Наукові перспективи
Видавнича група

СУЧАСНІ АСПЕКТИ МОДЕРНІЗАЦІЇ НАУКИ: СТАН, ПРОБЛЕМИ, ТЕНДЕНЦІЇ РОЗВИТКУ

у рамках роботи Видавничої групи
"Наукові перспективи"

Матеріали XXIII Міжнародної науково-практичної конференції (07 серпня 2022 року, м. Фікірх (Люксембург) дистанційно)

Мирного неба!
Вільної України!

Міжнародний економічний інститут (Есеніце, Чехія)
Central European Education Institute (Братислава, Словаччина)
Національний інститут економічних досліджень (Батумі, Грузія)
Казахський національний університету імені аль-Фарабі (Казахстан)
Інститут філософії та соціології Національної Академії Наук Азербайджану (Баку, Азербайджан)
Батумський навчальний університет навігації (Батумі, Грузія)
Регіональна Академія Менеджменту (Казахстан)
Громадська наукова організація «Всеукраїнська Асамблея докторів наук з державного управління» (Київ, Україна)
Громадська організація «Асоціація науковців України» (Київ, Україна)
Університет Новітніх Технологій (Київ, Україна)
Міждержавна гільдія інженерів консультантів (Київ, Україна)
у рамках Видавничої групи «Наукові перспективи»

СУЧАСНІ АСПЕКТИ МОДЕРНІЗАЦІЇ НАУКИ: СТАН, ПРОБЛЕМИ, ТЕНДЕНЦІЇ РОЗВИТКУ

Матеріали XXIII-ої Міжнародної науково-практичної конференції

(07 серпня 2022 року, м. Дікірх (Люксембург), дистанційно)

2022 р.

International Economic Institute s.r.o. (Jesenice, Czech Republic)
Central European Education Institute (Bratislava, Slovakia)
National Institute for Economic Research (Batumi, Georgia)
Al-Farabi Kazakh National University (Kazakhstan)
Institute of Philosophy and Sociology of Azerbaijan
National Academy of Sciences (Baku, Azerbaijan)
Batumi Navigation Teaching University (Batumi, Georgia)
Regional Academy of Management (Kazakhstan)
Public Scientific Organization "Ukrainian Assembly of Doctors of Sciences in Public Administration" (Kyiv, Ukraine)
Public Organization Organization "Association of Scientists of Ukraine" (Kyiv, Ukraine)
University of New Technologies (Kyiv, Ukraine)
Interstate Consultants Engineers Guild (Kyiv, Ukraine)
within the Publishing Group "Scientific Perspectives"

MODERN ASPECTS OF MODERNIZATION OF SCIENCE: STATUS, PROBLEMS, DEVELOPMENT TRENDS

Materials of the 23th International Scientific and Practical Conference

August 7, 2022, Diekirch (Luxembourg) remotely

2022

УДК 001.3-048.35:0/9](06)
С91

Схвалено до друку Президією Громадської наукової організації «Всеукраїнська Асамблея докторів наук з державного управління» (Рішення № 2/8-22, від 03.08.2022)

Матеріали конференцій індексуються у міжнародній пошуковій системі Google Scholar

Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XXIII Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Дікірх (Люксембург): ГО «ВАДНД», 07 серпня 2022 р. 335 с.

У матеріалах XXIII-ої Міжнародної науково-практичної конференції висвітлені: проблемні аспекти забезпечення безпеки національної економіки, її стабілізації та сталості, здатності до постійного оновлення, вдосконалення; дослідження щодо здійснення освітнього процесу в закладах післядипломної педагогічної освіти в умовах дистанційного та змішаного навчання; особливості формування соціально-психологічних особливостей «soft skills» у майбутніх психологів; питання пов'язані з протидією проявам корупції, особливо у секторі оборони України.

Матеріали будуть корисними та цікавими науковцям, викладачам, педагогам-практикам, представникам органів державної влади та місцевого самоврядування, здобувачам вищої освіти, громадсько-політичним діячам, а, також, усім, хто цікавиться міжнародним досвідом реалізації інноваційних освітніх процесів.

Матеріали подані в авторській редакції. Відповідальність за зміст та орфографію матеріалів несуть автори.

