УДК 004.056
DOI: 10.15587/1729-4061.2016.73315

РОЗРОБКА МОДЕЛІ ДЛЯ НАВЧАННЯ АДАПТИВНОЇ СИСТЕМИ РОЗПІЗНАВАННЯ КІБЕРАТАК ДЛЯ НЕОДНОРІДНИХ ПОТОКІВ ЗАПИТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

В. А. Лахно
Доктор технічних наук, доцент
Кафедра організації комплексного захисту інформації*
E-mail: lva964@gmail.com
Г. А. Могильний
Кандидат технічних наук, доцент**
E-mail: g.mogilniy@gmail.com
В. Ю. Донченко
Ассистент**
E-mail: donchenko79@mail.ru
О. О. Смагіна
Кандидат педагогічних наук, старший викладач**
E-mail: smagina1804@gmail.com
М. В. Пирог
Викладач
Кафедра інформаційних систем та математичних дисциплін*
E-mail: mykola.pyroh@bigmir.net
*Європейський університет
бул. Академіка Вернадського, 16В, м. Київ, Україна, 03115
**Кафедра інформаційних технологій та систем
Луганський національний університет ім. Тараса Шевченка
пл. Гоголя, 1, м. Старобільськ, Україна, 92703

Запропоновано математичну модель для модуля системи інтелектуального розпізнавання кібератак для неоднорідних потоків запитів та мережних класах кібератак. Модель враховує неоднорідні вхідні потоки запитів та можливість зміни нападниками інтенсивності запитів у інформаційних системах, що дозволяє здійснювати вибір способів протидії та нейтралізації наслідків від їх впливу, аналізувати більш складні види кібератак. За допомогою імітаційних моделей, створених у MatLAB та Simulink, досліджено динаміку зміни станів підсистеми блокування запитів в процесі розпізнавання кібератак у критично важливих комп'ютерних системах

Ключові слова: розпізнавання кібератак, інтелектуальні системи, шаблон кібератаки, неоднорідні потоки запитів

Предложена математическая модель для модуля системы интеллектуального распознавания кибератак для неоднородных потоков запросов и сетевых классах кибератак. Модель учитывает неоднородные входные потоки запросов и возможность изменения нападающими интенсивности запросов в информационных системах, позволяет осуществлять выбор способов противодействия и нейтрализации последствий их реализации, анализировать более сложные виды кибератак. С помощью имитационных моделей, созданных в MatLAB и Simulink, исследована динамика изменения состояний подсистемы блокировки запросов в процессе распознавания кибератак в критически важных компьютерных системах

Ключевые слова: распознавания кибератак, интеллектуальные системы, шаблон кибератаки, неоднородные потоки запросов

1. Вступ

Активне розширення інформаційно-комунікаційного середовища (ІКС) та критично-важливих інформаційних систем (КВІС) у багатьох державах світу супроводжується виникненням нових загроз для кібербезпеки (КБ), про що свідчить зростання кількості інцидентів, пов'язаних із захистом інформації, а також виявлених уразливостей у КВІС.

Глобальний розвиток корпоративних інформаційних систем (КІС) та КВІС, зокрема у таких сегментах як e-business (СЕВ) в промисловості, зв'язку на транспорті та ін., вимагає постійного відстеження кіберзагроз, а також уразливостей технічних компонентів, програмного забезпечення (ПЗ), систем управління базами даних та ін. Одним з пріоритетних напрямків кіберзахисту, що сприяє своєчасному виявленню атак і запобіганню їх наслідків для КІС та КВІС, є шлях розвитку систем інтелектуального розпізнавання кібератак (СІРКА). Для подібних систем актуальним залишається питання застосування моделей та алгоритмів розпізнавання кібератак, які дозволяють враховувати не тільки наявність і розмір черг запитів у КІС чи КВІС, але й можливість використання додат-

кової інформації про структуру вхідних потоків або зміну нападниками інтенсивності запитів, швидкості атаки, тривалості імпульсу та ін. Тобто актуальність досліджень у напрямку створення СІРКА, що мають здатність до адаптації під час навчання, поповнення репозиторію шаблонів кібератак та експлуатації, не викликає сумніву.

2. Аналіз літературних даних і постановка проблеми

Питанням про удосконалення моделей розпізнавання складних кібератак системами кіберзахисту у КІС та КВІС присвячено багато досліджень. У роботах [1, 2] запропоновані моделі для систем виявлення кібератак (СВКА), що враховують наявність і розмір черг запитів у КІС [3], але автори не враховують можливість зміни швидкості надходження запитів до серверу.

Є дослідження, присвячені моделям та алгоритмам розпізнавання кібератак, які враховують запити у модулях систем «клієнт-банк», електронних накладних, систем зв'язку [4, 5], швидкість надходження вимог [6, 7], інтервал між вимогами [8, 9], тип вимог [10–12] та ін. Але в цих роботах не розглядались варіанти використання інформаційних систем із змінною структурою, у тому числі оснащених декількома серверами та компонентами кіберзахисту, які здатні враховувати складну поведінку черги запитів в умовах їх неоднорідності (конфліктності). Тобто більшість робот, присвячена проблематиці інтелектуального розпізнавання кібератак, направлених проти КІС або КВІС, стосується лише базових ознак кібернападів. Але в цих публікаціях не враховується зміна режимів роботи КІС або КВІС у разі втрати запитів внаслідок блокування неоднорідних потоків відповідними системами захисту, які виникають при складних кібервторгненнях, наприклад цільових атаках, або коли втрати запитів з'являються через переповнення черг на серверах КІС або КВІС.

Велика кількість публікацій присвячена й проблематиці проектування СРКА. Моделі виявлення кібератак на основі кінцевих автоматів (КА) досить докладно викладені в роботах [13, 14]. Методам обчислювального інтелекту у СРКА присвячено роботи [15–17]. Подібні системи все ще знаходяться у стадії розробки. В роботах [18, 19] запропоновано моделі байєсівської мережі для СРКА. Проте аналіз цих робіт вказує на те, що в більшості випадків для подібних СРКА підґрунтям для прийняття рішень є статистичний аналіз ознак аномалій, загроз та кібератак, та не враховується можливість реалізації складних цільових кібернападів. Широкому застосуванню подібних СРКА заважає й значна складність оперативного налаштування репозиторію шаблонів об'єктів розпізнавання.

Велика кількість робіт присвячена моделям та методам розпізнавання, заснованим на використовуванні ланцюгів Маркова [20–23]. Типовим недоліком більшості СРКА, запропонованих у цих роботах, є відсутність можливості оперативно поповнювати репозиторій шаблонів атак, оскільки в них майже завжди використовується лише одна методологія розпізнавання.

