

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

ІНФОРМАЦІЙНА БЕЗПЕКА

Науковий журнал
№ 4 (12) 2013

Луганськ 2013

**Інформаційна
безпека**
СХІДНОУКРАЇНСЬКИЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
№ 4(12) 2013

НАУКОВИЙ ЖУРНАЛ
ЗАСНОВАНО У 2009 РОЦІ
ВИХІД З ДРУКУ – ЧОТИРИ РАЗИ НА РІК

ЗАСНОВНИК

**Східноукраїнський національний уні-
верситет імені Володимира Даля**

Журнал зареєстровано Міністерством
юстиції України

Свідцтво про державну реєстрацію
серія **KB №15063-3635P**

Редакційна колегія:

Головний редактор – проф., д.т.н. О.С. Петров (м. Луганськ)
Заступник головного редактора – проф., д.т.н. В.О. Хорошко (м. Київ)
Відповідальний секретар – доц., к.т.н. А.О. Петров (м. Луганськ)

Члени редакційної колегії:

проф., д.ф.-м.н. Ю.М. Арлінський (м. Луганськ), проф., д.т.н. Архіпов О. С. (м. Київ), проф., д.т.н. О.Л. Голубенко (м. Луганськ), проф., д.ф.-м.н. М.М. Дівізінюк (м. Севастополь), проф., д.т.н. В.Б. Дудикевич (м. Львів), проф., д.т.н. В.В. Дядичев (м. Луганськ), проф., д.т.н. Івашук Н.Л. (м. Краків, Польща), проф., д.т.н. М.П. Карпінський (м. Белсько-Бяла, Польща), проф., д.т.н. А.А. Кобозева (м. Одеса), проф., д.т.н. В.В. Козловський (м. Київ), проф., д.т.н. О.Г. Корченко (м. Київ), проф., д.ю.н. В.С. Кузьмічов (м. Київ), проф., д.т.н. С.В. Ленков (м. Київ), проф., д.т.н. І. І. Маракоча (м. Брест, Франція), проф., д.т.н. Д.М. Марченко (м. Луганськ), проф., д.т.н. О.С. Меньяйленко (м. Луганськ), проф., д.т.н. В.В. Поповський (м. Харків), проф., д.т.н. С.К. Рамазанов (м. Луганськ), проф., д.т.н. М.Ф. Смирний (м. Луганськ), проф., д.т.н. О.О. Скопа (м. Одеса), проф., д.т.н. В.О. Ульшин (м. Луганськ), проф., д.т.н. О.О. Шумейко (м. Дніпродзержинськ), проф., д.ю.н. М.Є. Шумило (м. Київ), проф., д.т.н. Л.М. Щербак (м. Київ), проф., д.т.н. О.К. Юдін (м. Київ).

Відповідальний за випуск: проф., д.т.н. О.С. Петров.

До журналу увійшли статті студентів, аспірантів і докторантів Східноукраїнського національного університету імені Володимира Даля, вищих навчальних закладів України, Росії та закордонних країн.

Журнал підготовлено кафедрою безпеки інформаційних систем СХУ ім. В. Даля.

Рекомендовано до друку Вченою радою Східноукраїнського національного університету імені Володимира Даля (протокол № 4 від 24.12.2013 р.)

Занесений до «Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук» з *технічних наук*, затверджений постановою президії ВАК України від 14.05.2010 р., № 1-05/3.

Матеріали номера друкуються мовою оригіналу.

© Східноукраїнський національний університет імені Володимира Даля, 2013
© Volodymyr Dahl East-Ukrainian National University, 2013

**Information
security**
VOLODYMYR DAHL EAST
UKRAINIAN NATIONAL
UNIVERSITY
№ 4(12) 2013

THE FIRST ISSUE OF THE JOURNAL
WAS PUBLISHED IN 2009
THE JOURNAL IS PUBLISHED
QUARTERLY
FOUNDER

**Volodymyr Dahl East Ukrainian
National University**

REGISTERED by the Ministry
of Justice of Ukraine
registration **certificate**
KB №15063-3635P
ISSN 2224-9613

