Силабус освітнього компонента
Програма навчальної дисципліни

Безпека систем Клієнт-Сервер

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Спеціальна (фахова) підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
1

Мова викладання
Українська, англійська

Викладачі, розробники

ДУНАЄВ Сергій Владиславович

Serhii.Dunaiev@cs.khpi.edu.ua
Асистент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: 5, з них 3 статті, що реферуються у науково метричних базах Scopus. Лектор з дисциплін: "Веб-програмування" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та

магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Система Клієнт-Сервер є основою сучасних інформаційних технологій, що використовуються в різноманітних сферах. Цей курс досліджує принципи та методи забезпечення безпеки в системах Клієнт-Сервер. Студенти вивчатимуть загрози, уразливості, а також сучасні технології і підходи для захисту даних, які передаються між клієнтом і сервером.

Мета та цілі дисципліни

Метою курсу полягає у формуванні у студентів знань і навичок, необхідних для розробки, реалізації та управління безпекою систем Клієнт-Сервер. Студенти зможуть ідентифікувати загрози, застосовувати методи захисту і виконувати аналіз безпеки інформаційних систем.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
КЗ–2. Здатність проводити дослідження на відповідному рівні.
КЗ–4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Безпека безперервності бізнес-процесів.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Введення в системи Клієнт–Сервер. Огляд архітектури клієнт–серверних систем, їхніх компонентів і принципів взаємодії. Типи клієнт–серверних моделей (2-tier, 3-tier, n-tier), роль серверів додатків, баз даних і клієнтів у забезпеченні продуктивності та безпеки.	6
Тема 2. Основи безпеки інформації. Основні поняття та принципи інформаційної безпеки: конфіденційність, цілісність, доступність. Загрози та вразливості клієнт–серверних систем. Моделі управління безпекою та політики захисту даних.	6
Тема 3. Аутентифікація та авторизація. Методи перевірки особи користувача (паролі, токени, біометрія, двофакторна аутентифікація). Механізми авторизації в мережевих системах (ACL, RBAC, OAuth, Kerberos). Забезпечення контролю доступу до серверних ресурсів.	6
Тема 4. Шифрування даних. Використання криптографічних методів для захисту інформації під час передавання і зберігання. Симетричні та асиметричні алгоритми шифрування (AES, RSA). Використання SSL/TLS для безпечного з'єднання між клієнтом і сервером.	6
Тема 5. Захист від атак на систему. Види атак на клієнт–серверні системи: SQL-ін'єкції, XSS, CSRF, DDoS, MITM. Методи виявлення та запобігання атакам. Налаштування міжмережевих екранів, IDS/IPS-систем, захист API.	4
Тема 6. Моніторинг та аудит безпеки. Принципи моніторингу подій безпеки, логування дій користувачів та адміністраторів. Використання систем SIEM для аналізу інцидентів. Аудит безпеки та тестування на проникнення як інструменти підвищення захищеності клієнт–серверних систем.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a

