Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра «Комп'ютерних систем, мереж і кібербезпеки» (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми


_____ Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

«_29_» ____серпня____2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

____Захист інформації в інформаційно-комунікаційних системах_____
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: 125 «Кібербезпека»
(код і найменування спеціальності)

Освітня програма: «Безпека інформаційних і комунікаційних систем»____
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): __Андрій Карпенко, ст. викладач, д-р філософії_ _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри _____
__комп’ютерних систем, мереж і кібербезпеки_____
(назва кафедри)

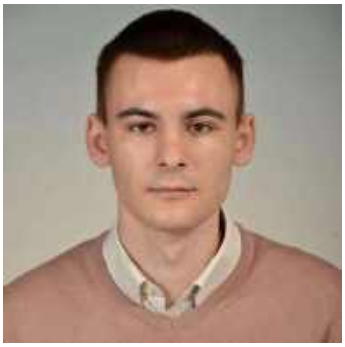
Протокол № 1 від « 29» серпня 2025 р.

Завідувач кафедри д.т.н., професор _____ _Вячеслав Харченко___
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК_____
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача



ПІБ: Карпенко Андрій Сергійович

Посада: старший викладач

Науковий ступінь: Ph.D.

Вчене звання: відсутнє

Перелік дисциплін, які викладає:
захист інформації в комп'ютерних мережах, теоретичні основи криптології, управління інформаційною безпекою, теорія та технології розробки безпечних розподілених систем.

Напрями наукових досліджень:
хмарні технології, кібербезпека, тестування програмного забезпечення.

Контактна інформація:
a.karpenko@csn.khai.edu, +380507095250

2. Опис навчальної дисципліни

Форма здобуття освіти	*денна*
Семестр	7-й
Мова викладання	Українська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна*: 4.5 кредитів ЄКТС / 135 годин (64 аудиторних, з яких: лекції – 32, лабораторні – 32; СРЗ – 71);
Види навчальної діяльності	Лекції, лабораторні заняття, розрахункова робота, самостійна робота.
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит.
Пререквізити	Операційні системи, прикладна криптологія, інформаційно-комунікаційні системи

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – ознайомлення тих, хто навчається, з методологією, основними напрямами, методами і алгоритмами реалізації функцій захисту інформації від руйнівних програм в інформаційних та комунікаційних системах, а також придбанні навичок розробці та використання стеганографічних алгоритмів щодо забезпечення захисту інформації.

Завдання – знати сучасні міжнародні та вітчизняні стандарти з інформаційної безпеки; знати загальні аспекти проблематики в галузі захисту інформації в інформаційно-комунікаційних системах, а також тенденції і перспективи розвитку механізмів захисту інформації та засоби подолання цих механізмів; розуміти властивості інформаційних ресурсів та технологій як об'єктів кібербезпеки, та вміння здійснювати класифікацію загроз безпеці інформаційних ресурсів, класифікацію та ранжирування джерел загроз і вразливостей безпеки, застосовуючи системний підхід та знання основ теорії інформаційної безпеки; розуміти принципи і методи теорії захищених систем, основних механізмів захисту, які реалізовані в сучасних операційних системах та системах управління базами даних, видів і прийомів використання шкідливого програмного забезпечення та методів його нейтралізації; знати методи та засоби захисту інформації в комп'ютерних мережах, включаючи технології міжмережних екранів, систем виявлення та запобігання вторгненням, віртуальних приватних мереж; розуміти принципи побудови стеганографічних систем та методи приховування інформації в різних типах носіїв.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(ЗК1) здатність застосовувати знання у практичних ситуаціях.

(ЗК2) знання та розуміння предметної області та розуміння професії.

(ЗК3) здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

(ЗК4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

(ЗК5) здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(КФ4) здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

(КФ5) здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

(КФ6) здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

(КФ7) здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

(КФ8) здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

(КФ9) здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

(КФ11) здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

(КФ12) здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання:

(ПРН1) застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

(ПРН2) організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

(ПРН3) використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

(ПРН4) 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.