ЗМІСТ CONTENTS

Н.Н. Вишневська	АНАЛІЗ МЕТОДІВ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОГО ПРОСТОРУ	5
М.В. Демчишин	ГРАФІЧНИЙ ПОШУК ОПТИМАЛЬНОГО РОЗПОДІЛУ РЕСУРСІВ В УМОВАХ РІЗНОНАПРАВЛЕНОГО ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ	8
В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець, Р.І. Банах	КОМПЛЕКСНИЙ ПІДХІД ДО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В ТЕХНОЛОГІЯХ БЕЗПРОВІДНОГО ЗВ'ЯЗКУ	16
Ж.Ю. Зеленцова, Н.Ф. Казакова	КОНВЕРГЕНЦИЯ ГЛОБАЛЬНОЙ СЕТИ КАК НОВЫЙ ЭТАП РАЗВИТИЯ: ОБЗОР ИНФРАСТРУКТУРНЫХ РЕШЕНИЙ И ТЕХНОЛОГИЙ С ЦЕЛЬЮ НАХОЖДЕНИЯ РЕШЕНИЙ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ДАННЫХ ПРИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ	23
Л.Ф. Єжова, Л.М. Скачек	ЗАСТОСУВАННЯ ТЕОРІЇ ГРАФІВ ЩОДО ОПИСУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ	41
Н.Ф. Казакова, Є.В. Вавілов	АВТОМАТИЗАЦІЯ ПРОЦЕСУ АДАПТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ ДО ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	49
І.В. Пампуха, О.І. Адаськов, Л.В. Охромович	РЕКОМЕНДАЦІЇ ЩОДО ПРОВЕДЕННЯ ІНФОРМАЦІЙНИХ ЗАХОДІВ В МЕРЕЖІ ІНТЕРНЕТ В ІНТЕРЕСАХ ВИКОНАННЯ ЗАВДАНЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ	57
О.С. Ленков, А.С. Шворов, В.М. Штепа, Ю.О. Царьов	ПРИНЦИПИ СИНТЕЗУ ЕКСПЕРТНОЇ СИСТЕМИ ОЦІНКИ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ НЕЧІТКОЇ НЕЙРОННОЇ МЕРЕЖІ	69
І.Л. Лозова, Ю.П. Бойко	МЕТОД ОЦІНКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ З УРАХУВАННЯМ СУМІЩЕННЯ ОБМІНУ І ОБЧИСЛЕНЬ	75
М.М. Мандрона, В.М. Максимович, Ю.Ю. Рибак, Ю.М. Костів, О.І. Гарасимчук	ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ПОБУДОВАНИХ З ВИКОРИСТАННЯМ R-БЛОКІВ	84
А.В. Міщенко	ФАКТОРИ ЕКОНОМІЧНОЇ БЕЗПЕКИ СИСТЕМИ ЕКОНОМІКИ АВІАТРАНСПОРТНОГО КОМПЛЕКСУ КРАЇНИ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ	93
А.О. Петров	ЗАХИЩЕНА ТЕХНОЛОГІЯ ВЕРИФІКАЦІЇ БІОМЕТРИЧНИХ ДАНИХ У СИСТЕМАХ ДОСТУПУ	97
Д.М. Самойленко	МОДЕЛЬ ЗАХИЩЕНОГО ІНФОРМАЦІЙНОГО РЕСУРСУ З ОБМАННИМИ ФУНКЦІЯМИ	107

