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
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої 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 ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 004.7

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ ДЛЯ ІДЕНТИФІКАЦІЇ АТАК У КОМП`ЮТЕРНИХ МЕРЕЖАХ

Н. Р. Кондратенко, к.т.н., професор;
Г. С. Захарченко, студент;
С. М. Захарченко, к.т.н., доцент
Вінницький національний технічний університет
galka_kuzka@mail.ru

З розвитком комп`ютерних мереж значно зросла кількість та різноманітність атак на мережі. Деякі атаки відрізняються великою складністю, інші по силі будь-якому користувачу, який може навіть не підозрювати до яких наслідків призведе його діяльність. Залежно від цілі, атака може вивести з ладу систему або порушити цілісність чи конфіденційність інформації. Тому важливим і актуальним є питання ідентифікації несанкціонованих дій та їх, хоча б приблизної, мети, щоб якісно захистити мережу та інформацію в ній.

Кожна атака складається з трьох етапів: сбір інформації, реалізація, завершення атаки. Перший етап є однаковим для всіх видів атак, зловмисник збирає дані про систему, вивчає її особливості, перевіряє рівень захищеності. Найкраще і найлегше ідентифікувати атаку на цьому рівні, оскільки значно зростає активність зловмисника і його легше виявити.

Існують різні методи виявлення атак, основними з яких можна визначити такі: метод виявлення аномалій та

сигнатурний метод. Останній базується на описі відомих порушень або атак і якщо поведінка суб`єкта співпадає з описом атаки то суб`єкт вважається зловмисником. Основною перевагою сигнатурного методу є низький рівень помилок системи виявлення. Але система здатна виявити лише відомі для неї атаки, якщо модель атаки не міститься у базі даних сигнатур, вона не буде виявлена.

Метод виявлення аномалій ґрунтується на наявності певної «нормальної» поведінки суб`єкта, і відхилення від неї вважається аномальним. Недоліком цього методу є велика кількість помилкових тривог, пов`язана з тим, що важко точно задати граничні значення, щоб адекватно ідентифікувати аномальну діяльність. Водночас є великий плюс у тому, що метод виявлення аномалій дає можливість виявити раніше невідомі атаки. Ефективність системи виявлення атак сильно залежить від методів аналізу отриманої інформації. Історично найпершим таким методом був статистичний метод. Та останнім часом, з розвитком обчислювальної техніки та математики, до нього додались нові методики починаючи з нечіткої логіки та закінчуючи нейронною мережею. Об’єднуючи різні види аналізу можна значно підвищити точність визначення атаки і значно зменшити кількість помилок.