(ПРН5) адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

(ПРН7) діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

(ПРН8) готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

(ПРН9) впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

(ПРН10) виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

(ПРН11) виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

(ПРН12) розробляти моделі загроз та порушника.

(ПРН14) вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

(ПРН18) використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

(ПРН19) застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

(ПРН20) забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

(ПРН27) вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

(ПРН31) застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

(ПРН34) приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

(ПРН50) забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

(ПРН51) підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

(ПРН53) вирішувати задачі аналізу програмного коду на наявність можливих загроз.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Базові технології та інфраструктурна безпека

Тема 1. Мережі та протоколи в кібербезпеці

Анотація: Розглядаються основи мережевої безпеки, модель OSI як карта атак, протоколи стеку TCP/IP та їх вразливості. Вивчаються мережеві атаки на кожному рівні OSI моделі, методи їх виявлення та захисту.

*Тема лекції 1***:** Мережева модель OSI як архітектура атак. Вразливості на кожному рівні: фізичні атаки, ARP poisoning, IP spoofing, SYN flood, session hijacking, атаки на рівень застосувань.

*Тема лекції 2***:** Основні протоколи стеку TCP/IP та їх безпека. Аналіз мережевого трафіку за допомогою Wireshark. Сканування мережі (nmap). Механізми захисту мережевої інфраструктури.

Тема лабораторного заняття 1: Дослідження мережевого трафіку за допомогою Wireshark. Аналіз протоколів та виявлення аномалій. Сканування мережі інструментом nmap.

Самостійна робота здобувачів: Вивчення методів DDoS атак та механізмів захисту. Аналіз реальних випадків мережевих атак (Target 2013, Mirai Botnet 2016). Дослідження інструментів мережевого моніторингу.

Тема 2. Віртуалізація та архітектура комп'ютерів у кібербезпеці

Анотація: Вивчаються принципи віртуалізації, типи гіпервізорів та їх вразливості. Розглядаються атаки на віртуальні середовища (VM Escape, Hyperjacking), безпека контейнерів Docker та Kubernetes. Аналізуються апаратні атаки (Meltdown, Spectre) та механізми захисту.

Тема лекції 3: Віртуалізація в кібербезпеці. Типи гіпервізорів (Type 1, Type 2). Атаки на віртуальні середовища: VM Escape, Hyperjacking, Side-channel attacks. Форензіка віртуальних машин.

Тема лекції 4: Container security та безпека Docker/Kubernetes. Апаратна безпека: атаки Meltdown, Spectre, Foreshadow. Hardware Security Modules, Trusted Computing та TPM.

Тема лабораторного заняття 2: Налаштування ізольованого віртуального середовища для аналізу шкідливого ПЗ. Дослідження безпеки контейнерів Docker.

Самостійна робота здобувачів: Аналіз вразливостей гіпервізорів VMware, Hyper-V, KVM. Вивчення механізмів ізоляції контейнерів. Дослідження апаратних модулів безпеки TPM.

Тема 3. Операційні системи та безпека

Анотація: Розглядаються принципи роботи та архітектура операційних систем з точки зору кібербезпеки. Вивчаються механізми контролю доступу, автентифікації та авторизації в Windows, Linux та macOS. Аналізуються атаки на ОС та методи захисту.

Тема лекції 5: Архітектура операційних систем та механізми безпеки. Управління процесами та пам'яттю. Файлові системи та безпека. Моделі контролю доступу (DAC, MAC, RBAC).

Тема лекції 6: Атаки на операційні системи: руткіти, експлойти, переповнення буферу. Атаки на парольний захист. Безпека Windows (UAC, Defender), Linux (SELinux, AppArmor), macOS (Gatekeeper, SIP).

Тема лабораторного заняття 3: Дослідження атаки типу "переповнення буферу" та методів протидії. Налаштування механізмів захисту операційних систем.