У розглянутих роботах, що представляють інтерес при вирішенні завдань розпізнавання кібератак, використовуються моделі, які базуються лише на інформації про вхідні потоки запитів й потоки насичення [6, 8, 15, 16, 20]. Сучасні кібератаки стали надзвичайно складними. Вузько направлені, систематичні і розподілені атаки, відомі як постійні складні загрози, здатні ховатися від антивірусів, не виявляються міжмережевими екранами та системами виявлення вторгнень [9, 17, 22]. Ці цільові загрози не мають сигнатур або добре маскуються [4, 23].

Таким чином, необхідні подальші дослідження, спрямовані на розвиток методологічних і теоретичних основ створення систем інтелектуального розпізнавання кібератак, які передбачають використовування додаткової інформації про структуру вхідних потоків, можливу зміну нападниками інтенсивності запитів, швидкості, тривалості імпульсу та ін. параметрів кібератаки.

3. Мета і завдання дослідження

Мета дослідження – розробка моделі для навчання створюваної адаптивної системи інтелектуального розпізнавання кібератак, яка дозволяє враховувати та зберігати у репозиторії шаблони складних кібератак із змінюваною інтенсивністю вхідних потоків запитів у КІС або КВІС.

Для досягнення мети роботи необхідно вирішити наступні завдання:

– розробити модель інтелектуального розпізнавання складних цільових кібератак із змінними параметрами потоків запитів у КІС або КВІС;

– провести імітаційні дослідження кібератак для неоднорідних потоків запитів в інформаційних системах.

4. Модель модуля системи інтелектуального розпізнавання кібератак для неоднорідних потоків запитів в інформаційних системах

Математичний опис модуля СІРКА для неоднорідних потоків запитів представлено наступним чином:

$$\Delta = \left\langle IS \times T \times SS \times \Omega S \times KB, MX^{|2|}, MB^{|2|}, o_1, o_2 \right\rangle, \quad (1)$$

де IS – множина вхідних сигналів, які визначають стан кібербезпеки КІС або КВІС; T – множина моментів часу, для яких здійснюється знімання даних про стан інформаційної безпеки (ІБ) об'єкту захисту; SS – простір ознак для розпізнавання певного класу кібератак; ΩS – простір функціональних станів ІБ; KB – база знань для ідентифікації кібератаки; $MX^{|2|}$ – навчальна матриця (еталон) які зберігаються у репозиторії СІРКА; $MB^{|2|}$ – бінарна навчальна матриця; o_1, o_2– оператори які формують вхідну та бінарну навчальні матриці СІРКА, відповідно.

Схема СІРКА наведена на рис. 1. Оператор $O\Theta$: $MB^{|2|} \rightarrow MR^{|2|}$ використовується для розбиття простору ознак кібератак на два класи розпізнавання. Параметр класифікації PF використовується для перевірки статистичної гіпотези про приналежність об'єкту розпізнавання до модельованого класу кібератак. Після оцінки статистичних гіпотез за допомогою оператору $O\gamma$, формується множина AR^g, яка характеризує точність

розпізнавання кібератаки у СІРКА. Прийнято q – кількість статистичних гіпотез, $g=q^2$ – кількість характеристик СІРКА. Оператор $o\mu$ формує множину ЕК, яка дозволяє виконувати процедуру оцінювання ефективності розпізнавання атаки в межах класу. Оператор $o\beta$ використовується для оптимізації системи контрольних відхилень від шаблонів атак. Множина SW, замикається послідовно оператором $o\alpha_1 : EK \to SW$ та оператором $o\alpha_2 : SW \to MX$, які дозволяють змінювати реалізації ознак кібератак різних класів в процесі навчання СІРКА.

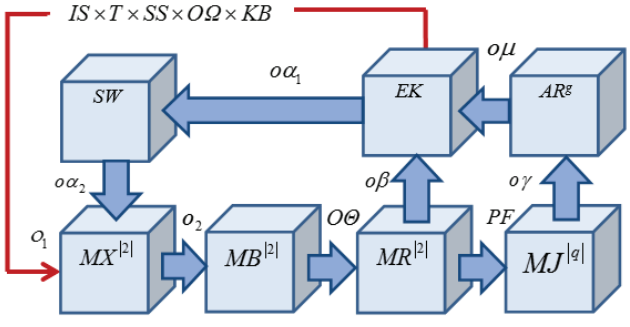


Рис. 1. Принципова схема СІРКА

Запропоновано модель для бази знань ідентифікації кібератак СІРКА (або репозиторію), коли у нападників є можливість створення неоднорідних потоків запитів із змінюваними під час атаки параметрами.

Потоки запитів вважаємо неоднорідними, якщо виконуються наступні умови:

1) відсутня можливість підсумовувати вхідні потоки запитів й зводити завдання розпізнавання у СІРКА підозрілих запитів до одномірного випадку;

2) обслуговування заявок неоднорідних потоків здійснюється в інтервали часу, що не перетинаються;

3) в системі є так звані «інтервали неприступності», протягом яких потоки не обслуговуються, наприклад у випадку аналізу запитів системою виявлення вторгнень у КВІС.

В системі розпізнавання апріорі виділяються найінтенсивніші вхідні потоки запитів (потоки найважливіші в сенсі оперативності обслуговування й потоки малої інтенсивності). Функціональна схема організації подібних кібератак виглядає так, як приведено на рис. 2.

Припустимо, що вхідні потоки запитів k_1, k_2, k_3 формують в деякому випадковому середовищі (ВС). Стан ВС може визначати імовірнісну структуру потоків запитів. Розглянемо наступні варіанти:

1) якщо ВС перебуває в стані $c^{(0)}$, то вхідні потоки вимог – це звичайні потоки запитів, тобто штатний режим роботи КІС або КВІС;

2) якщо ВС переходить у стан $c^{(1)}$, вхідні потоки є потоками пачок (потік запитів являє собою послідовність «пачок» [21, 23, 24] або BMAP – потік).

Прийнято, що: k_1 – пріоритетний потік запитів, які надходять з малою інтенсивністю; k_2 – потік запитів з нормальним пріоритетом та малою інтенсивністю; k_3 – пріоритетний потік запитів, які надходять з найбільшою інтенсивністю.

Інформативність потоку k_1 означає, що в динаміці роботи системи враховують наявність заявок у накопичувачі NO_1 та надходження вимог по цьому потоку. Пріоритетність відповідного потоку – необхідність оперативного обслуговування вимог, що надійшли у КІС або КВІС. Наприклад, для потоку k_3 його пріоритетність означає, що у випадку розриву, тобто за відсутності вимог по потоку k_1, продовжується обслуговування потоку запитів k_3.

