

**Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Белгородський державний університет, Росія
Гірничо-металургійна академія АГН, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE),
Українська секція**

**Тези доповідей
Третьої Міжнародної
науково-практичної конференції
«Методи та засоби кодування, захисту й
ущільнення інформації»**

**м. Вінниця, Україна
20-22 квітня 2011 року**

**Тезисы докладов
Третьей Международной
научно-практической конференции
«Методы и средства кодирования, защиты и
сжатия информации»**

**г. Винница, Украина
20-22 апреля 2011 года**

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-
практичної конференції. м. Вінниця, 20-22 квітня 2011 року. –
Вінниця: ВНТУ, 2011. – 231 с.

ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-
практичної конференції з сучасних проблем кодування, захисту й ущіль-
нення інформації за п'ятьма основними напрямками: методи та засоби ко-
дування інформації; методи та засоби криптографічного захисту інформа-
ції; інформаційна безпека комп'ютерних систем; методи та засоби ущіль-
нення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

©Автори статей, 2011

©Упорядкування, Вінницький національний
технічний університет, 2011

МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З УРАХУВАННЯМ КОНКУРЕНТНОГО СЕРЕДОВИЩА

**А. В. Дудатьєв, к.т.н., доцент
Вінницький національний технічний університет**

Для реалізації захисту інформаційних ресурсів сучасної соціотехнічної системи (людина, суспільство, підприємство, держава) необхідно створення відповідної теоретичної бази, яка б дозволяла реалізувати у практичній площині відповідні управлінські рішення щодо процесів оцінювання та забезпечення необхідного рівня захисту інформаційних ресурсів. З урахування того, що життєдіяльність сучасних соціотехнічних систем відбувається у конкурентному середовищі, проблему забезпечення необхідного рівня інформаційної безпеки необхідно розглядати, як комплексну і розділити на дві такі задачі:

1. Захист власних інформаційних ресурсів;
2. Захист від інформаційного впливу конкурентів.

Оскільки перша задача за своєю постановкою є класичною то і її рішення може бути реалізовано з використанням відомих методів та засобів з урахуванням відповідного нормативно-правового забезпечення. Друга задача є відносно новою, її виникнення пов'язано з використанням спеціальних технологій, які пов'язані з проведенням спеціальних інформаційних операцій та атак (технології проведення інформаційної війни). Відомо, що метою будь-якої інформаційної війни є широкомасштабне оперування об'єктами конкуруючої сторони з метою знищення, перекручування інформаційних ресурсів, або нав'язування вигі-

дної інформації та застосування психологічного тиску з метою досягнення власної мети.

На прикладі функціонування підприємства можна розглянути вирішення сформульованих задач. Забезпечення інформаційної безпеки є одним з пріоритетних питань, яким повинна займатися служба безпеки (СБ) підприємства. Відомо чотири основні напрямки діяльності і відповідні задачі, що вирішує служба безпеки і які спрямовані на захист інформаційних ресурсів підприємства. Основні напрямки забезпечення інформаційної безпеки підприємства:

- захист інформації про поточний стан і переміщення різноманітних ресурсів, що може ідентифікуватися, як економічна безпека;
- захист інформації про стан нематеріальних активів та їх носіїв (персонал), що може ідентифікуватися як інформаційна безпека;
- захист засобів збереження, обробки і передачі інформації.

Досвід показує, що жодне з підприємств не може ефективно проводити захист власних інформаційних ресурсів і працювати в умовах постійної і жорстокої конкуренції, якщо воно не має якісної і достовірної інформації щодо діяльності потенційних конкурентів і стану відповідного сегменту ринку. Тому, для вирішення цієї проблеми, у складі СБ підприємства створюють так звану інформаційно-аналітичну службу (ІАС) підприємства. Основними функціями ІАС.

Запропонований підхід надає можливість отримати математичну модель системи інформаційної безпеки підприємства, яка має важливу властивість враховувати можливі зміни, як внутрішніх так і зовнішніх чинників, зокрема конфліктні ситуації, що впливають на рівень інформаційної безпеки об'єкту захисту.