Силабус курсу

ІНФОРМАЦІЙНА БЕЗПЕКА

Ступінь вищої освіти – бакалавр

Освітньо-професійна програма: “Технології інтернету речей”

Рік навчання: III **Семестр:** VI

Кількість кредитів: 5 **Мова викладання:** українська

Керівник курсу

ПІП д.т.н., професор Яцків Василь Васильович

Контактна інформація v.yatskiv@wunu.edu.ua

Опис дисципліни

Курс «Інформаційна безпека» охоплює знання і навички, необхідні для успішної обробки завдань, обов'язків і зон обов'язків аналітика безпеки молодшого рівня, який працює в Центрі моніторингу та управління безпекою (SOC).

Після проходження курсу студенти зможуть виконувати такі завдання: аналізувати роботу мережевих протоколів і служб; пояснити принципи роботи мережевої інфраструктури; класифікувати різні типи мережевих атак; використовувати засоби мережевого моніторингу для визначення атак на мережеві протоколи і служби; застосовувати різні способи запобігання несанкціонованому доступу до комп'ютерних мереж, хостів і даними; знати способи визначення вразливостей кінцевих пристроїв і атаках на них; виявляти попередження безпеки мережі; аналізувати дані про вторгнення в мережу для перевірки потенційних загроз; застосовувати моделі реагування для усунення інцидентів безпеки.

Структура курсу

№	Тема	Результати навчання	Завдання
1	Кібербезпека і центр моніторингу та управління безпекою.	Знати поняття кібербезпеки, основні загрози інформаційним системам та роль центрів моніторингу та управління безпекою (SOC) в організації захисту. Вміти описувати типову архітектуру SOC, його функції (збір логів, кореляція подій, реагування на інциденти) та місце в системі управління інформаційною безпекою організації. Розуміти значення безперервного моніторингу, автоматизації обробки подій безпеки та взаємодії SOC з іншими підрозділами.	Тести, питання
2	Принципи забезпечення безпеки комп’ютерних систем.	Знати базові принципи інформаційної безпеки: конфіденційність, цілісність, доступність, аутентичність, невідмовність, а також принципи «мінімальних повноважень» і «захисту в глибину». Вміти застосовувати ці принципи при розробці та аналізі політик безпеки, налаштуванні доступу, резервуванні даних та сегментації мережі. Розуміти взаємозв’язок між організаційними, технічними та програмними заходами безпеки та їхній вплив на загальний рівень захищеності системи.	Тести, питання

3	Поширені атаки комп'ютерні системи.	Знати класифікацію поширених атак: шкодочинне програмне забезпечення (віруси, трояни, руткіти, програми-вимагачі), фішинг, соціальна інженерія, DoS/DDoS-атаки, підбір паролів, експлуатація вразливостей. Вміти наводити приклади реальних атак, описувати їхні ознаки та можливі наслідки для організації. Розуміти типові шляхи потрапляння шкідливого коду в систему та важливість просвітницької роботи зі користувачами як елементу захисту.	Тести, питання
4	Типи атак на комп'ютерні системи	Знати поділ атак за різними ознаками: пасивні та активні, внутрішні та зовнішні, цілеспрямовані та масові, мережеві, прикладні та фізичні. Вміти аналізувати сценарії атак з точки зору їхніх цілей (крадіжка даних, вивід із ладу, шантаж, шпигунство) та обирати відповідні заходи протидії. Розуміти, що комплексний захист повинен враховувати різні типи атак і вразливостей на всіх рівнях інформаційної системи.	Тести, питання
5	Моніторинг мережі і засоби моніторингу.	Знати основні підходи до моніторингу мережевого трафіку (SNMP, NetFlow, зеркалювання портів) та інструменти моніторингу (системи NMS, аналізатори трафіку, IDS/IPS). Вміти інтерпретувати основні показники мережі (пропускна здатність, затримка, втрата пакетів, аномалії трафіку) та виявляти потенційно небезпечну активність. Розуміти роль моніторингу в ранньому виявленні інцидентів безпеки та відмінність між технічним моніторингом продуктивності й моніторингом подій безпеки.	Тести, питання
6	Атаки на базові функції.	Знати, які базові функції інформаційних систем (автентифікація, авторизація, журналювання, резервне копіювання, оновлення) можуть стати ціллю атак. Вміти аналізувати приклади атак на механізми входу в систему, управління паролями, ведення логів, системи резервного копіювання та оновлення програмного забезпечення. Розуміти, що порушення базових функцій безпеки призводить до каскадних ризиків і потребує пріоритетного контролю.	Тести, питання
7	Атаки на службові протоколи.	Знати основні службові протоколи (DNS, DHCP, ARP, ICMP) та типові атаки на них (DNS-spoofing, ARP-spoofing, DHCP starvation, ICMP flood). Вміти пояснювати, як маніпуляції зі службовими протоколами дозволяють зловмиснику перенаправляти трафік, здійснювати «людину посередині» (MITM) та інші атаки. Розуміти необхідність захисту службових протоколів (використання захищених альтернатив, фіксованих налаштувань, списків контролю доступу, сегментації мережі).	Тести, питання
8	Захист мережі.	Знати основні засоби захисту мережі: міжмережеві екрани, системи виявлення та запобігання вторгнень (IDS/IPS), VPN, сегментація мережі, DMZ, фільтрація трафіку. Вміти проектувати базову архітектуру захищеної мережі, визначати правила фільтрації, обирати місця встановлення захисних пристроїв та політики доступу між сегментами. Розуміти важливість багаторівневого підходу до мережевої безпеки та інтеграції різних засобів захисту в єдину систему.	Тести, питання