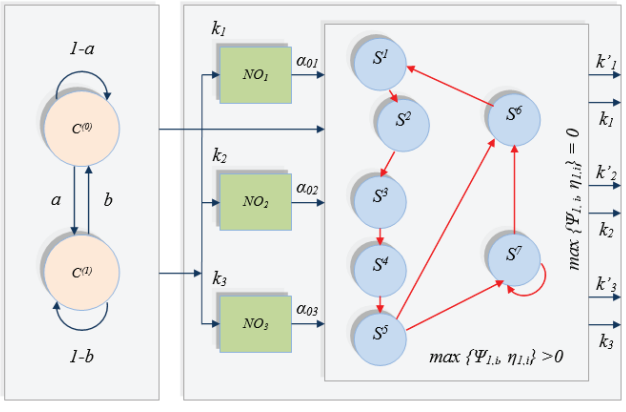


Рис. 2. Функціональна схема організації кібератак із неоднорідними потоками запитів: S^1 – вхід у КІС або КВІС; S^2 – сканування доступних ресурсів (ДР) у КІС або КВІС; S^3 – очікування відповіді про наявність ДР; S^4 – підключення до ДР; S^5 – передавання даних у КІС або КВІС; S^6 – передавання даних на доступні ресурси (автоматизовані робочі місця (АРМ), персональні комп'ютери (ПК) та ін.); S^7 – завантаження відправлення запитів на сервери КІС або КВІС

Відповідно до топології КІС або КВІС та прийнятих припущень щодо стану ВС, організовано роботу обслуговуючого обладнання (ОО), наприклад серверів КВІС та елементів СІРКА. Стани системи, у відповідності до графу, позначимо $S^{(r)}, r=\overline{1,7}$. Стани системи утворюють множину $S=\left\{S^{(r)} : r=\overline{1,7}\right\}$. Система в стані $S^{(r)}$ перебуває в продовж часу $\tau_r, r=\overline{1,7}$. ОО виконує завдання з аналізу й обслуговування вимог, а також керує вхідними потоками, формує черги у NO_i та ін. Відбір запитів із черг, відповідно до пріоритету, здійснюється за допомогою стратегій обслуговування, позначених як α_{O1}, α_{O2}, α_{O3}. Стан $S^{(2j-1)}$ для j=1, 2, 3 ОО відповідає обслуговуванню вимог потоку k_j. У стані $S^{(2j)}$ для j=1, 2, 3 вимоги жодного з вхідних потоків не обслуговують. У стані $S^{(7)}$ обслуговують вимоги потоку k_3. Згідно із графом, при кожному r=1, 2, 3, 4 стан $S^{(r)}$ переходить у стан $S^{(r+1)}$.

Розглянемо ситуацію, коли зловмисники, що атакують систему, можуть створювати черги. Відповідно, вихідні потоки при роботі системи з максимальним завантаженням та функціонуванням ОО без простоїв, трансформуються у потоки насичення, позначені як k_1', k_2', k_3', на відміну від реальних потоків запитів у системі – k_1, k_2, k_3.

Розглянуто такі варіанти інтелектуального розпізнавання загроз кібератак:

1) з посилкою пакетів з нульовою частотою щодо часової шкали часу проходження запитів до адресата й назад;

2) кібератак, у яких зловмисник може варіювати тривалість імпульсів;

3) з мінімальними випадковими значеннями щодо часової шкали часу проходження запитів до адресата й назад та інші.

Усі випадкові об'єкти, які аналізуються далі та використовуються для побудови моделі кібератаки, а також пов'язані із процесом обслуговування запитів, розглянуті на ймовірнісному просторі $(\Omega, A, P(*))$ елементарних випадкових подій $\omega \in \Omega$ з ймовірністю потрапляння запиту у систему – P(A). Опис вхідних потоків запитів здійснено за допомогою нелокального способу. Будь який потік запитів k_j у системі описується випадковою послідовністю у вигляді вектору $\{(\tau_i, v_i, \eta_{j,i}); i \geq 0\}$, де $\eta_{j,i}$ – кількість заявок зразку ν_i, які, відповідно, надходили за проміжок часу $[\tau_i, \tau_{i+1})$ цим потоком. Зразок заявок визначається у СІРКА, наприклад за допомогою маркеру ν_i у вигляді бінарної матриці ознак [25, 26], яка зберігається у репозиторії, а також станом ВС. Для спрощення моделі, поведінка випадкового середовища описується однорідною Марковською послідовністю $\{\nu_i; i \geq 0\}$ із двома станами $c^{(0)}$ – потік запитів з малою інтенсивністю, $c^{(1)}$ – великий потік заявок та ймовірностями переходу a, b $0 \leq a < b << 1$. Відповідно до прийнятих обмежень, зміна інтенсивності потоку відбувається не часто, отже, звичайний режим роботи КВІС із малоінтенсивним потоком заявок буває частіше, ніж потік з великою кількістю запитів. Таким чином, на підґрунті зроблених висновків вважаємо, що за час τ_r, коли ОО перебуває в стані $S^{(r)}$, інтенсивність запитів не буде змінюватися. Випадкові елементи $\nu_i; i \geq 0$ пов'язані співвідношеннями: $\nu_{i+1} = \varphi_i(\nu_i, \omega_i)$, де φ_i – опис простору $\{c^{(0)}, c^{(1)}\} \cdot \{0,1\}$ на $\{c^{(0)}, c^{(1)}\}$; $\{\omega_i; i \geq 0\}$ – послідовна множина незалежних випадкових величин з відомим розподілом. Для моделі розподіл прийнято рівномірним на інтервалі $(0,1)$.

Обслуговуюче обладнання у будь-який момент часу $\tau > 0$ перебуває в деякому стані $S(\tau) \in S$. Керування вхідними потоками запитів й перехід між станами ОО у відповідності до графу та з урахуванням вищевказаних попередніх зауважень, описано так:

$$S_{i+1} = u(S_i, \psi_{1,i}, \eta_{1,i}) = \begin{cases} S^{(1)} \text{ при} S_i = S^{(6)}; \\ S^{(r+1)} \text{при} S_i = S^{(r)}\ r = \overline{1,4}; \\ S^{(6)} \text{ при} S_i \in \{S^{(5)}, S^{(7)}\} \& \max\{\psi_{1,i}, \eta_{1,i}\} > 0; \\ S^{(7)} \text{ при} S_i \in \{S^{(5)}, S^{(7)}\} \& \max\{\psi_{1,i}, \eta_{1,i}\} = 0; \end{cases} \quad (2)$$

де $\psi_{j,i} = f(w)$ – довжина черги в NO_j по потоку k_j для i=0,1,...,k.

