СИСТЕМА ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЇ ПОРУШНИКА В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Анна Корченко, Владислава Волянська, Андрій Гізун

Національний авіаційний університет, Україна

КОРЧЕНКО Анна Олександрівна, к.т.н.

Рік та місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, комп'ютерна безпека, експертні системи.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, підручники та навчально-методичні посібники.
E-mail: annakor@ukr.net

ВОЛЯНСЬКА Владислава Вікторівна

Рік та місце народження: 1977 рік, м. Плавськ, Росія.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: асистент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека операційних систем, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації.
Публікації: більше 15 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях.
E-mail: volyanska.vladyslava@gmail.com

ГІЗУН Андрій Іванович

Рік та місце народження: 1987 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: асистент кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації, штучні імунні системи, управління безперервністю бізнесу та правове забезпечення захисту інформації.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: andriy.gizun@gmail.com

Анотація. *Ефективне виявлення порушника інформаційної безпеки в інформаційно-комунікаційних мережах та системах є складною задачею, що потребує використання спеціальних засобів захисту – систем виявлення порушника. Більшість таких систем грунтуються на застосуванні сигнатурних методів, що мають ряд недоліків, серед яких вимогливість до ресурсів і витрати різного характеру, наприклад, пов'язані з вибіркою статистичних даних, навчанням систем, їх адаптацією та ін. Більш ефективні в цьому відношенні є експертні підходи, засновані на використанні знань і досвіду фахівців відповідної предметної області. В роботі запропоновано структурне рішення системи виявлення і ідентифікації порушника на нечіткій логіці. Система складається з підсистем первинної обробки чітких і нечітких параметрів, формування нечітких еталонів і евристичних правил (відповідно по нечітким та чітким контрольованим параметрам), а також модулів формування кортежу, лінгвістичного виводу і візуалізації, які дозволяють виявити і ідентифікувати порушника. Результат роботи системи представляється у лінгвістичній і графічних формах.*

Ключові слова: *порушник інформаційної безпеки, ідентифікація порушника, системи виявлення вторгнень, системи виявлення порушника, нечітка логіка, безпека інформаційно-комунікаційних систем та мереж, евристичні правила.*

Актуальність

З розвитком інформаційних технологій, впровадженням інформаційно-комунікаційних систем (ІКС) в усі сфери діяльності людини, суспільства та держави проблема захисту інформації стає все більш важливою. При цьому поява нових технологій не лише сприяє підвищенню ефективності процесів обробки і обміну інформацією, а і породжує значну кількість нових загроз і можливостей порушення інформаційної безпеки (ІБ) незважаючи на широкий спектр систем захисту інформації.

Однак лише виявлення факту порушення захисту ІКС на сьогодні є недостатнім. Для ефективного вирішення проблеми зловмисної діяльності порушника слід також ідентифікувати його особу. Застосування концепції Honeypot-технологій дає змогу за допомогою аналізу поведінкових характеристик зловмисника визначити принаймні його приналежність до певної групи (або категорії) осіб, що досить важливо для подальшого розслідування. У цьому аспекті системи виявлення порушника (СВП), що можуть не тільки виявляти, але і ідентифікувати нелегітимних осіб в ІКС мають чи не вирішальне значення.

Проте більшість СВП побудовані за сигнатурним принципом, що є не ефективним при виявленні порушника в слабоформалізованому середовищі. Суттєвий недолік таких СВП пов'язаний з необхідністю довготривалого підготовчого етапу перед введенням їх в експлуатацію. В межах такої підготовки зазвичай здійснюється вибірка статистичних даних, реалізується процес навчання тощо [1]. Більш ефективні в цьому відношенні є системи, які засновані на експертному підході. Тому актуальним завданням є розробка відповідних технічних рішень, заснованих на цьому підході, який позбавлений зазначених недоліків.

Аналіз існуючих досліджень

У попередніх роботах були виділені основні типи порушника ІБ та параметри для їх виявлення і ідентифікації [2], а також розроблена модель еталонів лінгвістичних змінних для параметрів нечіткого характеру [3], які за рахунок формування множин пар «порушник → параметр» і «порушник → набір логіко-лінгвістичних зв'язок» дозволяють формалізувати процеси виявлення порушника в слабоформалізованому середовищі з нечіткими умовами. А виходячи з результатів виміру поточних величин визначених параметрів і прив'язки їх до певного типу порушника можна його ідентифікувати.