Тогобицька Д. М., Бєлькова А.І. 256
ОСОБЛИВОСТІ ВПЛИВУ ЕНЕРГЕТИЧНИХ ДОБАВОК НА ФІЗИКО-ХІМІЧНІ ВЛАСТИВОСТІ КІНЦЕВОГО ДОМЕННОГО ШЛАКУ

СЕКЦІЯ 9. 261
СОЦІОЛОГІЯ

Толстих Н.В. 261
НЕСТАНДАРТНА ЗАЙНЯТІСТЬ В СУЧАСНОМУ СВІТІ: ВИЗНАЧЕННЯ І НАПРЯМИ АНАЛІЗУ

СЕКЦІЯ 10. 266
ТУРИЗМ

Єрко І.В. 266
SWOT-АНАЛІЗ ГОТЕЛЬНО-РЕСТОРАННОГО ГОСПОДАРСТВА ЛУЦЬКОЇ ТЕРИТОРІАЛЬНОЇ ГРОМАДИ

Пеняк П. 270
НЕМАТЕРІАЛЬНА КУЛЬТУРНА СПАДЩИНА ЗАКАРПАТТЯ ЯК ТУРИСТИЧНИЙ РЕСУРС

СЕКЦІЯ 11. 276
МАРКЕТИНГ

Krapko O.M., Radchenko O.A. 276
TENDENCIES OF MARKETING STRATEGIC PRIORITIES OF COMPANY DEVELOPMENT IN THE DIGITAL ECONOMY

СЕКЦІЯ 12. 282
КІБЕРБЕЗПЕКА

Inozemtseva O.B. 282
CYBER SECURITY IN THE PROCESS OF STAFF TRAINING IN THE FIELD OF CIVIL DEFENSE

Одарущенко О.Б., Шишацький А.В., Налапко О.Л., Шкнай О.В., Кравченко С.І., Протас Н.М. 286
МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕВОЛЮЦІЙНОГО ПІДХОДУ

СЕКЦІЯ 13. 303
ГРОШІ, ФІНАНСИ І КРЕДИТ

Корнівська В.О. 303
ФІНАНСОВО-ІНСТИТУЦІЙНИЙ ПРОСТІР УКРАЇНИ У КОНТЕКСТІ ГЛОБАЛЬНОГО ТРАНСФОРМАЦІЙНОГО ПРОЦЕСУ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ

Шульга Н.П., Белянко Л.Л. 309
РИЗИК-АПЕТИТ БАНКІВ УКРАЇНИ

СЕКЦІЯ 14. 315
МЕНЕДЖМЕНТ

Трушкіна Н.В. 315
ЩОДО КОНЦЕПЦІЙ ФОРМУВАННЯ ЛОГІСТИЧНИХ СИСТЕМ

СЕКЦІЯ 15. 327
СУДОВА ЕКСПЕРТИЗА ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Федоренко В.Л., Гайдай О.Д., Шутович В.В. 327
ҐЕНЕЗИС І РОЗВИТОК СУДОВОЇ ЕКСПЕРТИЗИ ОБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В НЕЗАЛЕЖНІЙ УКРАЇНІ (1991-2022 РР.)

Одарущенко О.Б.
кандидат технічних наук, доцент
доцент кафедри інформаційних систем і технологій,
Полтавський державний аграрний університет
м. Полтава, Україна

Шишацький А.В.
кандидат технічних наук, старший дослідник
начальник відділу досліджень роботизованих систем,
Центр дослідження трофейного та
перспективного озброєння та військової техніки
м. Київ, Україна

Налапко О.Л.
доктор філософії
старший науковий співробітник
науково-дослідної лабораторії,
Центральний науково-дослідний інститут
озброєння та військової техніки
Збройних Сил України
м. Київ, Україна

Шкнай О.В.
кандидат технічних наук
провідний науковий співробітник
науково-дослідного відділу,
Військова частина А 1906,
м. Київ, Україна

Кравченко С. І.
кандидат технічних наук, доцент
доцент кафедри інженерії програмного забезпечення,
Національний авіаційний університет
м. Київ, Україна

Протас Н. М.
кандидат сільськогосподарських наук, доцент
доцент кафедри інформаційних систем і технологій,
Полтавський державний аграрний університет
м. Полтава, Україна

МАТЕМАТИЧНА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕВОЛЮЦІЙНОГО ПІДХОДУ

Аналіз останніх воєнних конфліктів, у тому числі результатів російського воєнного вторгнення на територію України, свідчить про збільшення кількості кібератак на інформаційно-телекомунікаційні системи спеціального призначення (ІТС СП), які використовуються не лише у воєнній сфері а й інших сферах людської діяльності для автоматизації вирішення різноманітних інформаційних завдань. Дані системи представляють собою функціонально пов’язану сукупність програмно-апаратних засобів обробки і обміну інформацією, таких як: обчислювальна техніка, тобто комп'ютери; телефонні канали зв'язку та система доступу до каналів зв'язку (комутаційне обладнання і регламенти їх використання) [1, 2]. Саме від їх працездатності залежить можливість вирішення більшості життєво важливих завдань.

