БЕЗПЕКА ЕКСПЛУАТАЦІЇ І ОБСЛУГОВУВАННЯ ІТ-СИСТЕМ

Циклова комісія програмування та інформаційних дисциплін
Відділення інформаційних технологій

Викладач	**Надозірний Святослав Вікторович**
Семестр	7
Освітній ступінь	Фаховий молодший бакалавр
Кількість кредитів ЄКТС	3
Форма контролю	Залік
Аудиторні години	90 (24 год. лекцій, 20 год. практичних, 46 год. самостійної роботи)

Загальний опис дисципліни

Дисципліна «Безпека експлуатації і обслуговування ІТ-систем» спрямована на формування у студентів комплексних знань та практичних навичок з забезпечення безпеки під час експлуатації та обслуговування ІТ-систем, розвиток здатності забезпечувати надійну та безпечну роботу інформаційних технологій в організації. Курс охоплює фундаментальні принципи інформаційної безпеки, методи захисту операційних систем, мережевої інфраструктури, баз даних, а також процедури моніторингу, аудиту та реагування на інциденти безпеки.

Завданнями вивчення дисципліни є опанування принципів безпечної експлуатації ІТ-інфраструктури; вивчення методів забезпечення безпеки серверних систем та мережевого обладнання; освоєння практичних навичок адміністрування систем безпеки; розвиток вмінь діагностування та усунення проблем безпеки; формування навичок планування та проведення регламентних робіт; вивчення процедур резервного копіювання та відновлення систем.

Теми лекцій

1. Основи безпечної експлуатації ІТ-систем. Принципи ІБ, класифікація загроз.
2. Безпека операційних систем Windows. Налаштування GPO, UAC.

3. Безпека операційних систем Linux. Права доступу, SELinux, AppArmor.
4. Основи мережевої безпеки. Протоколи, топології, сегментація.
5. Системи виявлення вторгнень. IDS/IPS, аналіз трафіку.
6. Безпека баз даних. MySQL, PostgreSQL, MSSQL захист.
7. Безпека веб-додатків. OWASP Top 10, захист API.
8. Основи SIEM систем. Збір логів, кореляція подій.
9. Контроль цілісності та аудит систем. AIDE, Tripwire, аудит подій.
10. Планування безперервності бізнесу. BCP, DRP, RTO/RPO. Стратегії резервного копіювання.
11. Реагування на інциденти. CERT процедури, форензика.
12. Розслідування інцидентів. Документування, звітність, уроки.

Теми практичних робіт

1. Аналіз політик безпеки, створення матриці ризиків.
2. Налаштування безпеки Windows Server, створення політик паролів.
3. Налаштування iptables, конфігурування SSH, управління користувачами.
4. Налаштування pfSense firewall, створення правил фільтрації.
5. Налаштування безпеки СУБД, створення ролей та привілеїв.
6. Створення дашбордів моніторингу в SIEM, налаштування алертів.
7. Налаштування моніторингу цілісності файлів, аналіз логів.
8. Налаштування Bacula/Amanda, тестування відновлення.
9. Симуляція реагування на інцидент, збір доказів.
10. Аналіз реального інциденту, складання звіту.