Крім того в роботі [4] сформовані евристичні правила, які за рахунок множини еталонних параметрів дозволяють провести безпосереднє виявлення ознак діяльності порушника ІБ і визначити його тип з певним показником небезпеки, породженої можливою атакою порушника.

На основі цього в даній роботі запропонована технічна реалізація СВП евристичного типу. За основу даної системи використаємо підхід до побудови системи виявлення аномального стану в комп'ютерних мережах, наведений в роботі [5].

Основна мета дослідження

Метою роботи є розробка нового структурного рішення для вирішення проблеми фіксування та ідентифікації порушника в ІКС. Таке рішення дозволяє розширити функціональні можливості сучасних СВП за рахунок використання експертних методів і, як наслідок, підвищити ефективність їх функціонування в умовах слабоформалізованого середовища.

Основна частина дослідження

До складу розробленої СВП (рис. 1) входять: підсистема первинної обробки нечітких параметрів (ППОНП) і підсистема первинної обробки чітких параметрів (ППОЧП), що призначені для формування множин атак та параметрів і їх фазифікації; підсистема формування нечітких еталонів (ПФНЕ), в якій формуються всі необхідні терми для кожної лінгвістичної змінної нечітких параметрів з метою виміру їх поточних значень; підсистеми формування евристичних правил (ПФЕП) і формування чітких евристичних правил (ПФЧЕП), в яких створюються множини правил на основі відповідно нечітких і чітких параметрів мережевого середовища та хостів для виявлення і ідентифікації порушника ІБ; модулі формування кортежів (МФК), логічного висновку (МЛВ) і візуалізації (МВ), призначені для формування результату в логіко-лінгвістичному та графічному представлені; модуль управління системою (МУС), що служить для переведення системи в режим корекції еталонів (РКЕ), корекції правил (РКП) і формування управляючого сигналу (УС), який запускає роботу ППОЧП при виявлені ознак порушення безпеки на основі аналізу нечітких параметрів.

Система виявлення і ідентифікації порушника (СВІП) в ІКС та мережах функціонує наступним чином. Перед початком обчислювального процесу в ПФНЕ на основі хостових та мережевих параметрів [2] формуються множини класів порушника $I_i(\mathrm{i}=\overline{1,n})$ і нечітких параметрів $P_i\ (\mathrm{i}=\overline{1,m})$, за допомогою яких на основі методу лінгвістичних термів з використанням статистичних даних (МЛТС) [1] генеруються еталони для певних лінгвістичних змінних по кожному терму T_{ij}^{ef}.

Відповідно до отриманих еталонів в ПФЕП створюються шаблони наборів евристичних правил $ER_i(\mathrm{i}=\overline{1,n})$, що використовуються для фіксації ознак діяльності порушника і подальшої його ідентифікації. Аналогічний процес проходить в ПФЧЕП, але вже на основі чітких хостових параметрів. Ці шаблони і еталони параметрів не змінюються на протязі всього часу роботи СВІП, але при появі необхідності можуть бути змінені шляхом переведення цих підсистем в РКЕ і РКП.

Оскільки СВІП є мультиагентною системою, агенти якої встановлені на l вузлах (хостах) контрольованої ІКС, то паралельно в l регістрів порушників та параметрів (РППk, $k=\overline{1,l}$) ППОНП заносяться ідентифікатори порушника I_i^k $(\mathrm{i}=\overline{1,n}$,

$k=\overline{1,l}$) і з певною, заздалегідь встановленою, періодичністю поточні значення параметрів P_i^k ($i=\overline{1,m}$, $k=\overline{1,l}$).