Разом з тим, паралельно із удосконаленням засобів та структури ІТС СП, розвитком технологій обміну даними,

розвиваються і технології здійснення кібератак на комп'ютерні мережі з обмеженим доступом. На даний час можна виділити такі основні типи мережевих атак як: сніффер пакетів; IP-спуфінг; парольні атаки; атаки на рівні додатків із використанням слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP); мережева розвідка та соціальна інженерія. Для вирішення задач виявлення та запобігання мережевим атакам використовують наступний науково-методичний апарат:

моделі виявлення: хостова (host-based), мережева (network-based);

методи запобігання: статистичного аналізу, нечіткої логіки, побудови експертних систем тестування на проникнення, генетичні алгоритми, штучні нейронні мережі, прихованої марківської моделі, аналізу переходу зі стану в стан, прогнозованих шаблонів та Data mining.

Найбільш вживаними при створенні систем захисту інформації є використання нейронних мереж та генетичних алгоритмів

Отже, для забезпечення оперативне реагування на різкі зміни стану та умов функціонування ІТС СП внаслідок проведення кібератак

вимагає удосконалення науково-методичного апарату для підвищення ефективності функціонування систем захисту інформації в ІТС СП від мережевих атак.

Аналіз наукової і технічної літератури показав відсутність на даний час єдиного підходу до комплексного рішення проблеми створення ефективної системи захисту інформації для ІТС СП [3, 4].

Існуючі системи захисту інформації не дозволяють оперативно протидіяти сучасним мережевим загрозам та вимагають участі адміністратора для контролю та управління

трафіком мережи ІТС СП, що суттєво обмежує можливості ІТС СП. Адаптивна парадигма, що пропонується авторами статті, поєднує методи виявлення, ефективні за відсутності апріорної інформації про динамічні характеристики ІТС СП, причому при використанні цих методів в процесі функціонування адаптивної системи захисту інформації з обмеженим доступом збирається апостеріорна інформація про динаміку зміни стану даних в мережі ІТС СП [6, 7].

Під критерієм ефективності функціонування системи захисту інформації ІТС СП в умовах здійснення кібератак будемо вважати стійкість каналів передачі даних до впливу активних (модифікування повідомлень, повторне використання повідомлень, вставлення фальшивих повідомлень, маскарад під авторизований об'єкт та відмова в обслуговуванні) та пасивних (протиправного розкривання інформації без змінення стану системи) загроз.

Враховуючи існуючі можливості системи захисту інформації із виявлення для забезпечення своєчасного реагування на кіберінциденти та кібератаки пропонується застосовувати удосконалену математичну модель системи захисту інформації у мережах ІТС СП.

Отже, *об'єктом дослідження* є процес визначення класу мережевої атаки у ІТС СП. А *метою зазначеного дослідження* слід вважати підвищення стійкості функціонування ІТС СП за рахунок використання удосконаленої математичної моделі системи захисту від мережевих атак на основі еволюційного підходу.

Виклад основного матеріалу дослідження. На даний момент машинне навчання активно застосовується в багатьох сферах: оптичному розпізнаванні символів, ідентифікації біометричних показників, виявленні індикаторів кіберзагроз та ін. Але в той же час при використанні машинного навчання

виникає ряд труднощів з ідентифікацією деструктивного впливу на ІТС СП [7–10].

В зазначеному дослідженні під навмисним деструктивним впливом на ІТС СП будемо розуміти: навмисні перешкоди – шумові та імітаційні; кібернетичні інциденти та атаки.

За визначенням виявлення деструктивного впливу на ІТС СП включає в себе не тільки ідентифікацію по шаблонам, проте і детектування впливу, що раніше не зустрічався. Разом з тим методи машинного навчання в контексті постановки такого завдання спрямовані всього лише саме на пошук взаємозв'язків і закономірностей функціонування ІТС СП, знаходженні активності, що схожа на ту, що раніше зустрічалася в навчальній вибірці [11].

Застосування інструментів машинного навчання в готовому вигляді до завдання виявлення деструктивного впливу на ІТС СП призводить до великої кількості не виявлених впливів та дезорганізації самої ІТС СП. Насамперед це зумовлено високою динамікою обміну даними та неоднорідним трафіком, що циркулює в ІТС СП. Крім того, важко відстежити циклічність або сезонність такого обміну [11–15].

