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

Кафедра інженерії програмного забезпечення в енергетиці (ІПЗЕ)

Методи і засоби забезпечення безпеки бездротових, мобільних та хмарних технологій

Робоча програма навчальної дисципліни

(Силабус)

Реквізитинавчальної дисципліни

Рівень вищої освіти	другий (магістерський)
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

Сьогодні все більше користувачів надають перевагу бездротовим, мобільним мережам, що міцно посіли важливе місце в нашому житті та зберіганню та обробки інформації на удаленних серверах хмарного середовища. Вони дозволяють отримати широкосмуговий доступ до мережі Інтернет, дають можливість обміну файлами у локальній мережі, не застосовуючи кабелі передачі даних. Перебуваючи в громадському місці чи в колі друзів, багато хто починає шукати найближчу точку доступу Wi-Fi, ні на хвилину не замислюючись про питання безпеки при користуванні бездротовими мережами. Слабке уявлення користувачів про загрози дозволяють зловмиснику отримати доступ до інформації користувачів, адже завдяки особливостям середовища передачі бездротові мережі не можуть забезпечити розмежування доступу до даних, тому пакети, що передаються клієнтом або точкою доступу, можуть бути отримані будь-яким пристроєм в зоні дії мережі.

Захист інформації та кібербезпека формують окремі важливим напрями діяльності спеціалістів ІТ, інженерів з програмного забезпечення. Вивчення вибіркової дисципліни «Методи і засоби забезпечення безпеки бездротових, мобільних та хмарних технологій (БМХТ)» присвячене різним підходам захисту інформації та забезпечення безпеки бездротових, мобільних і хмарних-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 бездротових, мобільних і хмарних-ресурсів.

Завдання. Основними завданнями вивчення дисципліни ««Методи і засоби забезпечення безпеки бездротових, мобільних та хмарних технологій»» є отримання студентом компетенцій для того, щоб приймати участь у проектуванні інформаційних систем, розглянуті загальні питання захисту інформації під час передавання в бездротових, мобільних і хмарних серверних технологій. Наведені приклади зламування шифросистем. Значна увага приділяється автентифікації, підпису, який підтверджує дійсність і цілісність документа.

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 у бездротових, мобільних та хмарних системах накопичення, зберіганні і передавання інформації.

3. Зміст навчальної дисципліни

Розділ 1. Історія безпеки бездротових, мобільних та хмарних технологій (БМХТ).

Короткий огляд історії безпеки програмного забезпечення. Розглянути передісторію витоків хакерства. 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. Організація мереж в БМХТ.

Методи оцінки вразливостей Wi-Fi; бездротові мережі; шифрування, автентифікація, точка доступу, мережеве обладнання, WEP, WPA, WPA2, WPS, WDS дозволяють розуміти особливості ураження інформаційних ресурсів.

Розділ 3. Методи зламу в БМХТ.

БМХЗ будуть мати розвиток та зростаючий трафік у цих мережах, може призвести до безлічі інцидентів інформаційної безпеки, наприклад: розголошення конфіденційної або внутрішньоїінформації; несанкціонований доступ до інформації;вірусна атака; компрометація облікових записів; перевищення повноважень; моніторинг інформаційної системи;атаки на мережеве обладнання та інше.

Розділ 4. Захист інформації в БМХТ.

Механізми захисту мереж БМХТ передбачають автентифікацію (клієнт та точка доступу представляються один одному і підтверджують права на обмін даними) та шифрування (обрання алгоритму шифрування інформації та даних, що передаються по бездротовій мережі, генерація та зміна ключів).

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 .WebApplicationSecurity: Exploitationandountermeasuresfor ModernWebApplications, - :,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 tosecureserversandWebapplications. – ISBN-10: 1907117040.

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

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

Джонсон Дэн Берг, ДеоганДэниел, СаванoДэниел /Безопасноbydesign/. — 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 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. ІСТОРІЯ БЕЗПЕКИ БЕЗДРОТОВИХ, МОБІЛЬНИХ ТА ХМАРНИХ ТЕХНОЛОГІЙ (БМХТ).
Лекція 1.1. Історія безпеки бездротових мобільних технологій.
Лекція 1.2.Методи захисту інформації хмарних технологій і серверів.
Розділ 2. ОРГАНІЗАЦІЯ МЕРЕЖ В БМХТ.
Лекція 2.1. Організація і особливості комп'ютерних мереж.
Лекція 2.2. Організація мобільних мереж.
Лекція 2.3. Організація бездротових мереж.
Лекція 2.4. Організація розполдіду інформації в хмарі. Біг дата
Розділ 3. МЕТОДИ ЗЛАМУ В БМХТ.
Лекція 3.1. Злам мобільних мереж.
Синтез і аналіз мислення хакера. Застосування даних, отриманих у процесі розвідки.
Лекція 3.2. Злам бездротових мереж
Підробка параметрів запиту. Зміна вмісту запиту GET. CSRF-атака на кінцеві точки POST
Лекція 3.3. *Вплив на хмарні технології.*
Лекція 3.4. *Особливості атак на хмарні технології.*
Розділ 4. ЗАХИСТ ІНФОРМАЦІЇ В БМХТ.
Лекція 4.1. Методи автентифікації клієнтів.
Лекція 4.2.Wi-Fi Protected Access 1 та Wi-Fi Protected Access 2.
Лекція 4.3. Методи шифрування даних.
Лекція 4.4. Вразливості протоколів інфокомунакаціних мереж.

6. Самостійна робота студента

1. **Розділ 2. ОРГАНІЗАЦІЯ МЕРЕЖ В БМХТ.**
2. **Розділ 3. МЕТОДИ ЗЛАМУ В БМХТ.**
3. **Розділ 4. ЗАХИСТ ІНФОРМАЦІЇ В БМХТ.**

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. Розробити технологію віддаленого виклику типу GRPC.процедур .	10
Завдання №2. Робота з брокерами повідомлень.	10
Завдання №3. На основі створеної **GRPC** *розробити децентралізовану систему.*	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 %.

<u>2. Модульний контроль</u>

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

Робочу програму навчальної дисципліни (силабус):

Складенопрофесором 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.