Враховуючи вирішальні правила $DR(p_{axi})$ [25], які визначають стани КВКС у випадку загроз ІБ, отримано рекурентні залежності для інтелектуального розпізнавання складних кібератак, коли зловмисник створює ситуацію, за якої $S_i \in \{S^{(5)}, S^{(7)}\}$ обслуговуються лише вимоги по потоку k_3, то при r=6, $y = 0,1,; x_{j,k} = \{0,1,\ldots k\}$ одержимо, що

$$Q_{i+1}\left(S^{(6)}, c^{(s)}, 0, w_3, DR(p_{axi})\right) = 0$$

при всіх $w_3 \geq 0$ та $i \geq 0$. При $w_1 \geq 1$ одержимо таку залежність:

$$Q_{i+1}\left(S^{(6)}, c^{(s)}, w_1, 0, DR(p_{axi})\right) =$$

$$= \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{x=0}^{w_1} \sum_{y=0}^{l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}(w_1 - x, T_5) \cdot \sum_{n_3=0}^{l_{3,h}-y} \varphi_{3,h}(n_3, T_5) + \\ + \sum_{x=0}^{w_1} \sum_{y=0}^{l'_{3,h}} Q_i\left(S^{(7)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}(w_1 - x, T_7) \cdot \sum_{n_3=0}^{l'_{3,h}-y} \varphi_{3,h}(n_3, T_7) \end{array} \right], \quad (3)$$

де p_{axi} – ознаки нелегітимної діяльності у сегменті мережі (кібератаки); $l_{1,s}, l_{3,s}, l'_{3,s}$ – цілі частини величин $\mu_{1,s}T_1$, $\mu_{3,s}T_5$, $\mu_{3,s}T_7$, $\mu_{j,s}$ – інтенсивність обслуговування по потоку k_j, якщо система перебуває в стані $c^{(s)}$ або $c^{(h)}$, а при будь-яких $w_3 \geq 1$:

$$Q_{i+1}\left(S^{(6)}, c^{(s)}, w_1, w_3, DR(p_{axi})\right) =$$

$$= \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{x=0}^{w_1} \sum_{y=0}^{w_3+l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}(w_1 - x, T_5) \times \\ \times \varphi_{1,h}(w_3 + l_{3,h} - y, T_5) + \\ + \sum_{x=0}^{w_1} \sum_{y=0}^{w_3+l'_3} Q_i\left(S^{(7)}, c^{(h)}, x, y\right) \cdot \varphi_{1,h}(w_1 - x, T_7) \times \\ \times \varphi_{1,h}(w_3 + l'_{3,h} - y, T_7) \end{array} \right]. \quad (4)$$

Для ймовірностей

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, w_1, w_3, DRv(p_{axi})\right)$$

одержимо

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, w_1, w_3, DR(p_{axi})\right) = 0$$

при будь-якому $w_1 \geq 0$, $i \geq 0$, $s \in \{1,0\}$:

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, 0, 0, DR(p_{axi})\right) =$$

$$= \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{y=0}^{l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}(0, T_5) \cdot \sum_{n_3=0}^{l_{3,h}-y} \varphi_{3,h}(n_3, T_5) + \\ + \sum_{y=0}^{l'_{3,h}} Q_i\left(S^{(7)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}(0, T_7) \cdot \sum_{n_3=0}^{l'_{3,h}-y} \varphi_{3,h}(n_3, T_7) \end{array} \right], \quad (5)$$

а при будь-яких $w_3 \geq 0$, $s \in \{1,0\}$:

$$Q_{i+1}\left(S^{(7)}, c^{(s)}, 0, w_3, DR(p_{axi})\right) =$$

$$= \sum_{h=0}^{1} P_{h,s} \left[\begin{array}{l} \sum_{y=0}^{w_3+l_{3,h}} Q_i\left(S^{(5)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}(0, T_5) \cdot \varphi_{3,h}(w_3 + l_{3,h} - y, T_5) + \\ + \sum_{y=0}^{w_3+l'_{3,h}} Q_i\left(S^{(7)}, c^{(h)}, 0, y\right) \cdot \varphi_{1,h}(0, T_7) \cdot \varphi_{3,h}(w_3 + l'_{3,h} - y, T_7) \end{array} \right]. \quad (6)$$

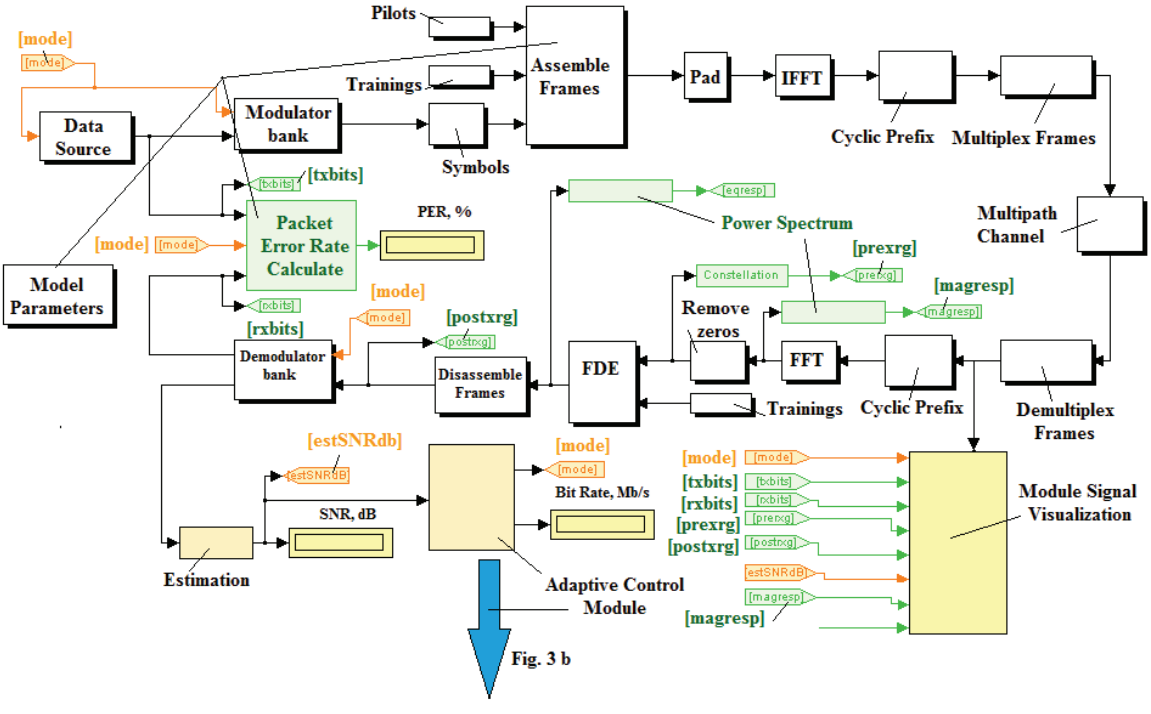
Враховуючи рекурентні вирази (2)–(6) та використовуючи інструментарій моделювання пакету MATLAB 7 та Simulink розроблена імітаційна модель для аналізу впливу кібератаки на функціональність сегменту КІС або КВІС, якщо нападник використовує неоднорідні потоки запитів у системі.

