УДК 004.032+004.728+004.057.4

Пасічник Ольга Олегівна
Старший науковий співробітник відділу, *ORCID: 0000-0002-1857-7161*
Військова частина А1906, Київ
Бурба Олег Ігорович
Кандидат технічних наук, старший науковий співробітник, старший науковий співробітник відділу, *ORCID: 0000-0001-6705-6613*
Військова частина А1906, Київ

КЛАСИФІКАЦІЙНІ ОЗНАКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНО-МОНІТОРИНГОВИХ СИСТЕМ НА ОСНОВІ МОДЕЛІ OSI

Анотація. *Висвітлено підхід до систематизації та класифікації інформаційних ознак об'єктів інформаційно-моніторингових систем на основі базової еталонної моделі взаємодії відкритих систем (OSI). Розроблена формалізація інформаційно-моніторингового процесу може бути покладена в основу методичного забезпечення функціонування перспективної автоматизованої системи підтримки прийняття рішень на основі сигнатурного моніторингу інформаційних об'єктів. Запропонований підхід дає змогу забезпечити повноту і комплексність моніторингових досліджень інформаційних об'єктів.*

Ключові слова: інформаційно-моніторингова система; інформаційна ознака; сигнатурний моніторинг; модель взаємодії відкритих систем

Постановка проблеми

Одним із основних завдань системи забезпечення національної безпеки є здійснення моніторингу як комплексної, цілісної системи заходів, призначених для пошуку інформаційних ознак об'єктів, властивості яких підлягають дослідженню та відображають важливі сторони їх змісту. При цьому під моніторингом, як правило, розуміють цілеспрямоване збирання даних з конкретної проблеми, опрацювання, аналіз і доведення результатів аналізу й рекомендацій до всіх зацікавлених осіб [1].

З метою забезпечення системного безпекового супроводу реалізації національних інтересів держави, як режиму функціонування системи забезпечення національної безпеки України, провідними фахівцями в цій галузі запропоновано створити інформаційно-моніторингову систему національної безпеки (ІМС НБ). Головним завданням функціонування ІМС НБ повинно стати постійне централізоване створення цілеспрямованих та безперервних у часі моніторингових досліджень, суть та зміст яких має полягати в одержанні цільової інформації, виявленні її достатності, усуненні невизначеностей стосовно виміру і прогнозування станів та динаміки змін у системі національної безпеки, постійному спостереженні за якісними та кількісними інтегральними показниками (індикаторами) для забезпечення своєчасного та адекватного реагування на загрози реалізації національних інтересів [1; 2].

При цьому до ключових питань в галузі науково-практичних розробок для програмно-інструментального забезпечення комплексного інформаційного моніторингу відносять класифікацію як загроз загалом, так і відповідних інформаційних ознак. Наявність обґрунтованого підходу до визначення класифікаційних ознак об'єктів моніторингу дасть змогу уніфікувати процедури отримання та обробки моніторингової інформації.

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень та публікацій свідчить, що попри актуальність дослідження питань класифікації інформаційних ознак об'єктів ІМС НБ, основна увага дослідників привернута до розробки системно-концептуальних методологічних засад інформаційного моніторингу як складової системи забезпечення національної безпеки.

Зокрема, у [1-3] викладено методологічні основи системних досліджень проблем національної безпеки України, розроблені теоретичні засади організації інформаційно-аналітичного забезпечення та оцінки ефективності стратегічного планування у сфері державного управління забезпеченням національної безпеки. Визначено особливості функціонування системи забезпечення воєнної безпеки України, запропоновано концептуальні підходи до розробки механізму безпекового супроводу реалізації національних інтересів з використанням ІМС НБ.

 © О.О. Пасічник, О.І. Бурба

У [4] розроблені теоретико-методологічні основи, теоретичні засади організації інформаційно-аналітичного забезпечення та оцінки ефективності стратегічного планування у сфері державного управління забезпеченням національної безпеки. Визначено, що вкрай актуальним на сьогодні є створення ефективної системи моніторингу загроз та захисту власних національних інтересів.

У [5] запропонована процедура моніторингу небезпек та загроз воєнній безпеці держави та зазначено, що підвищувати ефективність моніторингу небезпек і загроз у системі забезпечення національної безпеки (СЗНБ) держави можна лише за наявності механізму його здійснення.