У нашому випадку для *n=6* і *m=8* в *k*-ому вузлі ІКС фіксуються I_i^k і P_i^k, які дозволяють виявити ознаки діяльності 6 видів порушника [2] I_1^k, I_2^k, I_3^k, I_4^k, I_5^k і I_6^k (D^k, S^k, C^k, H^k, SB^k і B^k – дезінформатор, спамер, крекер, хакер, спам-бот і бот-зломщик відповідно) на основі 8 параметрів P_1^k, P_2^k, P_3^k, P_4^k, P_5^k, P_6^k, P_7^k і P_8^k ($T\log^k$, $N\log^k$, $TS\log^k$, I^k, CPU^k, NEF^k, NEr^k і $RT\,\mathrm{Pr}/F^k$ –час входу в систему, частота запитів на вхід у систему, час затрачений на вхід в систему, інтенсивність дій, процесорний час/завантаженість процесора, кількість виконуваних файлів, кількість збоїв та помилок і час виконання процесу/файлу відповідно).

Для формування зв'язки конкретного типу порушника ІБ з параметрами, що необхідні для його виявлення, використовуються *l* блоків зв'язки порушника з параметрами БЗПП$_k$($k=\overline{1,l}$), які являють собою спеціальним чином організовані запам'ятовуючі пристрої. Для нашого випадку при *n=6* і *m=8* в *k*-ому вузлі з ідентифікаторами порушника I_1^k, I_2^k, I_3^k, I_4^k, I_5^k і I_6^k відповідно створюються зв'язки з параметрами $P_{n_1}^k=P_{n_3}^k=P_{n_4}^k=(P_1^k, P_2^k, P_3^k, P_5^k, P_6^k, P_7^k, P_8^k)$, $P_{n_2}^k=P_{n_5}^k=(P_4^k, P_5^k, P_7^k, P_8^k)$ і $P_{n_6}^k=(P_1^k, P_2^k, P_3^k, P_4^k, P_5^k, P_6^k, P_7^k, P_8^k)$, тобто $D^k=C^k=H^k\to\{T\log^k, N\log^k, TS\log^k, CPU^k, NEF^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$, $S^k=SB^k\to\{I^k, CPU^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$ і $B^k\to\{T\log^k, N\log^k, TS\log^k, I^k, CPU^k, NEF^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$, ($k=\overline{1,l}$). Тут доцільно зробити відмітку стосовно організації БЗПП: ідентифікатори D^k, S^k, C^k, H^k, SB^k і B^k будуть адресами даного запам'ятовуючого пристрою, а $\{T\log^k, N\log^k, TS\log^k, CPU^k, NEF^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$, $\{I^k, CPU^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$і $\{T\log^k, N\log^k, TS\log^k, I^k, CPU^k, NEF^k, NEr^k, RT\,\mathrm{Pr}/F^k\}$ відповідно вмістом комірок за цими адресами.