В даному дослідженні для ідентифікації деструктивного впливу на ІТС СП пропонується використати адаптовану математичну модель штучної імунної системи побудовану на синтетичній теорії еволюції, яка описується:

$$AISEA = \langle D_\tau, D_M, S_A, S_N, G, R, \Psi \rangle, \quad (1)$$

де $D_\tau \subset D$ – набір часових імунних детекторів, D_M – набір імунних детекторів пам'яті, $S_A \subset S$ – навчальна вибірка, що складається з аномальних екземплярів (набір відомих

варіантів втручання в мережу ІТС СП), $S_N \subset S$ – тестова множина, що складається з нормальних екземплярів (множина критеріїв оцінки захищеності інформації в мережі ІТС СП), $D = D_\tau \bigcup D_M$ – набір імунних детекторів, $G = \{G_1, ..., G_K\}$ – стратегії генетичної оптимізації імунних детекторів, $R: D \times 2^{S_A} \times 2^{S_N} \times G \to D$ –правило навчання імунних детекторів, S – набор можливих вхідних об'єктів, $\Psi: D \times S \to \mathbb{R}_+$ – функція обчислення аффіності (правило відповідності) між імунним детектором $d \in D$ та тестовим об'єктом $s \in S$, де $\mathbb{R}_+ = \mathbb{R} \bigcap 0, +\infty)$.

Кожен імунний детектор $d \in D$ описується як кортеж наступного виду:

$$d = \langle representation, threshold, life\_time, state \rangle, \quad (2)$$

де

$representation \in \{BitString, RealVector, NeuralNetwork, PetrNet..., \}$ – внутрішнє представлення (внутрішня структура) імунного детектора *d*, який може бути заданий як двійковий рядок з правилом *r*-неперервних бітів (*BitString*), дійсний вектор (*RealVector)*, штучна нейронна мережа (*NeuralNetwork*), мережа Петрі (*PetriNet*) та ін., $threshold \in \mathbb{R}_+$ – поріг активації імунного детектора *d*, $life\_time \in \mathbb{R}_+$ – термін дії імунного детектора *d*, $state \in \{immature, semimature, mature, memory\}$ – поточний стан імунного детектора (1), який може представляти собою незрілий, напівзрілий, зрілий стани або стан, що відповідає детектору пам'яті $\mathbb{R}_+^* = \mathbb{R}_+ \cup \{+\infty\}$.

Загальний підготовчий процес побудови параметрів штучної імунної системи для ідентифікації деструктивного впливу на ІТС СП може бути описаний таким чином:

1. Визначення корегувального коефіцієнту на ступінь інформованості сили та засоби деструктивного впливу на ІТС СП. Ступінь інформованості може бути: повна невизначеність, часткова невизначеність, повна обізнаність

2. Вибір внутрішньої структури кожного детектора $d \in D : representation$.

3. Формування навчального набору даних S_A, що містить заздалегідь відібрані "чужі,, пакети даних.

4. Формування тестового набору даних S_N, що містить заздалегідь відібрані "свої,, пакети даних.

5. Вибір стратегії генетичної оптимізації імунних детекторів.

6. Вибір алгоритму навчання R імунних детекторів D в залежності від їх внутрішнього представлення [6].

7. Вибір правила відповідності Ψ між імунним детектором та вхідним об'єктом.

Фактично, запропонована модель штучної імунної системи – це набір імунних детекторів, представлених у вигляді часових детекторів і детекторів пам'яті, в сукупності із заданим алгоритмом їх навчання, який приймає як вхідні аргументи детектор, що налаштовується d, підмножини двох наборів даних (набору S_A, що складається з "чужих,, пакетів даних, та набору S_N, що складається зі "своїх,, пакетів даних), а також стратегію генетичної оптимізації.

Причому набір даних призначається для першого попереднього налаштування імунних детекторів, а роль набору даних S_N полягає в фільтрації навчених детекторів. Стратегії генетичної оптимізації імунних детекторів включають деякий набір генетичних операторів (кросоверу, мутації, інверсії) та їх комбінацій для зміни параметрів імунного детектора після його клонування. Правило навчання імунних детекторів є двокроковою процедурою. На першому

кроці імунні детектори навчаються виключно на елементах набору даних S_A та піддаються клональній селекції, в процесі якої створені копії імунних детекторів мутують згідно з обраною стратегією. $G' \in G$. З набору детекторів, представленого виробленим нащадків і вихідним детектором, відбираються ті детектори, які є найбільш придатними по відношенню до елементів набору згідно з обраним правилом відповідності Ψ.