Питання застосування ІМС є актуальним не тільки для СЗНБ, а й для інших сфер суспільного життя. Зокрема у [6] запропонована узагальнена структурна організація клієнт-серверної архітектури ІМС в галузі науки і освіти. Серед усіх модулів моніторингового комплексу основну увагу приділено модулю формування пошукового запиту, оскільки він відіграє важливу роль для якісного розв'язання задач інформаційного моніторингу. Для вдосконалення процесу формування пошукового запиту було запропоновано новий підхід з використанням інтелектуального квазісемантичного редактора запиту.

У [7] запропонована концептуальна модель побудови єдиного інформаційного простору для вирішення завдань автоматизованої технології ведення екологічних паспортів територій в рамках державної системи моніторингу довкілля, зазначені завдання цієї системи, які поєднані системним підходом і дають змогу конвергувати усі процедури моніторингу з метою досягнення оптимальних результатів з точки зору достатності й достовірності інформації, а також економії ресурсів.

Щодо комерційної сфери, то за оцінками аналітиків компанії IDC [8], підприємство, яке використовує в роботі зі знаннями 1 000 співробітників, втрачає $48 000 щотижня або майже $2,5 мільйона щорічно через нездатність класифікувати, знайти і доставити необхідну інформацію кінцевому користувачу. Для великих корпорацій ця проблема є ще гострішою внаслідок того, що їм доводиться вирішувати питання ефективного обміну величезної кількості фінансової, технічної і маркетингової інформації між своїми співробітниками і партнерами, розташованими по всьому світу.

Однак слід зауважити, що більшість з відомих ІМС доцільно розглядати як контент-моніторингові системи, оскільки аналіз відкритих джерел був і залишається основним способом збирання необхідної інформації. Пошук серед таких джерел, збирання матеріалів та їхня систематизація – на сьогодні це найпоширеніший і найоптимальніший за співвідношенням "ціна/якість" спосіб формування інформаційної бази для прийняття рішень у різних сферах діяльності. Що ж до використання більш широкого спектру моніторингової інформації про інформаційні системи як, насамперед, технічні системи та механізми класифікації їх інформаційних ознак, то ці питання не набули широкого висвітлення.

Отже, у наведених публікаціях та інших наукових працях, з якими змогли ознайомитися автори, розглядається питання удосконалення СЗНБ за рахунок впровадження системи моніторингу загроз в державі. Що ж до спеціальних розробок, які присвячені прикладним науково-методичним питанням в цій галузі, то їм не приділяється відповідної уваги науковців. Зокрема, відсутність методичного підходу до класифікації інформаційних ознак об'єктів моніторингу обмежує можливості щодо розробки та застосування формальних методів і моделей при здійсненні державного управління забезпеченням національної безпеки.

Мета статті

З урахуванням зазначеного, мета статті полягає у розробці методичного підходу до визначення класифікаційних ознак об'єктів ІМС. При цьому завданням дослідження є забезпечення комплексності класифікації інформаційних ознак об'єктів моніторингу як інформаційних систем.

Виклад основного матеріалу

Основними джерелами, на які направлені моніторингові дії на сучасному етапі розвитку, є інформаційні системи, які містять дані щодо показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах. Об'єктами моніторингу є засоби електронно-обчислювальної техніки, інформаційно-телекомунікаційні системи, локальні і глобальні інформаційні мережі тощо. Іншими словами, під об'єктами моніторингу розглядається широкий спектр інформаційних систем [9], які здійснюють обробку моніторингової інформації.

Прикладами ведення інформаційного моніторингу, який проводився під час антитерористичної операції на Сході України, є визначення місць дислокації терористичних підрозділів за реєстрацією у мобільних мережах; перехоплення телефонних переговорів між представниками терористичних угруповань, військовослужбовцями Російської Федерації, російських диверсійних груп та кураторами з російської сторони; моніторинг мережевої активності та здійснення DDOS-атак на інформаційні ресурси органів державної влади та військового керівництва; ідентифікація особового складу терористичних

угруповань, підрозділів Російської Федерації за особистими даними у соціальних мережах; доступ до електронної пошти осіб, причетних до організації та фінансування терористичних угруповань.