5. Імітаційна модель кібератак для неоднорідних потоків запитів в інформаційних системах

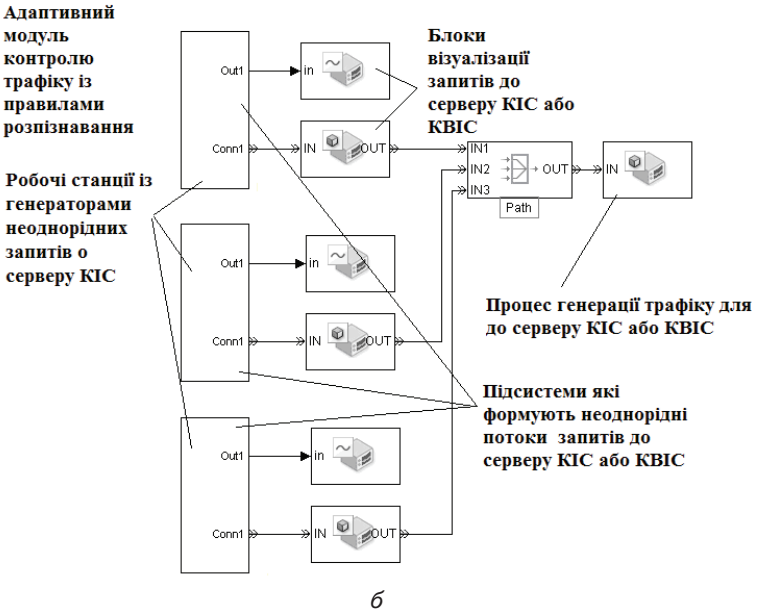
Імітаційна модель (сегмент КВІС) складається з однієї лінії передачі даних і трьох станцій (автоматизованих робочих місць – АРМ), які періодично надсилають

вимоги на передачу даних по лінії, рис. 3, *а*. Параметри запитів були сформовані відповідно до даних, рис. 3, *б*: АРМ1 – малоінтенсивний пріоритетний потік k_1; АРМ2 – малоінтенсивний потік k_2; АРМ3 – пріоритетний потік найбільшої інтенсивності k_3. Також припускалося, що час дискретний і змінюється від 0 до деякого значення T. АРМ працюють незалежно один від одного і в кожний момент часу з певною ймовірністю від будь-якої станції може надійти вимога на передачу даних по лінії або відбутися звільнення лінії. У блоці аналізу трафіку, використовуючи блок розпізнавання загроз [25] та закладені вирішальна правила DR(p_{axi}), можна блокувати відповідні атаки та несанкціоновану мережеву активність. Жовтим кольором на схемі показані компоненти, які використовували для візуалізації трафіку або окремих неоднорідних потоків запитів до серверу КІС. Зеленим кольором показані компоненти, які дозволяли змінювати параметри неоднорідних потоків запитів – наявність і розмір черг запитів у КІС чи КВІС, структуру вхідних потоків k_1, k_2, k_3, зміну атакуючими інтенсивності запитів, швидкості атаки, тривалості імпульсу та ін.

Для реалізації процесу інтелектуального розпізнавання по окремих класах загроз, кібератак та аномалій у імітаційній моделі КІС або ІКСТГ за допомогою пакету розширення Fuzzy Logic Toolbox були складені відповідні правила для системи розпізнавання, рис. 4.



а



б

Рис. 3. Схема імітаційного моделювання кібератаки для неоднорідних потоків запитів у сегменті КІС або КВІС:
а – сегмент КІС або КВІС (використовувалися бібліотечні компоненти MatLab);
б – блок для моделювання кібератаки для неоднорідних потоків запитів

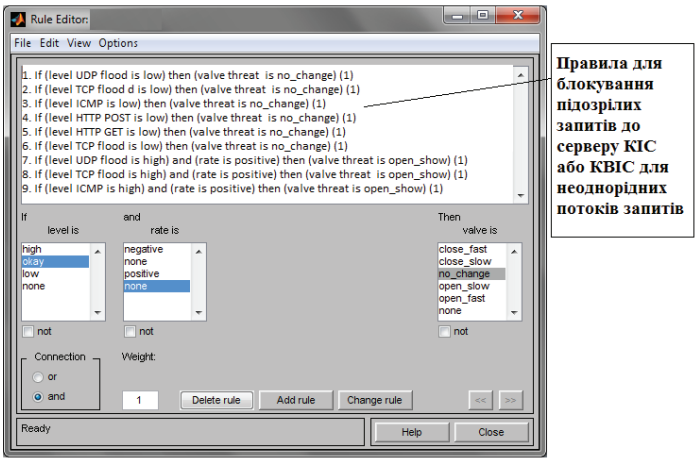


Рис. 4. Система правил для розпізнавання кібератак

На рис. 5 показана схема підсистеми блокування запитів від АРМ у складі КІС або КВІС при виявленні аномальної черги заявок, що надходять із терміналу.

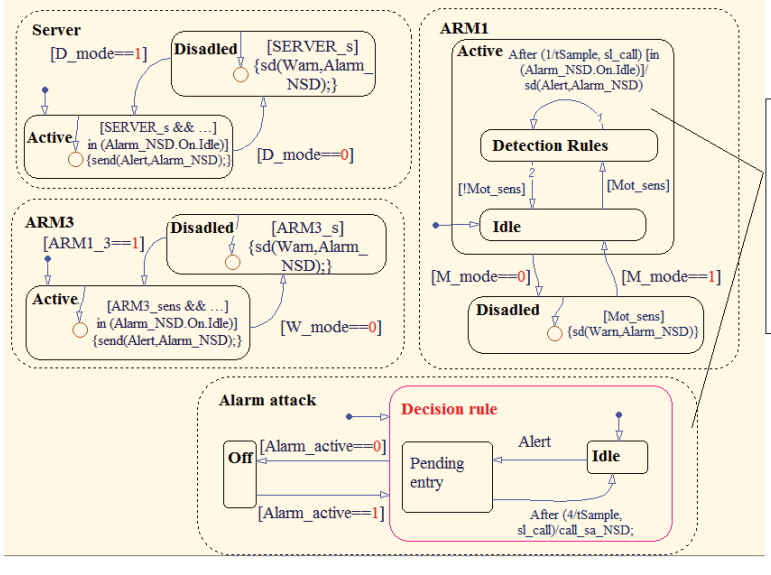


Рис. 5. Підсистема блокування запитів у системі інтелектуального розпізнавання кібератак у КВІС

Для дослідження можливості виявлення кібератак із неоднорідними потоками запитів був проведений імітаційний експеримент у сегменті комп'ютерної мережі КІС. При цьому мережа працювала у звичайному режимі й зазнала впливу атаки. Для візуалізації сигналів був спроектований спеціальний блок – «Signal Visualization», рис. 6, який дозволяє аналізувати основні параметри сегменту КВІС на рівні переданих пакетів даних, зокрема досліджувати зміну кількості запитів R за часовий інтервал – t.

В ході імітаційного моделювання досліджувалися режими роботи КІС або КВІС для випадків блокування запитів при їхньому відхиленні від «нормального» режиму. Відповідні результати імітаційного моделювання представлені у наступному розділі.