Ця фаза повторюється кілька разів для формування напівзрілих детекторів. На другій фазі навчання ці детектори перевіряються на відповідність “своїм,, об’єктам: ті з них, які помилково активуються, знищуються, заново ініціалізуються та навчаються. В рамках цієї моделі кожен імунний детектор піддається кільком етапам диференціювання. На початку свого розвитку кожен детектор ініціалізується довільним чином відповідно до свого внутрішнього уявлення. У процесі функціонування штучної імунної системи часові детектори здійснюють запис параметрів деструктивного впливу на ІТС СП в базу даних, що оновлюється S_{A^*} у разі виявлення.

Усі імунні детектори, крім детекторів пам’яті, мають кінцевий термін життя. Якщо протягом даного терміну життя вони не виявили жодного деструктивного впливу на ІТС СП, вони піддаються повторному навчанню на розширеному наборі даних, що містить елементи S_A та S_{A^*}. У той же час, якщо імунний детектор розпізнав деструктивний вплив на ІТС СП, його термін життя збільшується. На відміну від них, детектори пам'яті мають нескінченний термін життя і не беруть участі в наповненні оновлюваного набору деструктивного впливу.

Для виявлення кожного класу деструктивного впливу $c \in C$ виділяється кілька імунних детекторів, що

об'єднуються в клас детекторів $D_{\varsigma(C)}, \left(\bigcup_{c \in C} D_{\varsigma(C)} = D \right)$. Кожен із детекторів $d \in D_{\varsigma(C)}$ використовує глибоке навчання, запропоноване в роботі [6] на різних випадкових підвиборках множин S_A та $S_N - S_A^{(d)}$, и $S_{A^*}^{(d)}$ які, можливо, містять деякі дублюючі та переупорядковані об'єкти з вихідних наборів. Тим самим досягається різноманітність імунних детекторів усередині $D_{\varsigma(C)}$.

Відповідно під *q*-ою групою детекторів розуміється набір детекторів $D_{\varsigma(C)} \quad \left(\bigcup_{q=1}^{m} D^{(q)} = D \right)$, m – число класів деструктивного впливу на ІТС СП), які повністю покривають задану множину класів атак. Якщо детектор *d* реагує на будь-який елемент $s' \in S_N^{(d)}$ тобто якщо $\exists s' \in S_N^{(d)} \Psi\left(d, s'\right) > \min_{s \in S_A^{(d)}} \Psi\left(d, s\right)$, то детектор d піддається апоптозу та заміні новим довільно згенерованим детектором. Для кожного класу деструктивного впливу $c \in C$ визначається рівно один детектор пам'яті $d_m^{(C)}$ – детектор, який задовольняє вимозі максимальної пристосованості до розпізнавання об'єктів $S_A^{\left(d_m^{(C)}\right)} \bigcap C$. Таким чином, набір імунних детекторів пам'яті може бути визначений таким чином:

$$D_M = \bigcup_{c \in C} \left\{ \arg\max_{d \in D_{\varsigma(C)}} \left(\frac{\sum_{s \in S_A^{(d)} \bigcap C} \Psi\left(d, s\right)}{\#\left(S_A^{(d)} \bigcap C \right)} \right) \right\}. \qquad (3)$$

Набір часових імунних детекторів визначається наступним чином:

$$D_\tau = D \Big/ D_M \,. \tag{4}$$

Поріг активації імунного детектора $d \in D$, навченого на наборах $S_A^{(d)}$ та $S_N^{(d)}$ обчислюється наступним чином:

$$threshold = \frac{\overbrace{\min_{s \in S_A^{(d)}} \Psi(d,s)}^{h_d^-} + \overbrace{\min_{s \in S_N^{(d)}} \Psi(d,s)}^{h_d^+}}{2}. \tag{5}$$

Зазначена формула застосовується для обчислення порогу активації тільки тих детекторів *d*, які після навчання на множині аномальних даних $S_A^{(d)}$ не мають помилкових спрацьовувань на множині нормальних даних $S_A^{(d)}$, тобто $\forall s' \in S_N^{(d)} \Psi(d,s') < h_d^-$. Якщо така умова виконується, то з'являється додатковий проміжок, рівний величині $h_d = h_d^- - h_d^+ > 0$, і тим самим виникає можливість „зрушити" граничне значення h_d^-, що забезпечує реагування детектора *d* на будь-який „чужий" об'єкт $s \in S_A^{(d)}$ на величину $\frac{h_d^- - h_d^+}{2}$ в сторону h_d^+ $threshold = h_d^- - \frac{h_d^- - h_d^+}{2} = \frac{h_d^- - h_d^+}{2}$.