Як бачимо з наведеного вище, моніторингові дії здійснюються не тільки на рівні контенту, а й на рівнях інформаційних систем, які характеризують їх структурно-технічні характеристики. А це, в свою чергу, породжує необхідність комплексного дослідження об'єктів інформаційного моніторингу як інформаційних систем.

Побудова таких систем здійснюється з урахуванням відповідних принципів, серед яких одним із основних є принцип відкритості. За визначенням комітету 1003 Інституту інженерів з електроніки й електротехніки (Institute of Electrical and Electronic Engineers – IEEE) принцип відкритості інформаційних систем полягає у тому, що відкрита система реалізовує відкриті специфікації на інтерфейси, служби і формати даних, достатні для того, щоб забезпечити:

– можливість перенесення (мобільність) прикладних систем, розроблених належним чином з мінімальними змінами на широкий діапазон систем;

– спільну роботу (інтероперабельність) з іншими прикладними системами на локальних і віддалених платформах;

– взаємодію з користувачами у стилі, що полегшує останнім перехід від системи до системи (мобільність користувачів) [10].

Ключовим моментом є використання терміну "відкрита специфікація", яка визначається як загальнодоступна специфікація, що підтримується відкритим, узгоджувальним процесом, спрямованим на постійну адаптацію нової технології, і відповідає стандартам.

В широкому розумінні відкритою може бути названа будь-яка система (комп'ютер, обчислювальна мережа, операційна система, програмний пакет, інші апаратні чи програмні продукти), яка побудована відповідно до відкритих специфікацій. При цьому під терміном "специфікація" в обчислювальній техніці розуміють опис апаратних або програмних компонентів: способи їх функціонування, взаємодію з іншими компонентами, умови експлуатації, обмеження і особливі характеристики [10].

Враховуючи наведене, інформаційно-моніторингові об'єкти в цілому та їх елементи можна розглядати як відкриті системи, що взаємодіють між собою.

Таке припущення, в свою чергу, дає змогу обґрунтовано використовувати для класифікації і опису моніторингових ознак інформаційних об'єктів базову еталонну модель взаємодії відкритих систем (Open Systems Interconnection basic reference model – OSI).

В моделі OSI під відкритою системою розуміють мережевий пристрій (вузол), що може взаємодіяти з іншими мережевими пристроями (вузлами) з використанням стандартних правил, які визначають формат, зміст і значення прийнятих чи відправлених повідомлень. При цьому згідно з еталонною моделлю відкрита телекомунікаційна система повинна розглядатися як сукупність (стек) протоколів.

В цій моделі описані загальні принципи, які регламентують взаємодію відкритих систем. Ці принципи утворюють сім рівнів [11]:

7 – прикладний (Application Layer);
6 – представницький (Presentation Layer);
5 – сеансовий (Session Layer);
4 – транспортний (Transport Layer);
3 – мережевий (Network Layer);
2 – канальний (Data Link Layer);
1 – фізичний (Physical Layer).

Три нижніх рівні (фізичний, канальний і мережевий) є мережезалежними. Протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі та з використаним комунікаційним обладнанням. Наприклад, перехід на використання оптоволоконних технологій FDDI означає зміну протоколів фізичного і канального рівня у всіх вузлах мережі. Ці протоколи мають узагальнену назву – телекомунікаційна підсистема. Вони повністю вирішують завдання обміну інформацією із заданим рівнем якості в складних мережах, що складаються з мереж з довільною топологією та різними технологіями.

Три верхні рівні (сеансовий, представницький і прикладний) вирішують завдання надання прикладних сервісів на підставі наявної транспортної підсистеми. Вони орієнтовані на функціонування програмних додатків і мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають жодні зміни в топології мережі, заміна обладнання або перехід на іншу мережеву технологію. Так, перехід від Ethernet на високошвидкісну технологію 100VG-AnyLAN не потребує жодних змін в програмних засобах, що реалізовують функції прикладного, представницького і сеансового рівнів.

Транспортний рівень є проміжним, він приховує всі деталі функціонування протоколів нижніх рівнів від протоколів верхніх рівнів. Це дає можливість розробляти програмне забезпечення, що не залежить від технічних засобів передавання повідомлень, які безпосередньо реалізують транспортування.

Тому, об'єкти ІМС в нотації OSI можна надати сукупністю протоколів, які використовуються на відповідних рівнях взаємодії.

