

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет
«Харківський політехнічний інститут»

ВІСНИК

**НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХПІ"**

Серія: «Механіко-технологічні системи та комплекси»

№ 20(1242)2017

Збірник наукових праць

Видання засноване в 1961 р.

Харків
НТУ «ХПІ», 2017

Вісник Національного технічного університету «ХПІ».Збірник наукових праць. Серія: Механіко-технологічні системи та комплекси. – Х.: НТУ „ХПІ” – 2017р. – No20(1242) – 130 с.

Державне видання

Свідоцтво Держкомітету з інформаційної політики України

КВ No5256 від 2 липня 2001 року

Мова статей – українська, російська, англійська.

Вісник Національного технічного університету «ХПІ» внесено до «Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук», затвердженого рішенням Атестаційної колегії МОН України щодо діяльності спеціалізованих вчених рад, від 15 грудня 2015р. Наказ № 1328 (додаток 8) від 21.12.2015р.

Координаційна рада:

Л. Л. Товажнянський, д-р техн. наук, проф. (**голова**);

К. О. Горбунов, канд. техн. наук, доц. (**секретар**);

А. П. Марченко, д-р техн. наук, проф.; Є. І. Сокол, член-кор. НАН України, д-р техн. наук, проф.; Є. Є. Александров, д-р техн. наук, проф.; А. В. Бойко, д-р техн. наук, проф.; Ф. Ф. Гладкий, д-р техн. наук, проф.; М. Д. Годлевський, д-р техн. наук, проф.; А. І. Грабчєнко, д-р техн. наук, проф.; В. Г. Данько, д-р техн. наук, проф.; В. Д. Дмитриєнко, д-р техн. наук, проф.; І. Ф. Домнін, д-р техн. наук, проф.; В. В. Єпіфанов, канд. техн. наук, проф.; Ю. І. Зайцев, канд. техн. наук, проф.; П. О. Качанов, д-р техн. наук, проф.; В. Б. Клепєков, д-р техн. наук, проф.; С. І. Кондрашов, д-р техн. наук, проф.; В. І. Кравченко, д-р техн. наук, проф.; Г. В. Лісачук, д-р техн. наук, проф.; О. К. Морачковський, д-р техн. наук, проф.; В. І. Ніколаєнко, канд. іст. наук, проф.; П. Г. Перерва, д-р екон. наук, проф.; В. А. Пуляєв, д-р техн. наук, проф.; М. І. Рищенко, д-р техн. наук, проф.; В. Б. Самородов, д-р техн. наук, проф.; Г. М. Сучков, д-р техн. наук, проф.; М. А. Ткачук, д-р техн. наук, проф.

Редакційна колегія серії:

Відповідальний редактор: Дьомін Д. О., д-р техн. наук, проф., НТУ «ХПІ»;

Заст. відповідального редактора: Акімов О. В., д-р техн. наук, НТУ «ХПІ», Харків,

Відповідальний секретар: Пензєв П. С., НТУ «ХПІ»;

Члени редколегії: Березуцький В. В., д-р техн. наук, НТУ «ХПІ», Харків, Дмитрієв В. В., д-р техн. наук, НТУ «ХПІ», Харків, Дудніков А. А., канд. техн. наук, ПДАА, Полтава, Заблоцький В. К., д-р техн. наук, ДДМА, Краматорськ, Заміховський Л. М., д-р техн. наук, ІФТУНГ, Івано-Франківськ, Євстратов В. О., д-р техн. наук, проф., НТУ «ХПІ», Харків, Погрібний М. А., проф., НТУ «ХПІ», Харків, Пономаренко О. І., д-р техн. наук, проф., НТУ «ХПІ», Харків, Соболь О. В., д-р фіз.-мат. наук, НТУ «ХПІ», Харків, Шоман О. В., д-р техн. наук, НТУ «ХПІ», Харків, Jozef Voynarovsky, проф., Сілезького політехнічного інституту, Польща, Rab Nawaz Lodhi, проф. Bahria University Islamabad Pakistan, Пакистан, Меркер Е. Е., д-р техн. наук, проф., Старооскольський технологічний інститут – філія Національного дослідницького технологічного інституту «Московський інститут сталі і сплавів», Росія

У 2015 р. Вісник Національного технічного університету «ХПІ», Серія: «Механіко-технологічні системи та комплекси», включений у довідник періодичних видань бази даних **Ulrich's Periodicals Directory (New Jersey, USA)**

Рекомендовано до друку вченою радою НТУ „ХПІ”

Протокол № 5 від «02» червня 2017 р.

