

## ЗМІСТ

Умовні позначення .....	5
Вступ.....	7
<b>Розділ 1. Побудова інформаційних технологій відбирання різномірних даних у контексті стратегічної безпеки об'єктів .....</b>	<b>9</b>
1.1. Стратегічна безпека системи “об’єкт – інформаційна технологія” .....	9
1.2. Багаторівнева платформа інформаційних технологій у контексті інформатизації .....	16
1.3. Парадигма побудови інформаційних технологій для забезпечення стратегічної безпеки системи “об’єкт – ІТ” .....	35
<b>Розділ 2. Системна концепція створення інформаційних технологій відбирання різномірних даних від об’єктів дослідження.....</b>	<b>39</b>
2.1. Концепція створення ІТ відбирання різномірних даних від техногенних об’єктів .....	39
2.2. Методологія відбирання різномірних даних для ІТ у прикладних завданнях контролю технічного стану об’єктів.....	44
2.3. Концептуальна структура метрологічного забезпечення для ІТ відбирання різномірних даних від об’єктів.....	51
<b>Розділ 3. Методологічні засади створення ІТ відбирання різномірних даних для визначення роботоздатності об’єктів.....</b>	<b>59</b>
3.1. Методологічний підхід до створення ІТ відбирання даних про стан матеріалів методом акустичної емісії.....	59
3.2. Системний підхід до оцінювання концентрації водню у феромагнетиках на основі магніторелаксаційного методу.....	75
<b>Розділ 4. Моделі побудови ІТ відбирання даних про напружено-деформований стан матеріалів .....</b>	<b>86</b>
4.1. Парадигма визначення параметрів напружено-деформованого стану матеріалів .....	86
4.2. Комплексний підхід до визначення параметрів напружено-деформованого стану матеріалів на основі ІТ відбирання даних.....	91
4.3. Концептуальна модель оцінювання екологічного ризику на основі інтеграції ІТ відбирання параметрів води як технологічного ресурсу .....	107
<b>Розділ 5. Методологія забезпечення безпеки інформаційних технологій.....</b>	<b>119</b>
5.1. Гарантоздатність інформаційних технологій: функціональна та інформаційна безпека .....	119
5.2. Системна та нормативна моделі безпеки ІТ.....	126

---

5.3. Комплексна модель безпеки інформаційних технологій та методологія побудови .....	130
<b>Розділ 6. Управління комплексною системою безпеки ІТ .....</b>	<b>134</b>
6.1. Моделі управління безпекою інформаційних технологій .....	134
6.2. Управління життєвим циклом інформації та комплексною системою безпеки ІТ .....	142
<b>Розділ 7. Квінтесенція безпеки кіберфізичних систем: парадигма, концепція, універсальна платформа .....</b>	<b>153</b>
7.1. Тенденції розвитку безпеки кіберфізичних систем .....	153
7.2. Парадигма та концепція створення багаторівневої комплексної системи безпеки кіберфізичних систем .....	156
7.3. Модель інформаційно-технічних станів кіберфізичної системи та універсальна платформа побудови комплексних систем безпеки .....	161
<b>Розділ 8. Безпека кібернетичного простору кіберфізичної системи на основі концепції “об’єкт – загроза – захист” .....</b>	<b>166</b>
8.1. Комплексні системи безпеки інформаційних ресурсів: баз даних, баз знань, баз моделей, сховищ даних, масивів інформації .....	166
8.2. Комплексні системи безпеки інформаційних систем: модель тривірневого захисту на основі гарантоздатності .....	171
8.3. Комплексні системи безпеки інформаційних процесів на рівні: фаз, операцій, оброблення .....	183
<b>Розділ 9. Методологічні засади безпеки комунікаційного середовища кіберфізичних систем .....</b>	<b>191</b>
9.1. Методологія безпеки безпроводних технологій зв’язку – GSM, CDMA, WiMAX, LTE, сенсорних мереж – ZigBee, Wi-Fi, Bluetooth та хмарних обчислень .....	191
9.2. Комплексні системи безпеки інформаційних мереж на основі моделі OSI .....	211
9.3. Концептуальні підходи до захисту інформації в технологіях стаціонарного, стільникового та супутникового зв’язку .....	225
<b>Розділ 10. Безпека фізичного простору кіберфізичних систем .....</b>	<b>233</b>
10.1. Елементи фізичного простору кіберфізичних систем .....	233
10.2. Системна модель комплексної системи безпеки КФС “iPhone – Wi-Fi, Bluetooth – MEMS-давачі” .....	239
Висновки .....	244
Список літератури .....	247