При цьому класифікація інформаційних ознак об'єктів ІМС полягає у визначенні сукупності інформаційних ознак протоколів на рівнях моделі OSI.

У подальшому для використання в ІМС на їх основі здійснюється побудова відповідних комплексних моніторингових ознак – сигнатур.

Враховуючи зазначене, сигнатурний моніторинг полягає у визначенні сукупності моніторингових ознак на рівнях протоколів моделі OSI і побудові на їх основі відповідних сигнатур. В якості ознак загалом можна розглядати специфікацію протоколів, які на кожному рівні деталізуються відповідними значеннями пакетів, кадрів, байтів.

З урахуванням цього для моніторингу сигнатур можуть використовуватися такі підходи.

1) За шаблоном даних. Моніторингові дії направлені на виявлення фіксованої послідовності байтів в розглянутому елементі даних мережевого трафіку. Ці сигнатури містять деякі ключові слова або вирази.

2) За шаблоном стану. За результатами моніторингу одного пакету встановлюється стан потоку даних. Поява іншого пакету (або пакетів), який не відповідає даному стану, вважається аномалією.

3) За шаблоном протоколу. Для формування сигнатури використовується аналіз різних елементів протоколу. При цьому здійснюється порівняння зі специфікацією і згідно правил визначаються відмінності.

4) За частотою подій або перевищення граничної величини. Ці сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, кількість яких перевищує задані заздалегідь показники.

5) За законом розподілу частоти подій. Такі сигнатури мають місце за наявності достатньої статистики щодо характеру інтенсивності подій. Якщо така статистика відсутня, то доцільно використовувати 5-числові зведення [12].

Для формалізації запропонованої класифікації інформаційних ознак об'єктів ІМС введемо такі позначення.

1. О – інформаційний об'єкт моніторингових досліджень (інформаційна система).

2. $T_{ij} = \left\{ t_{ij}^{k}, i = \overline{1,7}; j = \overline{1,n_i}; k = \overline{1,m_{ij}} \right\}$ – множина інформаційних ознак $t_{ij_i}^{k}$ моніторингового об'єкта О (множина характеристик специфікацій протоколів об'єкта на і-х рівнях моделі OSI), де n_j – кількість відповідних протоколів (груп інформаційних ознак); m_k – кількість інформаційних ознак (характеристик) в j-му протоколі.

3. $S = \bigcup_{i=1}^{7} T_{ij_i}$ – комплексна моніторингова ознака інформаційного об'єкта (сигнатура).

4. П – інформаційно-моніторинговий процес (ІМП).

Спочатку деталізуємо множини інформаційних ознак:

$$\begin{bmatrix} T_{11} \\ T_{12} \\ \vdots \\ T_{1n_1} \end{bmatrix} = \begin{bmatrix} ph_{11}^{1} & ph_{11}^{2} & \cdots & ph_{11}^{m_{11}} \\ ph_{12}^{1} & ph_{12}^{2} & \cdots & ph_{12}^{m_{12}} \\ \vdots & \vdots & \cdots & \vdots \\ ph_{1n_1}^{1} & ph_{1n_1}^{2} & \cdots & ph_{1n_1}^{m_{1n_1}} \end{bmatrix};$$

$$\begin{bmatrix} T_{21} \\ T_{22} \\ \vdots \\ T_{2n_2} \end{bmatrix} = \begin{bmatrix} d_{21}^{1} & d_{21}^{2} & \cdots & d_{21}^{m_{21}} \\ d_{22}^{1} & d_{22}^{2} & \cdots & d_{22}^{m_{22}} \\ \vdots & \vdots & \cdots & \vdots \\ d_{2n_2}^{1} & d_{2n_2}^{2} & \cdots & d_{2n_2}^{m_{2n_2}} \end{bmatrix};$$

$$\begin{bmatrix} T_{31} \\ T_{32} \\ \vdots \\ T_{3n_3} \end{bmatrix} = \begin{bmatrix} n_{31}^{1} & n_{31}^{2} & \cdots & n_{31}^{m_{31}} \\ n_{32}^{1} & n_{32}^{2} & \cdots & n_{32}^{m_{32}} \\ \vdots & \vdots & \cdots & \vdots \\ n_{3n_3}^{1} & n_{3n_3}^{2} & \cdots & n_{3n_3}^{m_{3n_3}} \end{bmatrix};$$