МАТЕРІАЛОЗНАВСТВО

УДК 004.056.53

С. В. БАЛАКИН

ОРГАНИЗАЦИЯ ПРЕСЕЧЕНИЯ ВТОРЖЕНИЙ В КОМПЬЮТЕРНЫЕ СЕТИ АЛГОРИТМАМИ ВЫЯВЛЕНИЯ ИЗМЕНЕНИЙ

Розглядається моделювання системи постановки діагнозу шляхом аналізу ймовірності достовірності оцінки різних наборів станів структури проникнення комбінованих доказів симптомів для дерева діагностики, представленого деревом специфікації, щоб максимально точно визначити захищеність системи чи організму. Дослідження полягає в наданні необхідної теоретичної бази для використання приведених концепцій і теорій, які можуть комбінуватися з сучасними напрацюваннями для підвищення результатів ефективності виявлення вторгнень в комп'ютерній мережі.

Ключові слова: моделювання, діагностика, діагноз, вторгнення, алгоритми змін, теорія Демпстера-Шефера, комп'ютерна мережа, основне переконання, правдоподібність, проникливість.

Рассматривается моделирование системы постановки диагноза путем анализа вероятности достоверности различных наборов состояний в структуре проникновения и комбинированных доказательств симптомов для дерева диагностики, представленного деревом спецификации, чтобы максимально точно определить защищенность системы или организма. Исследование заключается в предоставлении необходимой теоретической базы для использования приведенных концепций и теорий, которые могут комбинироваться с современными наработками для повышения результатов эффективности обнаружения вторжений в компьютерной сети.

Ключевые слова: моделирование, диагностика, диагноз, вторжения, алгоритмы изменений, теория Демпстера-Шефера, компьютерная сеть, основное убеждение, правдоподобность, проницательность.

The modeling of the diagnostic system is considered. Analyzing the probability of estimating the various sets of states of the structure of the penetration of the combined evidence of symptoms for the diagnostic tree is presented by the specification tree in order to ascertain precisely the security of the system or organism. Main aim of the study is to provide the necessary theoretical basis for using the above concepts and theories that can be combined with current developments to enhance the effectiveness of detecting intrusions in a computer network. Given description shows improved results that can improve diagnosis functions and can be used in real-time computer systems.

Keywords: Modeling, diagnosis, diagnosis, invasion, algorithms of change, Dempster-Shafer theory, computer network, basic belief, plausibility, insight.

Введение. В области компьютерной безопасности много ресурсов направлено на повышение эффективности защиты пользователей от несанкционированных действий. Одним из способов повышения безопасности компьютерной системы является использование систем обнаружения вторжений (СОВ). Метод диагностирования очень тесно связан с СОВ, но основан на принципах и способах развитых в медицине. С помощью информатизации в сфере медицины становится возможным и развитие новых вех компьютерных технологий. Основная сложность при их проектировании - это подбор правильной технологической и методологической базы, что позволит применить такие методы в реальных условиях. Эти методы получили название диагностическое обнаружения вторжений (ДОВ).

В ДОВ мониторятся соответствующие функции системы, таким же образом как в медицине проводится обследование при симптомах болезни. Симптомы используют значение обследований, чтобы вычислить вероятность обнаружения определенного недуга в организме человека. Теория Демпстера-Шафера (ТДШ) применяется для характеристики таких убеждений, оперируя основными понятиями по комбинированию и использованию операторов слияния.

Разработанная система постановки диагноза путем анализа вероятности достоверности оценки различных наборов состояний структуры проникновения комбинированных доказательств симптомов для дерева диагностики, представленного деревом специ-

фикации, чтобы максимально точно определить защищенность системы или организма.

Анализ литературных данных и постановка проблемы. Существующие программные решения имеют определенную поддержку с точки зрения предотвращения и обнаружения вторжений, но в них отсутствует возможность диагностирования. Данные системы имеют недостатки в своевременности детектирования атак, но использование методов диагностирования может положительно повлиять на быстродействие и надежность известных методов, минимизируя затраты на проведение мониторинга сети и потоков. Основная идея заключается в сборе информации на нескольких архитектурных уровнях, с использованием нескольких фильтров безопасности для выполнения корреляционного анализа симптомов вторжения. Много таких работ базируется на теории Демпстер-Шафера (ТДШ), которая разработана Гленном Шафером и Артуром Демпстер и описана в работах [15, 63]. Теория отрабатывалась и развивалась в работах [14, 64, 88, 84, 62].

Идея сбора информации от источников принадлежит Джону Ф.Ф., и обосновывает само понятие атаки. Данные наработки были описаны теоретически в работах [3], [4] и [5]. Представленные работы используют понятие корреляции и мультианализа, но не решают проблему диагностики аномалий в системе. Актуальность данной статьи в том, что данная технология может расширить возможности систем обнаружения вторжений поднимая их на качественно новый уровень.

© С. В. Балакин. 2017