СИСТЕМИ МОНІТОРИНГУ ЗАГРОЗ ТА АТАК
Циклова комісія програмування та інформаційних дисциплін
Відділення інформаційних технологій

Викладач	Черняк Вадим Андрійович
Семестр	7
Освітній ступінь	Спеціаліст
Кількість кредитів ЄКТС	3
Форма контролю	Залік
Аудиторні години	90/44 (14 год. лекцій, 30 год. практичних)

Загальний опис дисципліни

Дисципліна **«Системи моніторингу загроз та атак»** присвячена вивченню технологій та методів, що застосовуються для контролю стану безпеки інформаційних систем, виявлення шкідливої активності та оперативного реагування на кібератаки. Основною метою курсу є формування у студентів знань і практичних умінь, необхідних для налаштування, експлуатації та вдосконалення систем моніторингу безпеки, здатних забезпечити стабільну та захищену роботу IT-інфраструктури.

У ході навчання розглядаються принципи побудови систем моніторингу, їхнє функціонування в сучасному середовищі кібербезпеки, а також засоби виявлення загроз на основі аналізу подій, мережевого трафіку та поведінкових аномалій. Студенти знайомляться з нормативно-правовими вимогами України та міжнародними стандартами, що регламентують моніторинг та реагування на інциденти, а також вивчають методики оцінювання ризиків і вразливостей інформаційних систем.

Програма передбачає опанування різних класів інструментів, серед яких **SIEM-системи**, **IDS/IPS-рішення**, аналізатори мережевого трафіку та інші програмно-апаратні комплекси, що використовуються для збору, оброблення та кореляції подій безпеки. Значну увагу приділено практичним навичкам: інтерпретації журналів подій, побудові правил виявлення загроз, створенню політик моніторингу та виконанню дій у відповідь на інциденти.

У межах курсу студенти вчаться моделювати сценарії атак, перевіряти стійкість систем до несанкціонованого доступу, здійснювати управління правами користувачів та приймати рішення, спрямовані на запобігання або мінімізацію наслідків кібератак. Практичний компонент

охоплює також роботу з інструментами аналізу та моніторингу продуктивності, що дозволяє підтримувати безперервне функціонування інформаційних ресурсів.

Завдяки вивченню дисципліни здобувачі освіти отримують комплекс компетентностей, необхідних для роботи у сфері інформаційної та кібербезпеки, зокрема: уміння проводити аналіз безпеки, реагувати на інциденти, підтримувати політику інформаційної безпеки організації та застосовувати сучасні технології для виявлення загроз у реальному часі. Курс готує студентів до діяльності на позиціях аналітиків SOC, фахівців із моніторингу подій, спеціалістів з реагування на інциденти та інших ролей, пов'язаних із забезпеченням кіберзахисту.

Теми лекцій

1. Поняття моніторингу, його роль у виявленні загроз. Основні елементи системи моніторингу та їх взаємодія.
2. Застосування моніторингу в енергетиці, транспорті, сільському господарстві, ІТ.
3. Призначення датчиків, види сигналів, способи передачі даних у системи моніторингу.
4. Виявлення загрози і спроби атак. Основні кроки створення простої системи кібермоніторингу.
5. Основи роботи з системами IDS, сканерами мереж.
6. Прості правила захисту від кіберзагроз.
7. Як працюють IDS-системи, які типи вторгнень вони фіксують, приклади програмних рішень.

Теми практичних робіт

1. Розробка та налаштування системи моніторингу мережевого середовища для виявлення інцидентів безпеки
2. Моніторинг, його види та основні напрямки застосування у різних сферах діяльності (енергетиці, транспорті, сільському господарстві, ІТ)
3. Складові елементи та принципи функціонування систем моніторингу
4. Порядок реєстрації авторського права на комп'ютерну програму. Підготовка та заповнення основних документів для подання заявки.
5. Особливості вільного використання програм у навчальних, наукових і службових цілях.
6. Датчики як основне джерело інформації для моніторингу.
7. Призначення датчиків, види сигналів, способи передачі даних у

системи моніторингу.

8. Організація системи моніторингу загроз та атак на підприємстві. Виявлення загрози і спроби атак.
9. Основні кроки створення простої системи кібермоніторингу. Приклади систем моніторингу для захисту технологічних процесів і даних підприємств АПК
10. Принципи побудови систем моніторингу мереж, способами виявлення атак та інструментами для аналізу мережевої активності.
11. Принципи функціонування систем IDS, SIEM та мережевих сканерів визначення їх призначення, роль у виявленні атак і зборі даних про інциденти інформаційної безпеки.
12. Кібергігієна — основа безпечної роботи в інформаційному середовищі.
13. Ефективні способи захисту персональних даних та пристроїв, правила користуватися паролями, антивірусами й системними оновленнями для запобігання кіберзагрозам.
14. Системи виявлення вторгнень (IDS): призначення, принципи роботи та типи вторгнень.
15. Системи запобігання вторгненням (IPS): робота в реальному часі. Відмінності між IDS і IPS.