Самостійна робота здобувачів: Аналіз механізмів захисту від експлойтів (ASLR, DEP, Stack Canaries). Дослідження методів підвищення привілеїв в ОС. Порівняльний аналіз безпеки Windows та Linux.

Тема 4. Бази даних та безпека

Анотація: Вивчаються архітектура баз даних як критична ціль для атак. Детально розглядаються SQL Injection атаки різних типів та методи захисту. Аналізуються ACID властивості, шифрування даних, backup стратегії та моніторинг БД.

Тема лекції 7: Архітектура баз даних та вектори атак. SQL Injection: типи атак (Union-based, Error-based, Blind, Time-based). Реальні випадки атак на БД (Equifax, Heartland). **Тема лекції 8:** Захист баз даних: параметризовані запити, WAF, принцип найменших привілеїв. ACID властивості та їх значення для

безпеки. Шифрування даних (TDE, Column-level). Backup стратегії та моніторинг.

Тема лабораторного заняття 4: Дослідження SQL Injection атак на тестовому середовищі. Налаштування захисту бази даних та аудит безпеки.

Самостійна робота здобувачів: Аналіз вразливостей NoSQL баз даних. Вивчення методів захисту від SQL Injection (OWASP рекомендації). Дослідження інструментів автоматизованого тестування БД на вразливості.

Модульний контроль 1

МОДУЛЬ 2
Змістовний модуль 1. Практична кібербезпека та реагування на інциденти

Тема 5. Криптографія та безпека

Анотація: Вивчаються основи криптографії та її застосування в кібербезпеці. Розглядаються симетричне та асиметричне шифрування, хешування, цифрові підписи. Аналізуються криптографічні протоколи (TLS, SSH) та атаки на криптосистеми.

Тема лекції 9: Основи криптографії. Симетричне шифрування (AES, DES). Асиметричне шифрування (RSA, ECC). Хешування та цифрові підписи (SHA, MD5).

Тема лекції 10: Криптографічні протоколи (TLS/SSL, SSH, VPN). Атаки на криптографію (Brute force, Man-in-the-Middle, Padding Oracle). Квантова криптографія та постквантові алгоритми.

Тема лабораторного заняття 5: Дослідження криптографічних алгоритмів та протоколів. Аналіз TLS з'єднань. Практика використання OpenSSL.

Самостійна робота здобувачів: Аналіз вразливостей криптографічних протоколів (Heartbleed, POODLE, BEAST). Вивчення принципів PKI та управління сертифікатами. Дослідження методів шифрування даних у хмарних сервісах.

Тема 6. Веб-безпека та захист додатків

Анотація: Розглядаються вразливості веб-додатків за класифікацією OWASP Top 10. Вивчаються атаки XSS, CSRF, Broken Authentication, Insecure Deserialization. Аналізуються методи захисту веб-додатків та інструменти тестування.

Тема лекції 11: OWASP Top 10 вразливості: Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration.

Тема лекції 12: XSS атаки (Stored, Reflected, DOM-based), CSRF, Insecure Deserialization. Secure Development Lifecycle (SDLC). WAF та інструменти захисту. Bug bounty програми.

Тема лабораторного заняття 6: Дослідження веб-вразливостей на платформі OWASP WebGoat. Тестування веб-додатків на вразливості за допомогою Burp Suite.

Самостійна робота здобувачів: Вивчення методології OWASP Testing Guide. Аналіз реальних випадків веб-атак. Дослідження інструментів автоматизованого сканування веб-додатків (OWASP ZAP, Nikto).

Тема 7. SOC, управління інцидентами та пентестування

Анотація: Вивчається організація та функціонування Security Operations Center (SOC). Розглядаються процеси управління інцидентами, SIEM системи. Детально аналізується методологія пентестування, етичний хакінг та інструменти тестування на проникнення.

Тема лекції 13: Security Operations Center: архітектура, ролі (Tier 1-3 аналітики), SIEM платформи. Incident Response: виявлення, аналіз, стримування, ліквідація, відновлення. **Тема лекції 14:** Пентестування та етичний хакінг. Методологія (Black Box, White Box, Grey Box). Фази пентесту: Reconnaissance, Scanning, Exploitation, Post-Exploitation, Reporting. Інструменти: Metasploit, Burp Suite, Nessus.