$$\begin{bmatrix} T_{41} \\ T_{42} \\ \vdots \\ T_{4n_4} \end{bmatrix} = \begin{bmatrix} tr_{41}^{1} & tr_{41}^{2} & \cdots & tr_{41}^{m_{41}} \\ tr_{42}^{1} & tr_{42}^{2} & \cdots & tr_{42}^{m_{42}} \\ \vdots & \vdots & \cdots & \vdots \\ tr_{4n_4}^{1} & tr_{4n_4}^{2} & \cdots & tr_{4n_4}^{m_{4n_4}} \end{bmatrix};$$

$$\begin{bmatrix} T_{51} \\ T_{52} \\ \vdots \\ T_{5n_5} \end{bmatrix} = \begin{bmatrix} s_{51}^{1} & s_{51}^{2} & \cdots & s_{51}^{m_{51}} \\ s_{52}^{1} & s_{52}^{2} & \cdots & s_{52}^{m_{52}} \\ \vdots & \vdots & \cdots & \vdots \\ s_{5n_5}^{1} & s_{5n_5}^{2} & \cdots & s_{5n_5}^{m_{5n_5}} \end{bmatrix};$$

$$\begin{bmatrix} T_{61} \\ T_{62} \\ \vdots \\ T_{6n_6} \end{bmatrix} = \begin{bmatrix} p_{61}^{1} & p_{61}^{2} & \cdots & p_{61}^{m_{61}} \\ p_{62}^{1} & p_{62}^{2} & \cdots & p_{62}^{m_{62}} \\ \vdots & \vdots & \cdots & \vdots \\ p_{6n_6}^{1} & p_{6n_6}^{2} & \cdots & p_{6n_6}^{m_{6n_6}} \end{bmatrix};$$

$$\begin{bmatrix} T_{71} \\ T_{72} \\ \vdots \\ T_{7n_7} \end{bmatrix} = \begin{bmatrix} a_{71}^{1} & a_{71}^{2} & \cdots & a_{71}^{m_{71}} \\ a_{72}^{1} & a_{72}^{2} & \cdots & a_{72}^{m_{72}} \\ \vdots & \vdots & \cdots & \vdots \\ a_{7n_7}^{1} & a_{7n_7}^{2} & \cdots & a_{7n_7}^{m_{7n_7}} \end{bmatrix},$$

де ph_{ij}^{k}, d_{ij}^{k}, n_{ij}^{k}, tr_{ij}^{k}, s_{ij}^{k}, p_{ij}^{k}, a_{ij}^{k} – інформаційні ознаки моніторингового об'єкта на фізичному, канальному, мережевому, транспортному, сеансовому, представницькому та прикладному рівнях моделі OSI відповідно.

Далі формалізуємо формування сигнатур:

$$S_{\forall j} = T_{1j} \cup T_{2j} \cup T_{3j} \cup T_{4j} \cup T_{5j} \cup T_{6j} \cup T_{7j} =$$

$$= \left[ph_{1j}^{1}, ph_{1j}^{2}, ..., ph_{1j}^{m_{1j}} \right], \left[d_{2j}^{1}, d_{2j}^{2}, ..., d_{2j}^{m_{2j}} \right],$$

$$\left[n_{3j}^{1}, n_{3j}^{2}, ..., n_{3j}^{m_{3j}} \right], \left[tr_{4j}^{1}, tr_{4j}^{2}, ..., tr_{4j}^{m_{4j}} \right],$$

$$\left[s_{5j}^{1}, s_{5j}^{2}, ..., s_{5j}^{m_{5j}} \right], \left[p_{6j}^{1}, p_{6j}^{2}, ..., p_{6j}^{m_{6j}} \right],$$

$$\left[a_{7j}^{1}, a_{7j}^{2}, ..., a_{7j}^{m_{7j}} \right].$$

Наприкінці представимо ІМП так:

$$П = S_1 + S_2 + ... + S_q ,$$

де q – кількість сигнатур інформаційного об'єкта, на який спрямовані моніторингові дії.

Запропонована формалізація дає змогу представити ІМП у формі, яка належним чином враховує інформаційні ознаки і надає можливість визначити їх у вигляді сукупності сигнатур, що характеризують властивості інформаційних об'єктів в рамках цього процесу.