Виявлення деструктивного впливу на мережу ІТС СП $s \in S$ за допомогою розглянутої моделі здійснюється наступним чином:

1. Визначення корегувального коефіцієнту навантаження трафіку в мережі ІТС СП.

2. Обчислення для кожного імунного детектора $d \in D$ значення його активації $a_d = \Psi(d,s) - threshold$. Вважається,

що якщо $a_d \geq 0$, то детектор d є активованим, інакше відповідний детектор не реагує на вхідний об'єкт .

3. Мажоритарне голосування всередині кожного класу детекторів $D_{\varsigma(C)}$ $\underbrace{\sum_{d \in D_{\varsigma(C)}} [a_d \geq 0]}_{A_C} > \underbrace{\sum_{d \in D_{\varsigma(C)}} [a_d < 0]}_{B_C = \# D_{\varsigma(C)} - A_C}$, то s розпізнається як „чужий" пакет даних. Якщо $A_C < B_C$, то s розпізнається як „свій" пакет даних. В разі наявності конфліктів, тобто $A_C = B_C$, s класифікується як „чужий" пакет даних, якщо $a_{d_m^{(C)}} \geq 0$, та s класифікується як „свій" пакет даних, якщо $a_{d_m^{(C)}} < 0$, де $d_m^{(C)} \in D_M \bigcap D_{\varsigma(C)}$, $d_m^{(C)}$ – детектор пам'яті, навчений для розпізнавання „свого" пакету даних та „чужого" пакету даних з класу C.

4. Формування множини класів імунних детекторів, що активувалися $\left\{D_{\varsigma(C')}\right\}_{C' \in c}$ які розпізнають вхідний пакет даних s як „чужий" пакет даних, де $C^* = \left\{C' \middle| C' \in c \wedge \left(A_{C'} > B_{C'} \vee \left(A_{C'} = B_{C'} \wedge a_{d_m^{(C')}} \geq 0\right)\right)\right\} \subset c$.

5. Визначення класу пакета даних s. Якщо $C^* = \varnothing$, то пакет даних s належить до класу „своїх" пакетів даних. Якщо $E_{c^*} \rightleftharpoons \underset{C' \in c^*}{max} A_{C'}$ досягається в одній єдиній точці, то клас пакета даних $\arg E_{C'}$, інакше клас пакета даних s - це $\arg \max_{C' \in \{\arg E_{c^*}\}} \sum_{d \in D_\varsigma(C')} \times [a_d \geq 0]$.

Даний алгоритм заснований на порівнянні величини афінності імунних детекторів з їх індивідуально

налаштованими порогами активації та врахуванні однакових голосів, отриманих від більшої частини детекторів. У разі виникнення конфліктів при розрізненні між нормальним та аномальним класом (крок 3) вирішальний голос віддається детектору пам'яті. Якщо ж після цього зберігається конфлікт лише на рівні групи детекторів, то береться до уваги сума величин афінності, що саме активувалися у відповідь на даний стимул (вхідний пакет даних) імунних детекторів (крок 5).

Вхідний пакет даних є „своїм" тоді й лише тоді, коли $\forall C \in c \;\; A_C < B_C \vee \left(A_C = B_C \wedge a_{d_m^{(C)}} < 0 \right)$.

Як основу для даної моделі використовувалися модель з життєвим циклом (M_1), запропонована в [12], і модель з бібліотекою генів (M_2) [13], запропонована в [14], модель AISEA (M_3) [15] та розроблена модель (M_4), що була доповнена низкою удосконалень, а саме: врахуванням невизначеності стану мережі ІТС СП; удосконаленим алгоритмом навчання імунних детекторів; механізмом автоматичного підбору їх порогу активації, а також процедурою вирішення конфліктних випадків класифікації одного пакета даних за допомогою імунних детекторів пам'яті.

Порівняння цих чотирьох моделей наведено в таблиці 1. Знаком "+" відмічені характеристики, які притаманні відповідній моделі, знак "–" означає відсутність підтримки цієї особливості моделі.