9	Управління доступом.	Знати моделі управління доступом (дискреційна, мандатна, рольно-орієнтована, атрибутивна), принципи «найменших привілеїв» та «розділення обов'язків». Вміти розробляти політики доступу до ресурсів, налаштовувати ролі, групи та права користувачів в операційних системах і прикладних сервісах. Розуміти ризики, пов'язані з надмірними правами користувачів, спільними обліковими записами та відсутністю регулярного перегляду прав доступу.	Тести, питання
10	Захист кінцевих пристроїв.	Знати основні загрози для кінцевих пристроїв (ПК, ноутбуки, смартфони, планшети, IoT-пристрої) та засоби їх захисту: антивірус, фаєрвол, шифрування дисків, оновлення, керування мобільними пристроями (MDM). Вміти формувати комплекс заходів захисту робочої станції та мобільного пристрою, враховуючи політики паролів, резервне копіювання, шифрування та обмеження встановлення програм. Розуміти роль користувача як ключової ланки в безпеці кінцевої точки та значення навчання цифровій гігієні.	Тести, питання
11	Моніторинг безпеки.	Знати поняття моніторингу безпеки, журнали подій (логи), системи централізованого збору та кореляції подій (SIEM). Вміти визначати, які події необхідно журналювати, аналізувати базові логи (автентифікація, доступ до ресурсів, зміни конфігурації), налаштовувати прості правила виявлення підозрілої активності. Розуміти різницю між реактивним та проактивним підходами до моніторингу безпеки та важливість побудови сценаріїв виявлення інцидентів.	Тести, питання
12	Аналіз даних вторгнень	Знати підходи до аналізу даних про вторгнення: кореляція подій, побудова часових ліній інциденту, виділення індикаторів компрометації (IoC), використання сигнатур та поведінкових моделей. Вміти інтерпретувати сповіщення систем виявлення вторгнень, аналізувати мережеві дампи та журнали подій для встановлення джерела й масштабу атаки. Розуміти роль аналітика безпеки в SOC, значення контексту (інфраструктура, бізнес-процеси) для коректної оцінки серйозності вторгнення.	Тести, питання
13	Реагування на інциденти і їх обробка.	Знати етапи життєвого циклу інциденту інформаційної безпеки: виявлення, класифікація, локалізація, усунення, відновлення, постінцидентний аналіз. Вміти розробляти та застосовувати базові процедури реагування на інциденти (playbooks): ізоляція уражених систем, зміна облікових даних, відновлення з резервних копій, комунікація з відповідальними особами. Розуміти важливість документування інцидентів, збереження цифрових доказів та подальшого вдосконалення політик і засобів захисту на основі отриманого досвіду.	Тести, питання
14	Обробка інцидентів.	Знати організаційні аспекти обробки інцидентів: розподіл ролей у команді реагування, канали комунікації, використання систем керування інцидентами. Вміти описувати та формалізувати інциденти (пріоритет, вплив, статус), планувати дії з їх усунення та контролювати виконання коригувальних заходів. Розуміти різницю між	Тести, питання

		технічними діями реагування та управлінськими рішеннями, значення обробки інцидентів для побудови зрілої системи управління інформаційною безпекою в організації.	

Літературні джерела

1. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. 412 с.
2. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. pp. 466-478.
3. Hamdani, Syed Wasif Abbas, et al. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons." ACM Computing Surveys (CSUR) 54.3, 2021. pp.1-36.
4. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. 341 p.
5. Grubb S. How Cybersecurity Really Works. 2021. 219 p.
6. Grimes, Roger A. Hacking Multifactor Authentication. John Wiley & Sons, 2020.

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності. Списування під час проведення контрольних за ходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об’єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування тощо) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Політика щодо визнання результатів навчання

Відповідно до «Положення про визнання в Західноукраїнському національному університеті результатів попереднього навчання» (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf) здобувачам вищої освіти може бути зараховано результати навчання (неформальної/інформальної освіти, академічної мобільності тощо) на підставі підтвердних документів (сертифікати, довідки, документи про підвищення кваліфікації тощо). Рішення про зарахування здобувачу результатів (певного освітнього компонента в цілому, або ж окремого виду навчальної роботи за таким освітнім компонентом) приймається уповноваженою Комісією з визнання результатів навчання за процедурою, визначеною вищезазначеним положенням.

Оцінювання

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Інформаційна безпека» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		**Модуль 2**	**Модуль 3**
40%	**40%**	**5 %**	**15 %**
Поточне оцінювання	Модульний контроль 2	Тренінг	Самостійна робота
Оцінка визначається як середнє арифметичне з отриманих оцінок за другий змістовий модуль	Виконання модульного завдання	Оцінка за виконання завдання	Оцінка за виконання самостійного завдання

Шкала оцінювання

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60-64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов’язковим повторним курсом)