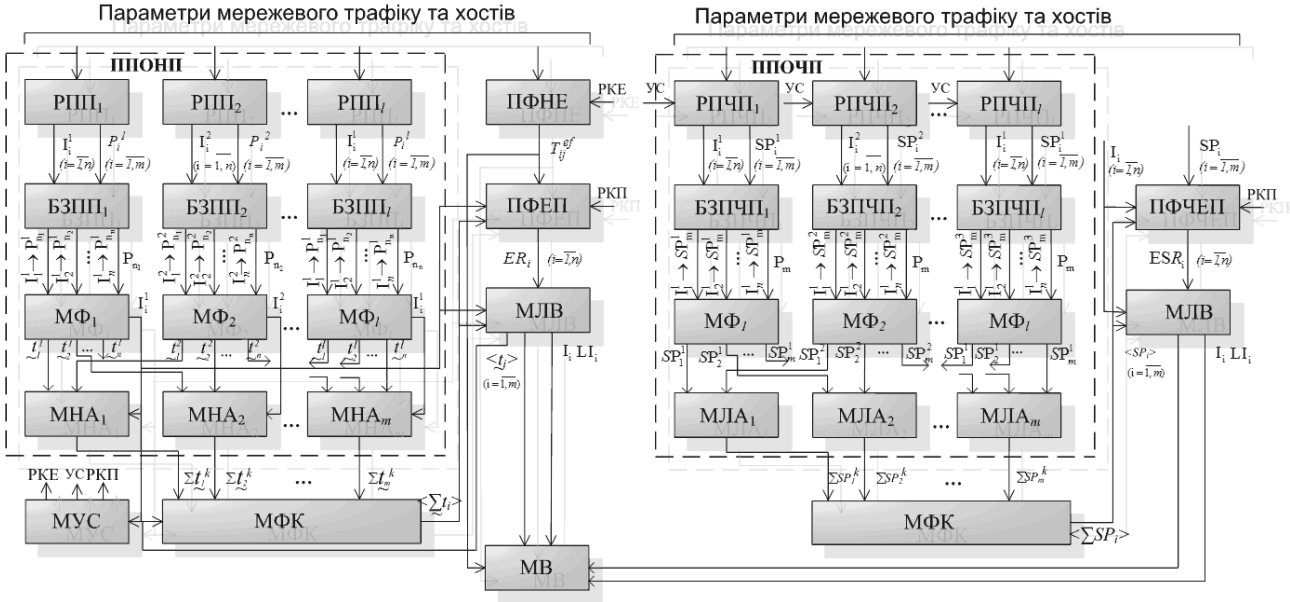

Рис. 1. Структура системи виявлення та ідентифікації порушника інформаційної безпеки в інформаційно-комунікаційних мережах

По закінченню процедури формування зв'язок $I_i^k\to P_{n_i}^k$ в БЗПП$_k$($k=\overline{1,l}$) за допомогою модулів фазифікації МФ$_k$($k=\overline{1,l}$) відбуваєтьсяперетворення множини поточних значень параметрів, що фіксуються протягом певного проміжку часу в одне нечітке число і таким чином на виході МФ$_k$ отримаємо *m* нечітких чисел $\underset{\sim}{t}_i^k$ ($i=\overline{1,m}$) по кожному параметру пов'язаних з відповідним I_i^k. Наприклад, при *m=6* матимемо: $\underset{\sim}{t}_1^k=\underset{\sim}{t}_{T\log}^k$, $\underset{\sim}{t}_2^k=\underset{\sim}{t}_{N\log}^k$, $\underset{\sim}{t}_3^k=\underset{\sim}{t}_{TS\log}^k$, $\underset{\sim}{t}_4^k=\underset{\sim}{t}_I^k$, $\underset{\sim}{t}_5^k=\underset{\sim}{t}_{CPU}^k$, $\underset{\sim}{t}_6^k=\underset{\sim}{t}_{NEF}^k$, $\underset{\sim}{t}_7^k=\underset{\sim}{t}_{NEr}^k$ і $\underset{\sim}{t}_8^k=\underset{\sim}{t}_{RT\,\mathrm{Pr}/F}^k$.

Після цього отримані $\underset{\sim}{t}^k$ ($i=\overline{1,n}$, $k=\overline{1,l}$) паралельно (на відміну від системи виявлення аномального стану, запропонованої в [5], де такі операції здійснювались послідовно по сигналу комутації) відповідно до кожного параметру передаються до модулів нечіткої арифметики МНА$_i$ ($i=\overline{1,m}$) для отримання сумарних показників $\sum\underset{\sim}{t}^k$, які характеризують величину контрольованих параметрів на всіх вузлах ІКС. У МНА використовується один з можливих методів реалізації операцій нечіткої арифметики відповідно до заданих користувачем критеріїв. Якщо процес виявлення порушника ІБ здійснюється тільки на одному вузлі ІКС, то МНА в системі лише один і є повністю

прозорим, тобто жодних логіко-арифметичних операцій на ньому не виконується і не створюються сумарні значення змінних.

Отримані сумарні показники передаються до МФК, де вони записуються по кожному параметру в кортеж $< \sum \underset{\sim}{t}_i >$. На основі сформованого кортежу з використанням ініційованих в ПФЕП множини правил ER_i $(\mathrm{i} = \overline{1,n})$ в МЛВ за допомогою логіко-лінгвістичних зв'язок $LI_i(\mathrm{i} = \overline{1,d})$ виконується виявлення можливого порушника і ідентифікація його типу. Отриманий результат може відображатися як в лінгвістичній так і через МВ в графічній формі у вигляді НЧ, зображеного на фоні сформованих в ПФНЕ еталонних значень лінгвістичних змінних.

Якщо результат роботи МЛВ є позитивним, тобто виявлені ознаки діяльності порушника, то МУС формує УС, що відкриває регістри порушника та чітких параметрів (РПЧП) ППОЧП, таким чином система переходить до 2-го етапу свого функціонування – виявлення та ідентифікації порушника на основі чітких параметрів.