Таблиця 1

Порівняння імунних моделей для виявлення деструктивного впливу на систему інформаційного захисту ІТС СП

Імунна модель	Незалежність від внутрішньої структури імунного детектору	Наявність клональної селекції та генетичної оптимізації	Наявність негативного відбору	Врахування типу невизначеності РЕО	Автоматичний підбір порога активації імунного детектора	Наявність механізмів навчання	Наявність детекторів пам'яті	Наявність життєвого циклу лімфоцитів	Динамічне перенавчання	Навчання детекторів на нових даних в процесі функціонування	Розподіл імунних детекторів	Підтримка мультикласового виявлення деструктивного впливу на ІТС СП	Автономність імунної системи (робота без втручання оператора)	Наявність сукупності процедур обробки різнорідних даних
M_1	–	–	+	–	–	–	+	+	+	+	–	–	–	–
M_2	–	+	+	–	–	–	+	–	+	+	+	–	–	–
M_3	+	+	+	–	+	+	+	+	+	+	–	–	+	–
M_4	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Результати порівняльного аналізу, що наведені в таблиці 1 дозволяють зробити висновок про перевагу зазначеної моделі у порівнянні з відомими. Зазначений підхід запропоновано використовувати в ході урегулювання воєнних конфліктів. Розроблена модель M_4 є універсальною по відношенню до внутрішнього представлення імунних детекторів, у той час як модель M_1 орієнтована на використання бітових рядків як імунні детектори, а модель

M_2 – на кластерну дискретизацію полів (генів) імунних детекторів. У моделі M_1 відсутня можливість клональної селекції детекторів, а також не передбачені оператори генетичної мутації. У всіх із представлених моделей у контексті виявлення деструктивного впливу на ІТС СП використовується динамічно оновлювана популяція імунних детекторів, що дозволяє штучній імунній системі адаптуватися до радіоелектронної обстановки, що змінюються, в режимі її функціонування. Однак тут для моделі M_1 вводиться додаткове обмеження: після активації детектора в результаті накопичення достатньої кількості збігів з антигенами повинен бути згенерований зовнішній по відношенню до системи сигнал зі сторони адміністратора (сигнал костимуляції). Такий сигнал дозволить активованому детектору отримати шанс для вступу в пул детекторів пам'яті та можливого подальшого безперервного аналізу радіоелектронної обстановки. Для моделі M_2 характерний розподілений механізм генерації детекторів: детектори, вигідні з точки зору розпізнавання аномалій, можуть бути розмножені інші мережеві вузли підвищення загальної продуктивності системи; ця властивість відсутня у моделей M_1 та M_3.

Проте в розробленій моделі M_4 додатково: враховуються тип невизначеності про наявні можливості радіоелектронної боротьби, засоби кібернетичного впливу на ІТС СП; використовується удосконалена сукупність процедур обробки різнотипних даних та забезпечення маршрутизації; використовується удосконалена процедура навчання; використовується механізм розв'язання конфліктних випадків класифікації; процедурою автоматичного обчислення порога активації імунних детекторів, а також універсальністю

структури їхнього представлення; постійним оновлення імунних детекторів протягом різних етапів дозрівання (життєвого циклу) та їх перенавчання з використанням набору деструктивного впливу на ІТС СП, що розширюється.

Обмеженнями зазначеного дослідження слід вважати: врахування часових обмежень на обмін конкретного типу повідомлення (формалізованого донесення); наявність первинної бази класифікаційних ознак мережевих ознак; необхідність повної та достовірної інформації щодо кількості абонентів мережі ІТС СП та технічних характеристик складових системи; обмеження щодо пропускної здатності та якості каналів передачі даних.

Висновки. У цьому дослідженні проведено розробка математичної моделі управління радіоресурсом систем радіозв'язку спеціального призначення на основі еволюційного підходу.

Результати дослідження стануть у нагоді при: розробці нових алгоритмів ідентифікації мережевих атак; обґрунтуванні рекомендацій щодо підвищення ефективності оперативного реагування системи інформаційного захисту від мережевих атак; аналізі ступеню захищеності мереж ІТС СП в ході ведення бойових дій (операцій); при створенні перспективних технологій підвищення ефективності системи захисту інформації у мережах ІТС СП; оцінці адекватності, достовірності, чутливості науково-методичного апарату системи захисту інформації у мережах ІТС СП; розробці нових та удосконаленні існуючих моделей системи захисту ІТС СП.

Напрямки подальших досліджень будуть спрямовані на розробку методології інтелектуального попередження загроз здійснення мережевих атак для нових вітчизняних інформаційно-телекомунікаційної (автоматизованої) системи спеціального призначення.