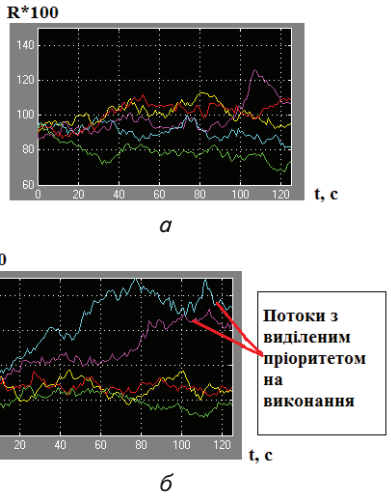


Рис. 6. Візуалізація потоків запитів у КВІС: *а* – звичайний режим роботи сегменту КВІС; *б* – створення атаки із неоднорідними потоками запитів

6. Результати імітаційного моделювання кібератак для неоднорідних потоків запитів в інформаційних системах

За допомогою імітаційної моделі (ІМ) проведено перевірку вірогідності результатів реалізації кібератак типу «відмова у обслуговуванні» та «переповнення буфера» у ІКС КІС. У якості вихідних даних використовувалися результати вимірювань параметрів отриманих реалізацій вхідних потоків у ІМ. Імітаційне моделювання та аналітичний розрахунок [3, 4, 21–23, 25, 26] пропускної здатності каналів, які використовуються у КІС або КВІС, проводився для різних наборів реалізацій неоднорідних потоків k_1 та k_3. В табл. 1 наведені отримані під час імітаційного експерименту показники – час затримки та ймовірність втрати заявки, а також порівняльні параметри очікуваних характеристик. Відповідно, $T_{ср.пр.}$ та $P_{пр.}$ – припустимі значення затримки та ймовірності втрат відповідно, $T_{ср.к.}$ та $P_{к.}$ – відповідні параметри мережі, розрахованої класичним методом, $T_{ср.з.}$ та $P_{з.}$ – відповідні параметри мережі, розрахованої за допомогою запропонованих моделей. На підставі аналізу та порівняння отриманих результатів, зроблено висновок про адекватність виконаних розрахунків характеристик елементів СІРКА у сегменті мережі КІС або КВІС.

У табл. 2 наведені результати імітаційного моделювання в умовах атаки типу «відмова у обслуговуванні» на сервер та АРМ у складі моделі КІС.

Середня помилка розрахованої оцінки ймовірності втрат заявок V_{zap} в результаті здійснення подібних кібератак не перевищує середньоквадратичне відхилення частоти втрат F_{zap} в серії експериментів.

Таблиця 1

Значення ймовірносно-часових характеристик при кібератаці «відмова у обслуговуванні»

Номер реалізації	$T_{ср.пр.}$, мс	$T_{ср.к.}$, мс	$T_{ср.з.}$, мс	$P_{пр.}$	$P_{к.}$	$P_{з.}$
1	10	11,7	10,2	5×10^{-8}	$6{,}28\times10^{-8}$	$4{,}93\times10^{-8}$
2	20	24,7	20,3	7×10^{-8}	$7{,}79\times10^{-8}$	$7{,}12\times10^{-8}$
3	50	61	49,5	3×10^{-6}	$3{,}6\times10^{-6}$	$3{,}15\times10^{-6}$
4	100	97,3	98,4	$1{,}5\times10^{-6}$	$2{,}36\times10^{-6}$	$3{,}07\times10^{-6}$
5	150	107,3	101,4	$1{,}7\times10^{-6}$	$2{,}56\times10^{-6}$	$2{,}98\times10^{-6}$
6	200	111,3	119,4	$1{,}8\times10^{-6}$	$2{,}7\times10^{-6}$	$2{,}81\times10^{-6}$
7	250	125,3	128,4	$1{,}95\times10^{-6}$	$2{,}8\times10^{-6}$	$2{,}47\times10^{-6}$
8	300	147,3	148,4	2×10^{-6}	$2{,}9\times10^{-6}$	$2{,}03\times10^{-6}$
9	350	180,3	155,4	$9{,}1\times10^{-5}$	$9{,}05\times10^{-5}$	$9{,}29\times10^{-5}$
10	400	247,3	190,4	$9{,}7\times10^{-5}$	$9{,}9\times10^{-5}$	$9{,}87\times10^{-5}$

Таблиця 2

Результати імітаційного моделювання сегменту КІС в умовах атаки «відмова у обслуговуванні»

Кількість сеансів моделювання	n	10
Середнє значення частоти втрат заявок	V_{zap}	8,6E–2
Середньоквадратичне відхилення частоти втрат	F_{zap}	1,01E–3
Розрахована оцінка ймовірності втрат заявок	P_{zap}	8,41E–2
Середня помилка	ΔP_{zap}	3,9E–4

На рис. 7, 8 показано основні результати моделювання неоднорідних потоків заявок k_1, k_2, k_3 у КВІС. Отже, при створенні пріоритетних неоднорідних потоків заявок у КВІС, час опрацювання даних збільшується у 1,5–3,5 рази.

Як показує аналіз отриманих результатів, при використанні нападниками тактики присвоювання під час кібератаки малоінтенсивному потоку запитів високого пріоритету й достатньому часі на проведення комп'ютерного вторгнення, можна значно збільшити ймовірність проникнення в систему. При цьому атакуючим, не обов'язково змінювати параметри потоку k_3, що має в системі найбільшу інтенсивність й високий пріоритет, рис. 8.

На рис. 9 представлений графік залежності теоретичної оцінки ймовірності втрати заявки в КІС або КВІС від кількості кроків запропонованої ітераційної процедури (2)–(6). Представлений графік дозволяє зробити висновок про необхідну кількість ітерацій для забезпечення заданої точності імітаційної моделі.

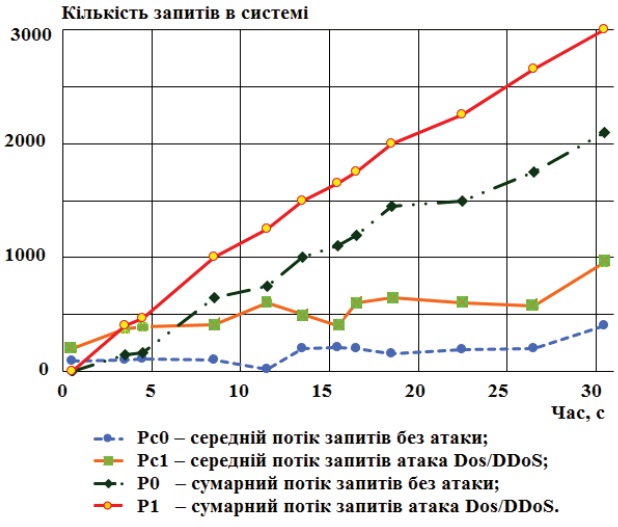


Рис. 7. Розподіл сумарного (P0, P1) й середнього (Pc0, Pc1) потоку запитів при звичайних режимах роботи сегменту КІС або КВІС