У l регістрів РПЧП, де l – кількість вузлів в ІКСзаносяться ідентифікатори порушника I_i^k $(\mathrm{i} = \overline{1,n}$, $\mathrm{k} = \overline{1,l})$ і з певною, заздалегідь встановленою, періодичністю поточні значення чітких параметрів SP_i^k $(\mathrm{i} = \overline{1,m}$, $\mathrm{k} = \overline{1,l})$.

У нашому випадку для n=6 і m=7 в k-ому вузлі ІКС проходить I_iі P_i, які дозволяють виявити ознаки діяльності 6 видів порушника I_1^k, I_2^k, I_3^k, I_4^k, I_5^k і I_6^k (D^k, S^k, C^k, H^k, SB^k і B^k) на основі 7 параметрів SP_1^k, SP_2^k, SP_3^k, SP_4^k, SP_5^k, SP_6^k і SP_7^k (UID^k, $AtEF^k$, $U\,\mathrm{Pr}^k$, $TrFin^k$, $ModF^k$, $TrFout^k$ і KS^k – ім'я користувача при вході, тип використовуваних файлів при атаці, невластиві процеси, передача файлу в систему, зміна файлів, копіювання/передача фалів з системи і натиснення клавіш консолі відповідно).

Аналогічно до процесів в ППОНП для формування зв'язки конкретного типу порушника ІБ з чіткими параметрами, що необхідні для його ідентифікації, використовуються l блоків зв'язки порушника з чіткими параметрами БЗПЧП$_\mathrm{k}$$(\mathrm{k} = \overline{1,l})$. Наприклад при n=6 і m=7 в k-ому вузлі з ідентифікаторами порушника I_1^k, I_2^k, I_3^k, I_4^k, I_5^k і I_6^k відповідно створюються зв'язки з чіткими параметрами $SP_{n_1}^k = SP_{n_2}^k = SP_{n_3}^k = SP_{n_4}^k = SP_{n_5}^k = SP_{n_6}^k = ($ SP_1^k, SP_2^k, SP_3^k, SP_5^k, SP_6^k, SP_7^k), тобто $\mathrm{D}^k = S^k = C^k = H^k = SB^k = B^k \to \{UID^k,\ AtEF^k,\ U\,\mathrm{Pr}^k,\ TrFin^k,\ ModF^k,\ TrFout^k,\ KS^k\}$. Організація БЗПЧП така ж сама як і в БЗПП. Слід зазначити, що оскільки всі чіткі параметри притаманні кожному типу порушника, то його ідентифікація здійснюється по значенню цих параметрів на основі чітких евристичних правил ESR_i $(\mathrm{i} = \overline{1,n})$.

По закінченню процедури формування зв'язок $I_i^k \to SP_{n_i}^k$ в БЗПЧП$_\mathrm{k}$$(\mathrm{k} = \overline{1,l})$ за допомогою модулів фазифікації МФ$_\mathrm{k}$$(\mathrm{k} = \overline{1,l})$ визначаються поточні значення чітких параметрів SP_i^k на момент запуску ППОЧП, які передаються з кожного вузла системи на відповідні кожному параметру модулі логічної арифметики (МЛА). В МЛА відбувається обробка чітких параметрів і обчислюється їх результуюче (сумарне) значення $\sum SP_i^k$ для всієї ІКС. Обчислення в МЛА відбувається за правилами звичайної логіки. Якщо значення чіткого параметру хоча б на одному з вузлів дорівнює 1, то сумарне значення також рівне 1. Якщо процес виявлення порушника ІБ здійснюється тільки на одному вузлі ІКС, то МЛА, за аналогією з МНА, в системі лише один і є повністю прозорим, тобто жодних логіко-арифметичних операцій на ньому не виконується і не створюються сумарні значення змінних.

Отримані дані в МФК формуються в кортеж $< \sum SP_i >$. На основі сформованого кортежу з використанням ініційованих в ПФЕЧП множини правил ESR_i $(\mathrm{i} = \overline{1,n})$ відповідних певному типу I_i^k в МЛВ виконується ідентифікація типу можливого порушника. Отриманий результат може відображатися в лінгвістичній формі через МЛВ та МВ.