Тема 1. Налаштування базової системи Клієнт–Сервер. Ознайомлення з архітектурою клієнт–серверних систем. Розгортання серверної частини, підключення клієнтів, налаштування мережевої взаємодії та перевірка працездатності системи.	4	0,2
Тема 2. Аутентифікація користувачів. Налаштування механізмів аутентифікації користувачів у клієнт–серверному середовищі. Використання паролів, токенів і сертифікатів для підтвердження особи користувача.	4	0,2
Тема 3. Шифрування даних. Реалізація симетричного і асиметричного шифрування. Захист даних при передачі через мережу. Практичне впровадження алгоритмів симетричного (AES) та асиметричного (RSA) шифрування. Налаштування захищених каналів зв'язку (SSL/TLS) для передачі даних між клієнтом і сервером.	2	0,1
Тема 4. Виявлення атак. Налаштування системи виявлення вторгнень. Проведення атак та вивчення їх наслідків. Ознайомлення з інструментами моніторингу безпеки. Налаштування IDS/IPS систем для виявлення вторгнень. Моделювання типових атак (наприклад, DoS, SQL Injection) та аналіз їхнього впливу на систему.	2	0,1
Тема 5. Захист веб-додатків. Дослідження вразливостей веб-додатків і методів їх усунення. Налаштування міжмережевого екрану та застосування механізмів фільтрації запитів для запобігання XSS, CSRF і SQL-ін'єкціям.	2	0,1
Тема 6. Аудит і моніторинг безпеки. Проведення аудиту безпеки клієнт–серверної інфраструктури. Аналіз журналів подій, моніторинг мережевого трафіку та створення звітів щодо виявлених загроз і рекомендацій із підвищення рівня безпеки.	2	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Архітектура та механізми безпеки клієнт–серверних систем. Розгляд архітектури клієнт–серверних систем, основних типів взаємодії та протоколів передачі даних. Аналіз ключових принципів інформаційної безпеки — конфіденційності, цілісності та доступності. Дослідження типових загроз, ризиків та методів захисту серверів і клієнтів у мережевому середовищі.	0,1
Тема 2. Аутентифікація, авторизація та криптографічний захист даних у клієнт–серверних системах. Вивчення методів і протоколів аутентифікації та авторизації користувачів (Kerberos, OAuth, LDAP). Розгляд застосування криптографічних алгоритмів для шифрування переданих даних (SSL/TLS, RSA, AES). Аналіз практичних засобів захисту від атак типу «людина посередині» (MITM) та забезпечення цілісності даних у процесі клієнт–серверної взаємодії.	0,1

Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Архітектура клієнт–серверних систем: моделі та принципи взаємодії. Вивчення типів архітектур (2-tier, 3-tier, multi-tier), їх переваг та недоліків у контексті безпеки.	8
Тема 2. Методи захисту мережевих протоколів TCP/IP. Аналіз уразливостей мережевих протоколів і способів їх захисту за допомогою фаєрволів, VPN і шифрування.	8
Тема 3. Використання SSL/TLS у клієнт–серверних системах. Розгляд принципів створення захищених каналів зв'язку, генерація та використання сертифікатів.	7
Тема 4. Контроль доступу в клієнт–серверних системах. Моделі контролю доступу: DAC, MAC, RBAC. Практичні підходи до реалізації політик безпеки.	7
Тема 5. Захист баз даних у клієнт–серверній архітектурі. Методи шифрування, контроль доступу до баз даних, аудит SQL-запитів і захист від ін'єкцій.	7
Тема 6. Інцидент-менеджмент у клієнт–серверному середовищі. Розгляд процесів виявлення, реагування та усунення інцидентів безпеки. Формування звітів і аналіз журналів подій.	7
Тема 7. Використання криптографічних бібліотек у програмуванні. Огляд інструментів для реалізації шифрування та аутентифікації (OpenSSL, Crypto++, PyCryptodome).	7
Тема 8. Засоби резервного копіювання та відновлення даних у клієнт–серверних системах. Методи створення резервних копій, політики відновлення після збоїв і катастроф.	7
Тема 9. Захист серверів додатків і API. Методи запобігання несанкціонованому доступу до API, обмеження запитів і використання токенів безпеки (OAuth, JWT).	7
Тема 10. Трендові технології забезпечення безпеки клієнт–серверних систем. Zero Trust Architecture, багатофакторна аутентифікація (MFA), контейнеризація (Docker Security), ізоляція середовищ.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «Endpoint Security»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. James Kurose, Keith Ross, Computer Networking: A Top-Down Approach. https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20_%20A%20Top%20Down%20Approach,%207th,%20converted.pdf
2. Pradeep Gohil, Web Security Testing Cookbook. https://www.redbooks.ibm.com/redbooks/pdfs/sg248411.pdf.
3. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. https://books.google.com.ua/books?id=eo4Otm_TcW8C&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

Додаткова література

4. William Stallings , Cryptography and Network Security: Principles and Practice. https://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf.
5. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.
https://edu.anarcho-copy.org/Against%20Security%20-%20Self%20Security/Dafydd%20Stuttard,%20Marcus%20Pinto%20-%20The%20web%20application%20hacker's%20handbook_%20finding%20and%20exploiting%20security%20flaws-Wiley%20(2011).pdf.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, K, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Ольга КОРОЛЬ