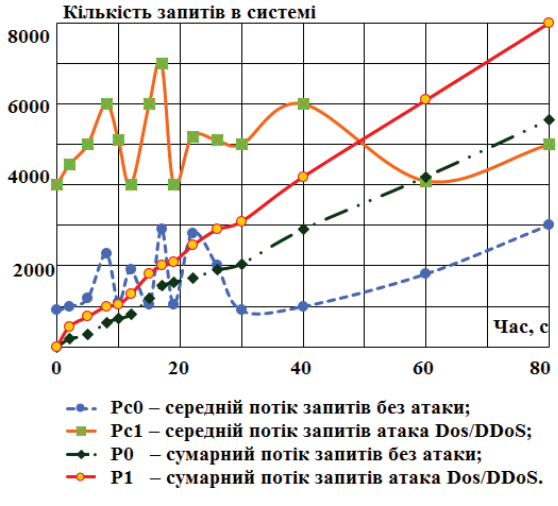


Рис. 8. Розподіл сумарного (P0, P1) й середнього (Pc0, Pc1) потоку при створенні нападниками неоднорідних запитів

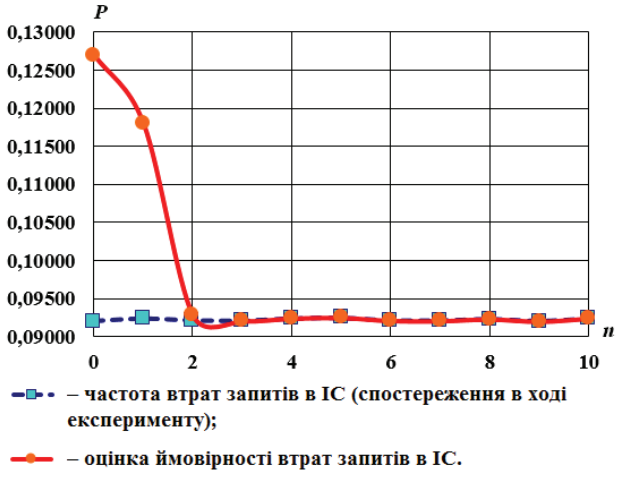


Рис. 9. Залежність теоретичної оцінки ймовірності (P) втрати запиту (заявки) від кількості кроків (n) ітераційних процедур

В ході досліджень встановлено, що ймовірність вирішення завдання розпізнавання кібератак для неоднорідних потоків запитів та мережних класах кібератак склала 85–98 %, залежно від типу атаки.

Аналіз результатів імітаційного експерименту дозволяє зробити висновок, що запропонована модель розпізнавання складних кібератак у випадку використовування нападниками неоднорідних потоків запитів має більшу точність, ніж існуючи моделі, приблизно на 5–7 %.

ом, для проведення успішної кібератаки на інформаційні ресурси КІС або КВІС, зокрема типу «відмова в обслуговуванні», не обов'язково створювати велику кількість запитів до сервера або знижувати смугу пропускання трафіку. Можна з досить високим ступенем ймовірності успіху експлуатувати уразливості, пов'язані зі створенням малоінтенсивного пріоритетного потоку, наприклад, варіюючи такими параметрами, як швидкість пакета (низькошвидкісні атаки); тривалість імпульсу та ін.

За попередніми розрахунками, розроблені імітаційні моделі дають змогу на 25–30 % зменшити час налагодження проектів СІРКА для КІС або КВІС.

7. Обговорення результатів тестування моделі та перспективи подальших досліджень

Таким чином, описані моделі реалізації кібератак із неоднорідними потоками запитів у КІС або КВІС не тільки становлять самостійний практичний інтерес, але і є прикладом можливої формалізації опису інших складних сценаріїв кібернападів.

Встановлено, що Марковські моделі процесів широко використовують при аналізі й синтезі СЗІ КВІС, причому властивість марковості є певним обмеженням на реальні сигнали які використовуються, але цілком достатнім для розроблення змістовних методів аналізу й синтезу комплексів кіберзахисту. Оскільки кожний стан системи може характеризуватися сукупністю значень квантованих цифрових сигналів, характерних для S_i, то, у термінах системи СІРКА, число градацій ознаки атаки – рівня квантування, виступає як універсальна множина, потужність якого дорівнює максимальному рівню квантування, характерному для даної моделі.

Недоліком моделі є певна громіздкість розрахунків, яка ускладнює практичне застосування апарату ланцюгів Маркова для моделювання розглянутих процесів. Однак в експонентному наближенні розрахунок ймовірності реалізації подібної кібератаки виявляється досить простим.

Наведений підхід дозволяє здійснювати кількісну оцінки можливостей реалізації мережевих загроз та атак у комп'ютерних мережах КІС або КВІС з урахуванням фактору часу й тим самим підвищити обґрунтованість проведених заходів із захисту інформації.

Науково-практичні результати досліджень у вигляді програмно-апаратних додатків і методичних матеріалів протягом 2014–2015 років були впроваджені на державному підприємстві «Проектно-конструкторське технологічне бюро з автоматизації систем управління на залізничному транспорті України» Міністерства інфраструктури України, а також в службі інформаційної безпеки обчислювального центру Придніпровської залізниці та Державному університеті телекомунікацій в рамках науково-дослідної роботи «Безпека-05П».

В даний час, з урахуванням результатів, раніше представлених у роботах [25, 26], та результатів тестових випробувань окремих модулів СІЗКА ведеться розробка системи підтримки прийняття рішень і експертної системи та наповнення репозиторію шаблонів кібератак.

8. Висновки

1. Розроблена модель інтелектуального розпізнавання складних кібератак, яка, на відміну від існуючих, враховує зміну інтенсивності вхідних потоків запитів в інформаційних системах, що дозволяє виконувати оцінку якості функціонування СЗІ, з урахуванням можливостей зміни нападаючими параметрів атаки.

2. Проведено тестування та апробація запропонованої моделі за допомогою імітаційного моделювання у пакеті MATLAB та Simulink. Встановлено, що запропонована модель розпізнавання складних кібератак у випадку використовування нападниками неоднорідних потоків запитів має більшу точність, ніж існуючи моделі, приблизно на 5–7 %. Розроблені імітаційні моделі дають змогу на 25–30 % зменшити час налагодження проектів систем кіберзахисту, зокрема, СІРКА для КІС або КВІС.