Висновки

У роботі запропоновано нове структурне рішення, на основі якого можна розробляти алгоритмічне, програмне і програмно-апаратне забезпечення, що застосовується для виявлення та ідентифікації типу порушника інформаційної безпеки в ІКС. Робота описаної СВІП проходить в 2 етапи, на кожному з яких система працює з нечіткими та чіткими параметрами, за якими здійснюється ідентифікація порушника. Основне завдання СВІП на першому етапі виявити факт порушення і за можливості провести попередню ідентифікацію зловмисника, другий етап є контрольним та уточнюючим з точки зору ідентифікації порушника. Запропонована СВІП може використовуватись автономно або як складова комплексної системи захисту інформації.

У подальших роботах буде детально описано метод виявлення та ідентифікації порушника, на основі якого і працює запропонована СВІП.

Література

[1] Корченко О.Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / О. Г. Корченко. — К. : МК-Пресс, 2006. — 320 с.

[2] Гізун А.І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк // Захист інформації. — 2013. — №1 (58). — С.66-75.

[3] Волянська В.В. Моделі еталонів лінгвіст-тичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки// В.В. Волянська, А.І. Гізун, В.О. Гнатюк / Безпека інформації. — №1 (19). — 2013. — С. 13-21.

[4] Корченко А.О. Евристичні правила на основі логіко-лінвистичних зв'язок для виявлення та

ідентифікації порушника інформаційної безпеки / А.О. Корченко, А.І. Гізун, В.В. Волянська, О.В. Гавриленко // Захист інформації. – 2013. — №3 (60). — С. 251-257.

[5] Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. — №2 (18). — 2012. — С. 80-84.

УДК 004.056.53 (045)

Корченко А.А., Волянская В.В., Гизун А.И. Система обнаружения и идентификации нарушителя в информационно-коммуникационных сетях

Аннотация. *Эффективное обнаружение нарушителя информационной безопасности в информационно-коммуникационных сетях и системах является сложной задачей, требующей использования специальных средств защиты – систем обнаружения нарушителя. Большинство таких систем основываются на применения сигнатурных методов и имеют ряд недостатков, среди которых требовательность к ресурсам и расходы различного характера, например, связанные с выборкой статистических данных, обучением систем, их адаптацией и др. Более эффективны в этом отношении экспертные подходы, основанные на использовании знаний и опыта специалистов соответствующей предметной области. В работе предложено структурное решение системы обнаружения и идентификации нарушителя на нечеткой логике. Система состоит из подсистем первичной обработки четких и нечетких параметров, формирования нечетких эталонов и эвристических правил (соответственно по нечетким и четким контролируемым параметрам), а также модулей формирования кортежа, лингвистического вывода и визуализации, которые позволяют обнаружить и идентифицировать нарушителя. Результат работы системы представляется в лингвистической и графических формах.*

Ключевые слова: *нарушитель информационной безопасности, идентификация нарушителя, системы обнаружения вторжений, системы обнаружения нарушителя, нечеткая логика, безопасность информационно-коммуникационных систем и сетей, эвристические правила.*

Korchenko A.O., Volyanska V.V., Gizun A.I. System of intruder detection and identification in information & communication networks

Abstract. *Efficient detection of information security intruder in information and communication networks and systems is a complex task that requires the use of special security means – intruder detection systems. Most of these systems are based on the use of signature methods and have several disadvantages, including the demands on resources and costs of various kinds (e.g., sampling statistics, systems studying, their adaptation and others). Expert approaches based on the use of knowledge and experience of specialists in some sector are more effective in this viewpoint. The paper presents a structural solution of intruder detection and identification system based on fuzzy logic. The system consists of preprocessing subsystem for clear and fuzzy parameters forming, fuzzy standards and heuristic rules forming (according to fuzzy and clear controlled parameters) and modules of cortege forming, linguistic output and visualization that can detect and identify the intruder. The result of the system work is represented in linguistic and graphical forms.*

Key words: *information security intruder, intruder identification, intrusion detection systems, intruder detection systems, fuzzy logic, security of information and communication systems & networks, heuristic rules.*

Отримано *10 вересня 2013 року*, затверджено редколегією *27 вересня 2013 року*