ОЦІНКА ТА УПРАВЛІННЯ РИЗИКАМИ В ІТ-БЕЗПЕЦІ

Циклова комісія програмування та інформаційних дисциплін
Відділення інформаційних технологій

Викладач	**Надозірний Святослав Вікторович**
Семестр	5
Освітній ступінь	Фаховий молодший бакалавр
Кількість кредитів ЄКТС	3
Форма контролю	Залік
Аудиторні години	90 (14 год. лекцій, 30 год. практичних, 46 год. самостійної роботи)

Загальний опис дисципліни

Дисципліна «Оцінка та управління ризиками в ІТ-безпеці» спрямована на формування у студентів комплексного розуміння принципів, методів і моделей оцінювання ризиків інформаційної безпеки, а також розвиток практичних навичок управління ризиками в інформаційно-телекомунікаційних системах з урахуванням вимог законодавства України, національних та міжнародних стандартів у сфері ІБ/КБ. Курс охоплює життєвий цикл управління ризиками, від ідентифікації загроз та уразливостей до розробки стратегій обробки ризиків, впровадження заходів захисту та постійного моніторингу.

Завданнями вивчення дисципліни є надання знань про понятійний апарат ризик-менеджменту; формування розуміння нормативно-правової та стандартної бази з оцінювання ризиків; навчання ідентифікації активів, загроз, уразливостей та сценаріїв атак; формування навичок якісного та кількісного оцінювання ризиків; навчання обирати стратегії обробки ризиків; розвиток вмінь здійснювати моніторинг та документування ризиків.

Теми лекцій

1. Основи управління ризиками в ІТ-безпеці. Життєвий цикл управління ризиками.
2. Стандарти та методології оцінки ризиків. ISO/IEC 27005, NIST RMF, FAIR, OCTAVE.

3. Ідентифікація та класифікація загроз. MITRE ATT&CK, STRIDE, DREAD.
4. Методи оцінки ризиків. Якісні, кількісні та напівкількісні підходи. Матриці ризиків.
5. Розробка стратегій управління ризиками. Уникнення, зменшення, передача, прийняття.
6. Впровадження заходів захисту для зниження ризиків. Технічні та організаційні заходи.
7. Моніторинг, контроль і перегляд ризиків. KPI, KRI, звітність.

Теми практичних робіт

1. Аналіз інцидентів. Ідентифікація компонентів ризику.
2. Карта зацікавлених сторін ризик-менеджменту.
3. Порівняльний аналіз методологій оцінки ризиків.
4. План впровадження процесу управління ризиками.
5. Реєстр загроз. Аналіз за MITRE ATT&CK.
6. Оцінка ймовірності та впливу загроз.
7. Розробка сценаріїв реалізації загроз.
8. Якісний аналіз ризиків. Розрахунок ALE, ROI.
9. Побудова матриці ризиків.
10. Використання програмних засобів управління ризиками.
11. Розробка стратегій обробки ризиків.
12. План обробки ризиків. Аналіз ефективності заходів.
13. Вибір засобів захисту. Розробка технічного завдання.
14. Етапи впровадження заходів захисту. Оцінка ефективності.
15. Показники моніторингу. Дашборд ризиків. Звіт про стан управління ризиками.