Список використаних джерел:

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч.закл. / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

2. Тимчук С. Методика комплексної обробки інформації від технічних засобів моніторингу. Traektoriâ Nauki. Path of Science. 2017. Vol. 3. No 3. pp. 4.1–4.9. DOI: 10.22178/pos.20-4.

3. Romanenko, I. O., Shyshatskyi, A.V., Zhyvotovskyi, R. M., Petruk, S.M. The concept of the organization of interaction of elements of military radio communication systems // Science and Technology of the Air Force of the Armed Forces of Ukraine. 2017. No 1. pp. 97-100.

4. Шевченко Д. Г. Сукупність показників ефективності функціонування системи кібербезпеки в інформаційно-телекомунікаційних мережах Збройних Сил України. // Сучасні інформаційні технології у сфері безпеки та оборони. Том 38, № 2 2020. С. 57–62. DOI: https://doi.org/10.33099/2311-7249/2020-38-2-57-62.

5. Макаренко С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности. 2017. № 2. С. 18-68. URL: http://sccs.intelgr.com/archive/2017-02/02-Makarenko.pdf.

6. V. Dudnyk, Yu. Sinenko, M. Matsyk, Ye. Demchenko, R. Zhyvotovskyi, Iu. Repilo, O. Zabolotnyi, A. Simonenko, P. Pozdniakov, A. Shyshatskyi. Development of a method for training artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies. Vol. 3. No. 2 (105). 2020. pp. 37–47. DOI: https://doi.org/10.15587/1729-4061.2020.203301.

7. Brownlee, J. Clever algorithms: nature-inspired programming recipes / J. Brownlee. 2011. 441 pp.

8. Гороховатський В., Стяглик Н., Царевська В. Комбінаційний метод прискореного метричного пошуку даних у задачах класифікації зображень. // Сучасні інформаційні системи. 2021. Том 5, № 3, с. 5–12. https://doi.org/10.20998/2522-9052.2021.3.01.

9. Meleshko, Y., Drieiev, O., Drieieva, H. Метод ідентифікації профілів ботів на основі нейронних мереж у рекомендаційних системах. Сучасні інформаційні системи, Том 4, № 2, с. 24–28. https://doi.org/10.20998/2522-9052.2020.2.05.

10. Dasgupta, D. Immunological computation: theory and applications / D. Dasgupta, F. Nino. CRC press, 2008. 277 pp.

11. Celada, F. A computer model of cellular interactions in the immune system / F. Celada, P. E. Seiden // Immunology today. 1992. Vol. 13, No. 2. pp. 56–62.

12. Chan-Tin, E. The frog-boiling attack: Limitations of secure network coordinate systems / E. Chan-Tin, V. Heorhiadi, N. Hopper, Y. Kim // ACM Transactions on Information and System Security (TISSEC). 2011. Vol. 14, no. 3.

13. Hofmeyr, S. A. Architecture for an artificial immune system / S. A. Hofmeyr, S. Forrest // Journal of Evolutionary computation. 2000. Vol. 8, No. 4. pp. 443–473.

14. Kim, S. S. Statistical techniques for detecting traffic anomalies through packet header data / S. S. Kim, A. Reddy // IEEE/ACM Transactions on Networking (TON). 2008. Vol. 16, No. 3. pp. 562–575.

15. Barford, P. A signal analysis of network traffic anomalies / P. Barford, J. Kline, D. Plonka, A. Ron // In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement. pp. 71–82.

Матеріали XXIII-ої Міжнародної науково-практичної конференції (07 серпня 2022 року, м. Дікірх (Люксембург),дистанційно)

СУЧАСНІ АСПЕКТИ МОДЕРНІЗАЦІЇ НАУКИ: СТАН, ПРОБЛЕМИ, ТЕНДЕНЦІЇ РОЗВИТКУ

Підписано до друку 04 серпня 2022 р.
Формат 60х90/8. Папір офсетний.
Друк офсетний. Гарнітура Times New Roman.
Ум. друк. арк. 8,2. Наклад 100 прим.

Видавець: Громадська наукова організація «Всеукраїнська асамблея докторів наук з державного управління» Свідоцтво серія ДК No4957 від 18.08.2015 р., Андріївський узвіз, буд.11, оф 68, м. Київ, 04070.

Надруковано рекламним агентством
«GoToPrint» Адреса, Україна,
Київська обл., м. Київ, вул. Льва Толстого, 63
e-mail: gotoprint@gmail.com