ограничений и связей между объектами конструкции, что существенно сокращает сроки проектирования. Реализация метода и его использование в составе действующей САПР показала его эффективность и жизнеспособность. Безусловно, что при использовании в конструкциях, существенно отличающихся от конструкций корпусной мебели, потребуется, возможно, наложение дополнительных связей конструктором.

ЛІТЕРАТУРА

[1] Ли К. (2004). Основы САПР (CAD/CAM/CAE). СПб.:Питер.

[2] Малюх В. (2013). Введение в современные САПР. Москва:ДМК.

[3] Ершов, А. (2007). Новый метод моделирования задач параметрического проектирования. Все возможности вариационного подхода при эффективности иерархического. САПР и графика, 9, 37-40.

[4] Булгаков, В. (2013). Инструменты для виртуозного исполнения работы инженера-конструктора в новой версии КОМПАС-3D V14. САПР и графика, 1, 11-16.

[5] Бунаков, П. (2009). БАЗИС 8.0: новые возможности автоматизации мебельных предприятий. САПР и графика, 9, 21-24.

[6] Програмне забезпечення для професійного виробництва меблів. Астра Конструктор Меблів. Взято з http://www.astrapro.com.ua/default.asp?page=astra-konstruktor-mebeli

Parametric modeling of composition objects in the design of the case furniture

Partas Viktor[1], Udovitsky Dmitro[2]
[1]National University of Shipbuilding
[2]Technos LTD

Abstract. The paper presents a modified method of variational parametric modeling, which involves the formation of constraints and relationships between objects depending on the design features. The method is implemented as part of software for cabinet furniture design and allows to significantly reduce the overall design process.

Keywords: automated design, parameterization, variational modeling, cabinet furniture

УДК 004.4:004.7

ПРОГРАМНІ СИСТЕМИ ДЛЯ ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК

Пасюк Б.Б.[1], Фаріонова Т.А.[2]
[1]аспірант кафедри програмного забезпечення автоматизованих систем Національного університету кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна,
bwolverine44@gmail.com
[2]кандидат технічних наук, доцент кафедри програмного забезпечення автоматизованих систем Національного університету кораблебудування імені адмірала Макарова,
м. Миколаїв, Україна,
tetyana.farionova@nuos.edu.ua

Анотація. Розглядаються програмні засоби, що мають функціональні можливості для визначення мережевих атак, та визначення аномалій в комп'ютерній мережі. Проведено аналіз останніх версій систем визначення атак (СВА), а також досліджень та публікацій на задану тему. Внаслідок проведеного порівняльного аналізу програмних систем виявлення мережевих атак та аномального трафіку було обґрунтовано доцільність розробки програмного рішення, що забезпечує захист від загроз 0-го дня (zero-day threats) та інших мережевих атак.

Ключові слова: мережеві атаки, аномальний трафік, комп'ютерні мережі, системи визначення атак, неавторизована сторона, інформаційна система.

Стрімкий розвиток та поширення систем електронних комунікацій або комунікаційних систем спеціального призначення (КС) обробки інформації вимагає забезпечення постійного контролю коректного їх використання та впливу кіберзагроз на стан та властивості системи (хостову або мережеву їх частину). Основними особливостями побудови та застосування КС є динамічна топологія, децентралізоване управління елементами та системами, спільний доступ вузлів до середовища передачі трафіку, масштабованість, необхідність збору значної кількості інформації про стан мережі на різних рівнях мережевої моделі OSI.

Одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень до інформаційних систем (ІС) з боку неавторизованої сторони (НАС).

Система виявлення атак (англ. Intrusion Detection System, IDS) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними в основному через глобальну мережу Інтернет. IDS аналізує отриманий трафік і сигналізує при виявленні підозрілої активності. Виявлення порушення безпеки проводиться з використанням евристичних правил та аналізу сигнатур відомих комп'ютерних атак. Найбільш розумним рішенням в масштабованих комп'ютерних мережах є «зеркалювання» трафіку на сервер IDS за для зменшення навантаження на сам сервер та підвищення роботоспроможності всєї комп'ютерної мережі.