Висновки

Обґрунтовано підхід до систематизації класифікаційних ознак об'єктів інформаційно-моніторингових систем національної безпеки на основі моделі OSI, який забезпечує повноту і комплексність моніторингового дослідження інформаційного об'єкта та уніфікацію процедур отримання й обробки моніторингової інформації.

Запропонована формалізація інформаційно-моніторингового процесу може бути покладена в основу методичного (математичного) забезпечення функціонування перспективної автоматизованої системи підтримки прийняття рішень на основі сигнатурного моніторингу інформаційних об'єктів.

Подальшим напрямом досліджень може бути розвиток робастих механізмів сигнатурного моніторингу інформаційних об'єктів, придатних до практичного використання як технологічних складових інформаційно-моніторингових систем національної безпеки.

Список літератури

1. Богданович В.Ю. Концептуальна модель інформаційно-моніторингової системи національної безпеки / В.Ю. Богданович, А.Л. Висідалко // Сучасний захист інформації. – К. : ДУТ, 2014. – №1. – С. 81–88.

2. Богданович В.Ю. Забезпечення безпеки інформаційних процесів безпекового супроводу реалізації національних інтересів / В.Ю. Богданович, А.Л. Висідалко // Сучасний захист інформації. – К. : ДУТ, 2013. – №3. – С. 60–66.

3. Горбулін В. П. Стратегічне планування: вирішення проблем національної безпеки [Монографія] / В.П. Горбулін, А.Б. Качинський – К. :НІСД, 2010. – 288 с.

4. Семенченко А.І. Стратегічне планування у сфері державного управління забезпеченням національної безпеки: [Монографія] / А.І. Семенченко. – К., 2007. – 296 с.

5. Богданович В.Ю. Методологічний підхід до автоматизації інформаційно-аналітичних процесів безпекового супроводу реалізації національних інтересів / В.Ю. Богданович, А.Л. Висідалко // Сучасний захист інформації. – К. : ДУТ, 2014. – №3. – С. 4–10.

6. Перспективи застосування контент-моніторингових комплексів в науково-освітньому сегменті електронного інформаційного простору Електронний ресурс] – Режим доступу: http://elibrary.kubg.edu.ua/2897/1/A_Mykhailiuk_ VSNUIVD _13_IS.pdf

7. Доманецька, І. М. Концептуальна модель побудови єдиного інформаційного простору для вирішення завдань автоматизованої технології ведення екологічних паспортів територій в рамках державної системи моніторингу довкілля [Текст] / І. М. Доманецька, О. В. Хроленко: зб. наук. пр. // Управління розвитком складних систем. – К. : КНУБА, 2010. – №4. – С. 40-44.

8. Pricing and Leasing Intelligence [Електронний ресурс] – Режим доступу: http://www.idc.com/prodserv/insights/financial/index.jsp

9. Самохвалов Ю.Я. Предпроектное проектирование автоматизированных систем [Монография] / Ю.Я. Самохвалов, О.И. Бурба – К.: ТриК, 2013. – 295 с.

10. Thomas E. Service-Oriented Architecture (SOA): Concepts, Technology, and Design / E. Thomas Prentice Hall PTR, 2005. 792 с.

11. Капустин С.П. Информационно-вычислительные сети : учебное пособие / С.П. Капустин, В. Е. Дементьев. – Ульяновск : УлГТУ, 2011. – 141 с.

12. Тьюки Дж. Анализ результатов наблюдений : разведочный анализ [Перевод с англ.]/ Дж. Тьюки. – М.: Мир, 1981. – 696 с.

Стаття надійшла до редколегії 20.03.2015

Рецензент: д-р техн. наук, проф. В.Ф. Єрохін, Інститут спеціального зв'язку і захисту інформації Національного технічного університету України "КПІ", Київ.