Тема лабораторного заняття 7: Проведення базового пентесту на тестовому середовищі. Використання Metasploit Framework та інструментів Kali Linux.

Самостійна робота здобувачів: Вивчення стандартів реагування на інциденти (NIST, SANS). Аналіз MITRE ATT&CK framework. Дослідження кар'єрних шляхів у пентестуванні та SOC.

Тема 8. Хмарна безпека, форензіка та розвідка загроз

Анотація: Розглядаються особливості безпеки хмарних технологій (AWS, Azure, GCP) та DevSecOps практики. Вивчаються методи цифрової форензіки та розслідування інцидентів. Аналізуються підходи до розвідки загроз (Threat Intelligence) та проактивного полювання на загрози (Threat Hunting).

Тема лекції 15: Cloud Security: моделі (IaaS, PaaS, SaaS), Shared Responsibility Model. DevSecOps: CI/CD безпека, SAST/DAST, Container security. Кіберфорензіка: збір та аналіз цифрових доказів.

Тема лекції 16: Threat Intelligence: типи розвідки (стратегічна, тактична, операційна), джерела IOC. Threat Hunting: проактивний пошук загроз, використання MITRE ATT&CK. Інструменти: YARA, Sigma rules, threat feeds.

Тема лабораторного заняття 8: Аналіз цифрових доказів та проведення форензичного розслідування. Практика Threat Hunting з використанням SIEM логів.

Самостійна робота здобувачів: Вивчення безпеки основних хмарних провайдерів (AWS Security, Azure Security Center). Аналіз методів memory forensics. Дослідження джерел Threat Intelligence та IOC платформ.

Модульний контроль 2

5. Індивідуальні завдання

Виконання РР (Оцінка вразливостей).

6. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

7. Методи контролю

Поточний контроль: опитування на лекційних та лабораторних заняттях з основних понять мережевої безпеки, віртуалізації, операційних систем та баз даних; аналіз та порівняння методів захисту на різних рівнях моделі OSI; виконання письмових контрольних робіт з окремих розділів курсу (мережеві протоколи та атаки, безпека віртуальних середовищ, захист операційних систем, SQL Injection та захист БД, криптографічні алгоритми, веб-вразливості OWASP Top 10, SOC та пентестування, хмарна безпека та форензіка); програмований контроль (тестування, онлайн-тести) з теоретичних основ та практичних аспектів кібербезпеки; оцінювання виконання індивідуальних лабораторних робіт з аналізу мережевого трафіку Wireshark, дослідження атак на віртуальні середовища, тестування вразливостей операційних систем, SQL Injection атак, криптографічних протоколів, веб-вразливостей, проведення пентестів та форензичного аналізу; перевірка звітів з лабораторних робіт та їх захист; оцінювання виконання індивідуальних завдань з аналізу загроз та розробки рекомендацій щодо захисту інформаційних систем.

Модульний контроль: складання модульного контролю з змістового модуля 1 "Базові технології та інфраструктурна безпека" та змістового модуля 2 "Практична кібербезпека та реагування на інциденти"; перевірка знань з мережевих протоколів та атак на моделі OSI, безпеки віртуалізації та контейнерів, механізмів захисту операційних систем, SQL Injection та захисту баз даних, криптографічних алгоритмів та протоколів, веб-вразливостей OWASP Top 10, організації SOC та методології пентестування, хмарної безпеки та цифрової форензіки, розвідки загроз та Threat Hunting; оцінювання практичних навичок роботи з інструментами кібербезпеки (Wireshark, nmap, Metasploit, Burp Suite, SIEM), проведення аналізу вразливостей та розробки захисних заходів.

