## ДИСЦИПЛІНА «МЕТОДИ ПРОГНОЗУВАННЯ ТА МОДЕЛЮВАННЯ В СФЕРІ КІБЕРБЕЗПЕКИ»

**Анотація.** Належить до переліку дисциплін вільного вибору аспіранта. У ній розглядаються математичні методи та алгоритмічні моделі, що дозволяють передбачати розвиток кіберзагроз та оцінювати наслідки атак на інформаційні системи. Програма курсу охоплює вивчення теоретико-ігрових моделей протиборства в кіберпросторі, методів аналізу часових рядів для виявлення прихованих тенденцій, а також марковських процесів для моделювання станів безпеки систем. Особлива увага приділяється прогнозуванню поширення шкідливого ПЗ (епідеміологічні моделі), оцінці імовірності успішної реалізації атак на основі дерев відмов та побудові прогнозних моделей поведінки зловмисників.

**Мета навчальної дисципліни:** формування в аспірантів системних знань та навичок застосування математичного апарату для побудови прогнозних моделей захищеності; розвиток здатності до моделювання складних процесів у кіберпросторі з метою прийняття обґрунтованих управлінських рішень щодо мінімізації ризиків.

**Попередні вимоги:**

**Аспірант повинен знати:** теорію ймовірностей та математичну статистику; основи дискретної математики; принципи функціонування сучасних ІКС; базові методи аналізу вразливостей.

**Аспірант повинен вміти:** використовувати мови програмування (Python або R) для статистичної обробки даних; будувати прості логіко-імовірнісні моделі; аналізувати структуру складних систем.

**Змістові модулі:**

- **Основи прогностики в кібербезпеці.** Об'єкти, методи та часові горизонти прогнозування.
- **Математичне моделювання атак.** Використання графів атак (Attack Graphs) та дерев атак (Attack Trees) для аналізу вразливостей.
- **Теорія ігор у кібербезпеці.** Моделювання взаємодії «захисник – зловмисник» та пошук стратегій рівноваги.
- **Прогнозування часових рядів інцидентів.** Статистичні методи та експоненціальне згладжування для передбачення інтенсивності атак.
- **Марковські моделі живучості систем.** Оцінка ймовірності перебування системи у працездатному та безпечному станах.
- **Імітаційне моделювання процесів захисту.** Використання агентного моделювання для симуляції кіберпротиборства.
- **Прогнозне оцінювання збитків та ризиків.** Моделі Монте-Карло в задачах кількісної оцінки кіберризиків.

**Мова викладання:** українська.

**Рік підготовки, шифр навчальної дисципліни:** друге півріччя другого року навчання, ВБ 2.02.07.

**Кількість кредитів:** 4 кредити ЄКТС.

**Форма заключного контролю:** іспит.

**Структура навчальної дисципліни:** загальний обсяг 120 годин.

**Викладач:** Наконечний Володимир Сергійович, доктор технічних наук, професор.