Як правило, методи виявлення атак розділяють на методи виявлення зловживань і аномалій [1]. Зловживання засновані на використанні існуючих недоліків ІС. Основною відмінністю між аномалією і зловживанням є те, що аномалія – це процес, який виникає перед можливим вторгненням в систему або вказує на наявність вже існуючої атаки. Фактично, аномалія – це відхилення від нормального стану системи, незвичайна активність в ній, що може свідчити про певні атакуючі дії. Слід зазначити, що аномалія може виникнути і за інших причин, наприклад, внаслідок неправильної роботи системи.

Саме тому за допомогою ефективного аналізу аномалій, що виникають у системі, можна попередити кібератаки певних типів і вчасно вжити необхідних заходів щодо їх блокування та захисту ІС. Варто сказати, що широке використання сучасних засобів захисту від кібератак не гарантує безпеки на належному рівні, оскільки останнім часом:

- зростають атаки, спрямовані на корпоративні системи, публічні, конфіденційні та державні інформаційні ресурси;
- кібератаки, постійно модифікуються, удосконалюються і стають більш регулярними;
- виявлення кібератак класичними засобами захисту не завжди є ефективним;
- частішають випадки здійснення складних атак на ІС [1-3].

В таблиці 1 наведені функціональні можливості найбільш поширених програмних систем [4] для визначення мережевих атак.

Відповідно до проведеного аналізу можна зазначити, що сучасні програмні засоби СВА аномального принципу, в основному, засновані на математичних моделях, що потребують багато часу для отримання статистичних даних, реалізацію процесу навчання (в основному для нейромережевих систем) та здійснення інших складних і довготривалих підготовчих процедур.

Одним з недоліків СВА є закладений в неї процес створення відповідного профілю нормального стану ІС, а при її модифікації та інших змінах набрана статистика не має необхідної повноти та є неактуальною. Більш ефективні у цьому відношенні є експертні підходи, що засновані на використанні знань та досвіду спеціалістів відповідної предметної області.

Крім того, побудова відповідних методів, технічних рішень та створення засобів (СВА, виявлення кібератак та інші), орієнтованих на обробку слабкоструктурованих даних з метою

встановлення фактів несанкціонованого доступу до ІС є основою для успішної протидії відповідним кібератакам.

Таблиця 1 – Зведені дані функціональних можливостей розглянутих СВА

№	СВВ	Види кібератак		Адаптивність	Відкритість	Методи виявлення атак											Масштабованість	Система СВА	Мережева СВА	Рівень спостереження		Підтримка ОС			
		Зловживання	Аномалії			Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль змін	Кластерний	Динамічний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин				Реакція на кібератаку	Захищеність	UNIX	Linux	Windows	MacOS
1	Snort	+	+	-	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	+	+	+	-
2	Prelude SIEM	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	+	+	+	+	+	-	-
3	NetSTAT	+	+	+	+	-	-	+	-	+	-	-	-	-	-	-	+	+	+	+	+	+	+	-	-
4	Shadow	+	+	-	-	-	-	-	-	+	-	-	-	-	-	-	+	-	+	-	+	+	+	-	-
5	ASAX	+	-	-	+	+	-	-	-	-	-	-	-	-	-	-	+	+	-	-	-	+	+	-	-
6	Bro	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	-	-	+	+	-	+	+	-	+
7	OSSEC	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	+	-	+	+	+	+	+	+
8	Cisco IPS	+	+	+	-	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	-
9	Arbor Networks Spectrum	+	+	+	-	-	+	+	-	-	-	+	-	-	-	-	+	+	+	+	-	+	+	+	-
10	InfoWatch ASAP	+	+	+	-	-	+	+	-	-	-	-	-	-	-	-	+	+	+	-	-	+	+	+	+
11	IPS	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	+	+	+	+	+	-	-	+	-
12	Tipping Poing NGIPS	+	+	+	-	-	-	+	-	-	-	+	+	-	-	-	+	+	+	+	+	-	-	+	+
13	Axoft invGUARD	+	+	-	-	-	+	+	-	-	-	+	-	+	+	-	+	+	+	-	-	+	+	-	-
14	DefensePro	+	+	+	-	-	+	+	-	-	-	-	-	+	-	-	+	-	+	+	+	+	+	+	+
15	KATA Platform	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	+	+	+	+	+	+	+	+	+
16	Suricata	+	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	-	+	+	+	+
17	Samhain	+	+	+	+	-	+	-	-	-	-	+	-	+	-	-	+	+	-	+	+	+	+	+	+
18	Security Onion	+	+	+	+	-	+	+	-	+	-	+	-	+	-	-	+	+	+	+	-	+	+	-	-

Більшість СВА достатньо дорогі, мають закритий код, потребують кваліфікованого налаштування (під певні вимоги організації та сервіси), яке можуть здійснити тільки висококваліфіковані фахівці.