Підсумковий контроль: іспит, що включає теоретичні питання з усіх розділів курсу та практичні завдання з аналізу мережевого трафіку, виявлення вразливостей операційних систем та баз даних, застосування криптографічних методів захисту, тестування веб-додатків на вразливості, проведення базового пентесту, аналізу інцидентів кібербезпеки, форензичного розслідування та

розвідки загроз для забезпечення комплексного захисту інформаційних систем.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1 Змістовний модуль 1			
Робота на лекціях	0...1	4	0...4
Лабораторні заняття	0...6	2	0...12
Модульний контроль	0…10	1	0…10
Змістовний модуль 2			
Робота на лекціях	0...1	4	0...4
Лабораторні заняття	0...6	2	0...12
Модульний контроль	0…9	1	0…10
Модуль 2 Змістовний модуль 3			
Робота на лекціях	0...1	4	0...4
Лабораторні заняття	0...6	2	0...12
Модульний контроль	0…10	1	0...9
Змістовний модуль 4			
Робота на лекціях	0...1	4	0...4
Лабораторні заняття	0...6	2	0...12
Модульний контроль	0…7	1	0...7
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови здобувача освіти від балів підсумкового контролю. Під час складання семестрового іспиту здобувач освіти має можливість отримати максимум 100 балів.

Білет для заліку складається з двох теоретичних і одного практичного запитання. За теоретичні запитання студент отримує до 60 балів (до 30 балів за кожне) , за практичне – до 40 балів. Під час складання семестрового заліку здобувач має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60-74) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Написав чотири модульні контрольні роботи. Знає основні визначення та термінологію в галузі кібербезпеки. Розуміє модель OSI та основні мережеві протоколи стеку TCP/IP. Знає типи атак на мережевому рівні (ARP poisoning, IP spoofing, SYN flood). Описує принципи віртуалізації, типи гіпервізорів та базові загрози (VM Escape). Розрізняє механізми захисту операційних систем Windows та Linux. Знає основні типи SQL Injection атак та методи захисту баз даних. Пояснює різницю між симетричним та асиметричним шифруванням. Описує базові принципи хешування та цифрового підпису. Знає поняття OWASP Top 10 вразливостей веб-додатків. Розуміє основні функції SOC та етапи реагування на інциденти. Знає базову методологію пентестування. Описує принципи цифрової форензіки та збору доказів. Виконує лабораторні роботи з аналізу мережевого трафіку, тестування вразливостей та базового пентестування. Використовує стандартні інструменти кібербезпеки для розв'язання базових задач.

Добре (75-89) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Написав чотири модульні контрольні роботи. Додатково до вимог на оцінку "задовільно": Проводить порівняльний аналіз атак на різних рівнях OSI моделі, порівнює їх ефективність та область застосування. Самостійно аналізує мережевий трафік за допомогою Wireshark та виявляє аномалії. Розуміє атаки на віртуальні середовища (Hyperjacking, Side-channel) та контейнери Docker. Знає структуру та особливості апаратних атак Meltdown та Spectre. Аналізує вразливості операційних систем та застосовує механізми захисту (SELinux, AppArmor, UAC). Самостійно проводить тестування SQL Injection різних типів (Union-based, Blind, Time-based). Розраховує та застосовує криптографічні алгоритми (AES, RSA). Знає структуру TLS протоколу та його вразливості. Виконує тестування веб-додатків за методологією OWASP. Розуміє архітектуру SOC та ролі аналітиків (Tier 1-3). Проводить базовий пентест з використанням Metasploit Framework. Знає методи форензичного аналізу та збереження цифрових доказів. Порівнює різні інструменти кібербезпеки та обґрунтовує вибір оптимальних рішень.

