

ЗМІСТ

ВСТУП.....	6
 ГЛАВА 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ	
БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ	9
1.1. Об'єкти критичної інфраструктури: елементи, процедури, структура	9
1.2. Загрози безпеці об'єктам критичної інфраструктури. Класифікатор загроз як формальне подання типів та властивостей кіберзагро 17	17
1.3. Концепція багатоконтурних систем безпеки об'єктів критичної інфраструктури	20
1.4. Система управління як система з критичною кіберінфраструктурою	24
1.5. Модель виявлення та пошуку об'єктів з критичною кіберінфраструктурою	28
Висновки за главою 1	32
 ГЛАВА 2. МОДЕЛЮВАННЯ ДИНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ	
СИСТЕМ БЕЗПЕКИ	34
2.1. Концепція моделювання поведінки взаємодіючих агентів систем безпеки.....	34
2.2. Модельний базис методології моделювання процесів поведінки антагоністичних агентів	38
2.3. Системно-динамічна модель поведінки антагоністичних агентів	43
2.4. Динамічні моделі безпеки на основі підходу Лотки-Вольтери.....	46
2.5. Концепція побудови диференціально-ігрових розподілених систем інформаційної безпеки.....	50
2.6. Диференціально-ігрова модель розподіленої системи інформаційної безпеки.....	57
2.7. Диференціально-ігрова нетейлорівська модель.....	63
2.8. Синтез оптимальної поведінки в системі кіберзахист–кібератака	66
2.9. Багатокритерійна диференціально-ігрова модель процесу кібернападу на державні інформаційні ресурси об'єкта критичної інфраструктури	74
2.10. Ієрархічна диференціально-ігрова модель для задач оцінювання ефективності систем інформаційної безпеки	81
Висновки за главою 2.....	88

ГЛАВА 3. МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 92

3.1. Властивості постквантових алгоритмів забезпечення послуг безпеки об'єктів критичної інфраструктури.....	92
3.2. Забезпечення послуг безпеки об'єктів критичної інфраструктури на основі крипто-кодових конструкцій на ЕС (МЕС)	99
3.3. Забезпечення послуг безпеки об'єктів критичної інфраструктури на основі гібридних крипто-кодових конструкцій на збиткових кодах	102
Висновки за главою 3	105

ГЛАВА 4. ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ ОБ'ЄКТАМИ ТА БАЗИ ЗНАНЬ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ 107

4.1. Архітектури та алгоритми функціонування безперервних нейронних мереж адаптивної резонансної теорії, здатних визначати декілька рішень	107
4.2. Стабільно-пластичні нейронні мережі Гемінга, Хебба та мережі на основі перцептрону здатні розпізнавати нову інформацію, донавчатися та визначати декілька рішень	117
4.3. Багатоспрямовані бази знань побудовані на моделях асоціативної пам'яті, що дозволяють донавчатися та визначати кілька рішень.....	144
Висновки за главою 4.....	162

ГЛАВА 5. МОДЕЛІ УПРАВЛІННЯ ТРАФІКОМ ІНТЕГРАЛЬНИХ ПОТОКІВ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ... 164

5.1. Моделювання трафіку, створюваного інтегральними потоками даних ...	164
5.2. Модель процесу буферизації при управлінні трафіком інтегральних потоків даних	171
5.2.1. Сплайн-інтерполяція еластичного трафіку	172
5.2.2. Ітераційний метод оцінки адекватності моделі трафіку	175
5.3. Моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури.....	177
5.4. Конвергенція трафіку в мультисервісних мережах	181
5.5. Визначення характеристик викидів агрегованого трафіку	185
5.6. Фрактальна модель трафіку ПІД	193
5.6.1. Визначення фрактальної розмірності трафіку	193

5.6.2. Фрактальні властивості трафіку ІПД з повторними запитами	197
5.6.3. Фрактальна модель трафіку ІПД, що використовує властивість масштабної інваріантності	201
5.7. Модель процесу буферизації при управлінні трафіком інтегральних потоків даних	211
5.8. Моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури	215
Висновки за главою 5	225

ГЛАВА 6. ПРИКЛАДНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ	226
6.1. Диференціально-ігровий шаблон нормальної поведінки Web-сервера Житомирського військового інституту імені С. П. Корольова	226
6.2. Експериментальна верифікація диференціально-ігрових моделей критичної кіберінфраструктури на прикладі сайту Центральної виборчої комісії	239
6.3. Методологія синтезу диференціально-ігрових моделей та методів моделювання процесів кібернападу	253
6.4. Верифікація моделей постквантових алгоритмів у модифікації протоколу SSL/TLS	258
6.5. Методологія побудови багатоконтурних систем захисту об'єктів критичної інфраструктури	263
Висновки за главою 6	268
ВИСНОВКИ	272
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	275