Пасечник Ольга Олеговна
Старший научный сотрудник отдела, *ORCID: 0000-0002-1857-7161*
Воинская часть А1906, Киев
Бурба Олег Игоревич
Кандидат технических наук, старший научный сотрудник, старший научный сотрудник отдела, *ORCID: 0000-0001-6705-6613*
Воинская часть А1906, Киев

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ ОБЪЕКТОВ ИНФОРМАЦИОННО-МОНИТОРИНГОВЫХ СИСТЕМ НА ОСНОВЕ МОДЕЛИ OSI

Аннотация. *Рассмотрен подход к систематизации и классификации информационных признаков объектов информационно-мониторинговых систем на основе базовой эталонной модели взаимодействия открытых систем (OSI). Разработанная формализация информационно-мониторингового процесса может быть положена в основу методического обеспечения функционирования перспективной автоматизированной системы поддержки принятия решений на основе сигнатурного мониторинга информационных объектов. Предложенный подход позволяет обеспечить полноту и комплексность мониторинговых исследований информационных объектов.*

Ключевые слова: информационно-мониторинговая система; информационный признак; сигнатурный мониторинг; модель взаимодействия открытых систем

Pasichnyk Olga
Senior Researcher, *ORCID: 0000-0002-1857-7161*
Military unit A1906, Kiev
Burba Oleg
Doctor of Technical Sciences, Senior Researcher, Senior Researcher, *ORCID: 0000-0001-6705-6613*
Military unit A1906, Kiev

CLASSIFICATION FEATURES OF THE OBJECT OF INFORMATION MONITORING SYSTEM BASED ON THE MODEL OSI

Abstract. *An important aspect of providing integrated information monitoring is a classification of information threats in general and relevant information features. Availability of reasonable approach to determining classifications monitoring facilities will help standardize procedures for obtaining and processing monitoring information. The article highlights examples of conduct monitoring information to be considered not only at the level of content, but also on the level of information systems, which creates the need for a comprehensive study of objects as information monitoring information systems. This assumption allows to be used reasonably to classify and describe the features of monitoring information object son the basic of reference model of open systems interconnection (OSI). Signature monitoring is determining the set of monitoring features at the protocol level of the OSI model and building on their basis respective signatures. As can be seen signs of general data protocols at each level of detail appropriate values packets, frames, bytes. Developed formalization of information and the monitoring process can be the basis for the functioning of promising methods of automated decision support system based on signature monitoring information objects. The proposed approach makes it possible to ensure a comprehensive and integrated monitoring research information objects.*

Keywords: information and monitoring system; information sign; signature-based monitoring; OSI model.

References

1. Bogdanovich, V.U. (2014). Conceptual model of information and monitoring of national security. DUT: Modern Data Protection, 1, 81-88.

2. Bogdanovich, V.U. (2013). Securing information security processes support the realization of national interests.DUT: Modern Data Protection, 3, 60-66.

3. Horbulin, V.P. & Kaczynski, A.B. (2010). Strategic planning: addressing national security issues. Monograph, 288.

4. Semenchenko, A.I. (2007). Strategic planning in public administration national security. Monograph, 296.

5. Bogdanovich, V.U. (2014). Methodological approach to automation of information and analytical support processes Security pursue national interests / V.U. Bogdanovich, A.L.Vysidalko // Modern Data Protection, 3, 4-10.

6. Prospects of content – monitoring systems in science and education segment of electronic information space [electronicsource]. - http://elibrary.kubg.edu.ua/2897/1/A_Mykhailiuk_VSNUIVD_13_IS.pdf.

7. Domanetska, I. (2010). Conceptual model of building a common information space to meet the challenges of automated technologies for environmental passports areas within the Environmental Monitoring / I. Domanetska, A.V.Hrolenko // Management of development of complex systems, 4, 40-44.

8. Pricing and Leasing Intelligence [electronicsource] . – http://www.idc.com/prodserv/insights/financial/index.jsp

9. Samokhvalov, Yu.Ya., Burba O.I. Pre-design of the automated systems. Monograph, 295.

10. Thomas, E. (2005). Service-Oriented Architecture (SOA): Concepts, Technology, andDesign.PrenticeHall PTR, 792.

11. Kapustin, S.P. (2011). Information and computing Network. Tutorial , 141.

12. Tukey, J. (1981). Analysis of the results of observations: exploratory analysis. Monograph, 696.

Посилання на публікацію

APA *Pasichnyk, O., & Burba, O. (2015). Classification features of the object information monitoring system based on the model OSI. Management of Development of Complex Systems, 22 (1), 116-121.*

ГОСТ *Пасічник, О.О. Класифікаційні ознаки об'єктів інформаційно-моніторингових систем на основі моделі OSI [Текст] / О.О. Пасічник, О.І. Бурба // Управління розвитком складних систем. – 2015. - № 22 (1). – С. 116-121.*