Відмінно (90-100) – здобувач має глибокі знання, навички та вміння для досягнення результатів навчання за програмою на високому рівні. Написав чотири модульні контрольні роботи на відмінно. Додатково до вимог на оцінку "добре": Вільно оперує термінологією кібербезпеки та мережевих технологій. Самостійно розробляє стратегії захисту мережевої інфраструктури на всіх рівнях OSI. Проектує безпечні віртуальні середовища з урахуванням ізоляції та захисту від VM Escape. Обґрунтовує вибір механізмів захисту операційних систем для конкретних сценаріїв. Розробляє комплексні заходи захисту баз

даних від SQL Injection та інших атак. Аналізує криптографічні протоколи та виявляє потенційні вразливості (POODLE, Heartbleed, BEAST). Проводить повний аудит безпеки веб-додатків за стандартами OWASP. Самостійно проектує архітектуру SOC та розробляє процедури реагування на інциденти. Проводить комплексне пентестування з використанням професійних інструментів та складає детальні звіти. Виконує форензичний аналіз із збереженням цілісності доказів для судового використання. Застосовує методи Threat Intelligence та Threat Hunting для проактивного виявлення загроз. Демонструє творчий підхід до розв'язання нестандартних задач кібербезпеки, пропонує інноваційні рішення для захисту інформаційних систем.

9. Політика навчального курсу

Відвідування занять. Обов'язкове відвідування лекційних та лабораторних занять з навчальної дисципліни "Інструментальні та прикладні застосунки в інформаційній та кібербезпеці" через їх інтерактивний характер та необхідність практичного освоєння методів аналізу мережевого трафіку, тестування вразливостей операційних систем та баз даних, роботи з криптографічними алгоритмами, проведення пентестування та форензичного аналізу для забезпечення комплексного захисту інформаційних систем. Здобувачі освіти, які не можуть регулярно відвідувати заняття, зобов'язані узгодити з викладачем протягом тижня графік відпрацювання пропущених занять. Пропущені заняття необхідно відпрацювати під час найближчої консультації протягом тижня з моменту пропуску, як правило, у формі усного опитування за попередньо визначеними питаннями з відповідних тем курсу. У деяких випадках допускається відпрацювання пропущених лабораторних занять у формі виконання письмових завдань з аналізу мережевого трафіку Wireshark, дослідження SQL Injection атак, тестування веб-вразливостей або проведення базового пентесту на тестовому середовищі. Пропуск модульних контрольних робіт без поважної причини не допускається.

Дотримання вимог академічної доброчесності Здобувачі освіти зобов'язані дотримуватися загальних морально-етичних норм, а також вимог академічної доброчесності, викладених у "Положенні про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут»" (https://khal.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Роботи здобувачів освіти (звіти з лабораторних робіт, розрахункова робота, модульні контрольні роботи) повинні бути оригінальними. Прикладами порушення академічної доброчесності є відсутність посилань на джерела, вигадування джерел, плагіат, перешкоджання роботі інших здобувачів освіти. Виявлення ознак порушення академічної доброчесності в письмових роботах (звітах з лабораторних робіт, розрахунковій роботі, модульних контрольних роботах) призводить до оцінки "незадовільно" незалежно від масштабу плагіату або обману. Особлива увага приділяється оригінальності програмного коду, реалізованого під час лабораторних робіт з дослідження криптографічних

алгоритмів та стеганографічних методів. Використання готових рішень без посилань на джерела та без власного аналізу та модифікації вважається порушенням академічної доброчесності.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khal.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор»: [Ел. ресурс]. https://mentor.khai.edu/course/view.php?id=2165

11. Рекомендована література

Базова

1. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем._ К.: Вид.група BHV, 2009.-608 с.
2. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб.
3. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.
4. Захист інформації в автоматизованих системах управління: навч. посіб. /Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.
5. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий світ-2000», 2020 . – 678 с

Допоміжна

1. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.
2. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/ 4

3. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
4. Open Web Application Security Project [Електронний ресурс]. Режим доступу: a. www.owasp.org 6. Когут Ю.І. Кібербезпека

Інформаційні ресурси

1. http://dstszi.gov.ua/
2. Офіційний сайт Google, на якому розміщена документація по роботі із Google App Engine. [Електронний ресурс]. – Режим доступу: https://cloud.google.com/products/appengine
3. 2. Офіційний сайт Microsoft, на якому розміщена документація по роботі із платформою Microsoft Azure. [Електронний ресурс].