час тестування зазвичай складає 100 хвилин, але може бути скоригований лектором та (або) викладачам, що приймає залік.*

9. Додаткова інформація з дисципліни (освітнього компонента)

Вимоги до спеціального матеріально-технічного та/або інформаційного забезпечення:

Наявність діючих облікових записів: Користувача на Платформі дистанційного навчання "Сікорський" та Сервісів Google;

Вимоги до мережевої інфраструктури: достатні для отримання доступу до https:// google.com/ та https://do.ipo.kpi.ua.

Операційна система: не специфікується;

Інтернет браузер: не специфікується;

Текстовий редактор: не специфікується;

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. РаспределеннаяDDoS-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 інженерії програмного забезпечення в енергетиці НН ІАТЕ, д.т.н., проф., Гаврилком Євгеном Володимировичем*

***Ухвалено** кафедрою інженерії програмного забезпечення в енергетиці НН ІАТЕ(протокол № 28 від 15.05.2023 р.)*

***Погоджено** Методичною комісією НН ІАТЕ (протокол № 9 від 26.05.2023 р.)*