Литература

1. Yu, S. Can We Beat DDoS Attacks in Clouds? [Text] / S. Yu, Y. Tian, S. Guo, D. O. Wu // IEEE Transactions on Parallel and Distributed Systems. – 2014. – Vol. 25, Issue 9. – P. 2245–2254. doi: 10.1109/tpds.2013.181
2. Peng, T. Survey of Network-Based Defense Mechanisms Countering the dos and ddos Problems [Text] / T. Peng, C. Leckie, K. Ramamohanarao // ACM Computing Surveys. – 2007. – Vol. 39, Issue 1. – P. 1–3. doi: 10.1145/1216370.1216373
3. Bogdanoski, M. Analysis of the SYN Flood DoS Attack [Text] / M. Bogdanoski, T. Shuminoski, A. Risteski // International Journal of Computer Network and Information Security. – 2013. – Vol. 5, Issue 8. – P. 11–15. doi: 10.5815/ijcnis.2013.08.01
4. Logota, E. Analysis of the Impact of Denial of Service Attacks on Centralized Control in Smart Cities [Text] / E. Logota, G. Mantas, J. Rodriguez, H. Marques. – Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 2015. – P. 91–96. doi: 10.1007/978-3-319-18802-7_13
5. Zargar, S. T. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks [Text] / S. T. Zargar, J. Joshi, D. Tipper // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, Issue 4. – P. 2046–2069. doi: 10.1109/surv.2013.031413.00127

6. Ciancamerla, E. Modeling cyber attacks on a critical infrastructure scenario [Text] / E. Ciancamerla, M. Minichino, S. Palmieri // Information, Intelligence, Systems and Applications (IISA), Fourth International Conference, 2013. – P. 1–6. doi: 10.1109/iisa.2013.6623699
7. Rinaldi, S. M. Identify, understanding, and analyzing critical infrastructure interdependencies [Text] / S. M. Rinaldi, J. P. Peerenboom, T. K. Kelly // IEEE Control Systems Magazine. – 2001. – Vol. 21, Issue 6. – P. 11–25. doi: 10.1109/37.969131
8. Ahmed, I. Scada systems: Challenges for forensic investigators [Text] / I. Ahmed, S. Obermeier, M. Naedele, G. G. Richard III // Computer. – 2012. –Vol. 45, Issue 12. – P. 44–51. doi: 10.1109/mc.2012.325
9. Liu, R. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid [Text] / R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, A. K. Srivastava // IEEE Transactions on Smart Grid. – 2015. – Vol. 6, Issue 5. – P. 2444–2453. doi: 10.1109/tsg.2015.2432013
10. Chen, Q. A Model-Based Validated Autonomic Approach to Self-Protect Computing Systems [Text] / Q. Chen, S. Abdelwahed, A. Erradi // IEEE Internet of Things Journal. – 2014. – Vol. 1, Issue 5. – P. 446–460. doi: 10.1109/jiot.2014.2349899
11. Wasicek, A. Aspect-oriented modeling of attacks in automotive Cyber-Physical Systems [Text] / A. Wasicek, P. Derler, E. Lee // Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference - DAC '14, 2014. – P. 1–6. doi: 10.1145/2593069.2593095
12. Ericsson, G. N. Cyber security and power system communication-essential parts of a smart grid infrastructure [Text] / G. N. Ericsson // IEEE Transactions on Power Delivery. – 2010. – Vol. 25, Issue 3. – P. 1501–1507. doi: 10.1109/tpwrd.2010.2046654
13. Ilgun, K. State transition analysis: a rule-based intrusion detection approach [Text] / K. Ilgun, R. A. Kemmerer, P. A. Porras // IEEE Transactions on Software Engineering. – 1995. –Vol. 21, Issue 3. – P. 181–199. doi: 10.1109/32.372146
14. Khan, L. A new intrusion detection system using support vector machines and hierarchical clustering [Text] / L. Khan, M. Awad, B. Thuraisingham // The VLDB Journal. – 2007. – Vol. 16, Issue 4. – P. 507–521. doi: 10.1007/s00778-006-0002-5
15. Al-Jarrah, O. Network Intrusion Detection System using attack behavior classification [Text] / O. Al-Jarrah, A. Arafat // 2014 5th International Conference on Information and Communication Systems (ICICS), 2014. – P. 1–6. doi: 10.1109/iacs.2014.6841978
16. Selim, S. Intrusion Detection using Multi-Stage Neural Network [Text] / S. Selim, M. Hashem, T. M. Nazmy // International Journal of Computer Science and Information Security (IJCSIS). – 2010. – Vol. 8, Issue 4. – P. 14–20.
17. Pawar, S. N. Intrusion detection in computer network using genetic algorithm approach: a survey [Text] / S. N. Pawar // International Journal of Advances in Engineering Technology. – 2013. – Vol. 6, Issue 2. – P. 730–736.
18. Heckerman, D. A tutorial on learning with bayesian networks. Innovations in Bayesian Networks [Text] / D. Heckerman // Theory and Applications. – 2008. –Vol. 156. – P. 33–82. doi: 10.1007/978-3-540-85066-3_3
19. Nguyen, K. C. A decentralized Bayesian attack detection algorithm for network security [Text] / K. C. Nguyen, T. Alpcan, T. Basar // IFIP – The International Federation for Information Processing, 2008. –P. 413–428. doi: 10.1007/978-0-387-09699-5_27
20. Vrakopoulou, M. Chapter Cyber Physical Systems Approach to Smart Electric Power Grid [Text] / M. Vrakopoulou, P. Mohajerin Esfahani, K. Margellos, J. Lygeros, G. Andersson. – Power Systems, 2015. – P. 303–328. doi: 10.1007/978-3-662-45928-7_11
21. Lecchini-Visintini, A. Stochastic optimization on continuous domains with finite-time guarantees by markov chain monte carlo methods [Text] / A. Lecchini-Visintini, J. Lygeros, J. Maciejowski // IEEE Transactions on Automatic Control. – 2010. – Vol. 55, Issue 12. – P. 2858–2863. doi: 10.1109/tac.2010.2078170
22. Befekadu, G. K. Risk-Sensitive Control Under Markov Modulated Denial-of-Service (DoS) Attack Strategies [Text] / G. K. Befekadu, V. Gupta, Panos J. Antsaklis // IEEE Transactions on Automatic Control. – 2015. – Vol. 60, Issue 12. – P. 3299–3304. doi: 10.1109/tac.2015.2416926
23. Subil, A. Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains [Text] / A. Subil, N. Suku Nair // Journal of Communications. – 2014. – Vol. 9, Issue 12. – P. 899–907. doi: 10.12720/jcm.9.12.899-907
24. Esmalifalak, M. Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study [Text] / M. Esmalifalak, G. Shi, Z. Han, L. Song // IEEE Transactions on Smart Grid. – 2013. – Vol. 4, Issue 1. – P. 160–169. doi: 10.1109/tsg.2012.2224391
25. Lakhno, V. Improving the transport cyber security under destructive impacts on information and communication systems [Text] / V. Lakhno, A. Hrabariev // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 1, Issue 3(79). – P. 4–11. doi: 10.15587/1729-4061.2016.60711
26. Lakhno, V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering [Text] / V. Lakhno // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 2, Issue 9 (80). – P. 18–25. doi: 10.15587/1729-4061.2016.66015