Результати аналізу сучасних СВА показав, що існуючі засоби не є ефективними проти нових типів вторгнень. Тому, розробка відповідних методів та математичної моделі для ідентифікації аномальних станів для СВА з метою розширення їх функціональних можливостей (за рахунок засобів, що використовують відповідний математичний апарат), дозволить цим системам бути дієвими щодо виявлення нових типів кібератак (0-day атак), які характеризуються невстановленими або нечітко визначеними критеріями у відповідному гетерогенному середовищі. Такі розширені можливості СВА дозволять їм, фактично, залишатися функціональними у потенційно небезпечному оточенні характерному впливам різноманітних загроз.

ЛІТЕРАТУРА

[1] Корченко А. А., Ахметова С. Т. Классификация систем обнаружения вторжений. Інформаційна безпека. К. : НАУ, 2014. № 1 (13). № 2 (14). С. 168-175.

[2] Зоріна Т. І. Системи виявлення і запобігання атак в комп'ютерних мережа. Вісник східноукраїнського національного університету імені Володимира Даля, 2013. № 15 (204). С. 48-52.

[3] Мєшков В. І., Віролайнен В. О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. Проблеми безпеки інформації в інформаційно-комунікаційних системах. К.: НТУУ КПІ РТФ, 2015. №. 1. С. 1-4.

[4] Best FREE Intrusion Detection Software in 2020. Режим доступу URL: https://www.addictivetips.com/net-admin/intrusion-detection-tools/ (дата звернення 27.06.2021).

Software systems for detecting network attacks

Pasyuk Bohdan Borysovych[1], Farionova Tetyana Anatoliivna[2]

[1,2]Admiral Makarov National University of Shipbuilding, Heroiv Ukrainy avenue, 9, Mykolaiv, 54025, Ukraine

Abstract. Software tools that have the functionality to detect network attacks and detect anomalies in a computer network are discussed. An analysis of the latest versions of intrusion detection system (IDS), as well as research and publications on a given topic were done. As a result of the comparative analysis of software systems for detecting network attacks and anomalous traffic, the expediency of developing a software solution that provides protection against 0-day threats (zero-day threats) and other network attacks was substantiated.

Keywords: network attacks, abnormal traffic, computer networks, intrusion detection system, unauthorized party, information system

УДК 330.341.1:339.13(477)

ІННОВАЦІЙНА СПРОМОЖНІСТЬ РЕГІОНІВ ЯК ЧИННИК ЕКОНОМІЧНОГО РОЗВИТКУ

Ревенко Н. Г.[1]

[1]кандидат економічних наук, професор, професор кафедри економіки Херсонської філії Національного університету кораблебудування імені адмірала Макарова, м. Херсон, Україна

bobelur@meta.ua

Анотація. Розглянуто проблемні питання забезпечення інноваційної спроможності розвитку регіонів. Зазначено необхідність підвищення інноваційної компоненти освіти випускників закладів вищої освіти. Запропоновано удосконалення системи організації використання інноваційних ідей на регіональному рівні.

Ключові слова: інноваційна спроможність, розвиток, економіка, професійна освіта, інноватизація, регіональний рівень.

Сучасний світ характеризується інтенсивним розвитком і глибокими системними змінами, які супроводжують всі напрями діяльності суспільства. Це впливає на інтенсивність появи інноваційних ідей, нових технологій, товарів, послуг, зміни в організації виробництва, в управлінні виробничими і економічними процесами, створюючи умови для інтеграції багатьох наукових галузей і наукових досягнень. Здійснювані зміни і нові технології мають одну спільну ключову ознаку. Вони створюються завдяки потужним можливостям нових інформаційних технологій, які, у свою чергу, є продуктом інноваційних відкриттів та інноваційної діяльності. Комп'ютерні можливості, доступність великих обсягів інформації, хмарні технології, технології 3D-друку, передова робототехніка та інші можливості інформаційних технологій стають