О.О. Фразе-Фразенко	МЕТОД АНІЗОТРОПНОЇ ФІЛЬТРАЦІЇ НЕСТАБІЛЬНИХ ЗОБРАЖЕНЬ У СИСТЕМАХ ДОСТУПУ З БІОМЕТРИЧНОЮ АУТЕНТИФІКАЦІЄЮ	112
Е.В. Иванченко, В.А. Хорошко, Е.П. Сластенко	СИНТЕЗ СТРУКТУРНО-ОПТИМАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ СЛОЖНЫМИ ОБЪЕКТАМИ	126
В.А. Хорошко, Ю.Е. Хохлачова, Е.П. Сластенко	СИНТЕЗ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ, ИМЕЮЩИХ ДОПУСКОВЫЙ РАЗБРОС ПАРАМЕТРОВ	130
О.Р. Чертов, Д.Ю. Тавров	МЕТЕТИЧНИЙ АЛГОРИТМ ІЗ НЕЧІТКИМИ ОБМЕЖЕННЯМИ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ГРУПОВОЇ АНОНІМНОСТІ	135
А.А. Шиян	УЗГОДЖЕНА СИСТЕМА ІНФОРМАЦІЙНО- АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВИ В УКРАЇНІ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	145
Ю.С. Яремчук	ЗАХИЩЕНА ВЕБ-СИСТЕМА ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ АСИМЕТРИЧНИХ РИПТОГРАФІЧНИХ ТЕХНОЛОГІЙ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ	152

Н.Ф. Казакова¹, Є.В. Вавілов²

¹к.т.н., доцент, кафедра інформаційних систем в економіці, Одеський державний економічний університет (м. Одеса)

²аспірант, Одеський національний університет ім. І.І. Мечникова

АВТОМАТИЗАЦІЯ ПРОЦЕСУ АДАПТАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ ДО ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розглядається спосіб здійснення моніторингу та аудиту безпеки інформаційних систем з метою встановлення та автоматичної ліквідації виявлених інцидентів інформаційної безпеки. Спосіб дозволяє спростити розв'язок завдання адміністрування інформаційної безпеки та процедури контролю за системними конфігураційними параметрами безпеки, систематизувати реакції на порушення безпеки та автоматично синтезувати відповідні управлячі рішення.

Ключові слова: інформаційна безпека, автоматизована інформаційна система, інцидент, інформаційний вплив, управляюче рішення, адміністрування.

Поста новка проблеми у загальному вигляді та її зв'язок із важливими науковими та практичними завданнями

Автоматизована інформаційна система (АІС) – це система, що складається з персоналу та комплексу засобів автоматизації її діяльності, які реалізують інформаційну технологію (ІТ) виконання встановлених функцій [1]. Враховуючи різноманітність сучасних засобів автоматизації, особливий інтерес представляють питання моніторингу ризиків в гетерогенних (різноманітних) АІС.

Обслуговування будь-якої АІС пов'язане з рішенням такого завдання, як результативно та ефективно використання механізмів захисту на всіх рівнях системної архітектури. При цьому задіяються компоненти, орієнтовані на забезпечення надійності її роботи, живучості, безпеки зберігання та обробки інформації, що дозволяє експлуатувати систему при побудові захищених інфраструктур, що забезпечують необхідний рівень безпеки інформації при збереженні сумісності з існуючими ІТ [2...5]. Втім, багаторівність, багатокомпонентність, складність взаємозв'язків структурних складових АІС обумовлюють інерційність механізмів захисту, що не дозволяє динамічно протистояти порушенням безпеки та забезпечити своєчасний захист інформації (ЗІ) [6, 7]. Рішення проблеми вимагає застосування специфічних технологій управління інформаційною безпекою (ІБ). При цьому дії по управлінню великими системами вимагають безперервних оцінок безпеки, виявлення її порушень, синтез керуючих впливів на механізми ІБ з метою ліквідації порушень [8]. В силу обмеженості людських можливостей це виконується не завжди адекватно, оперативно та результативно. Цей факт підтверджується статистикою кіберзлочинів [9].

Згідно з сучасними уявленнями, аудит та оцінка ризиків виконуються в ході моніторингу ІБ автоматизованими системами [10]. Основним завданням моніторингу ІБ є оцінка внутрішніх механізмів контролю ІТ та їх ефективності, а також архітектури АІС в цілому. Моніторинг ІБ включає в себе багато завдань, у тому числі оцінку ефективності

системи обробки інформації, оцінку безпеки використовуваних протоколів і технологій, процесу розробки та управління. Стратегічною метою моніторингу ІБ є забезпечення доступності інформації в інформаційній системі (ІС), цілісності інформації і, при необхідності, конфіденційності інформації. Деталізація цієї мети при моніторингу конкретних ІС призводить до необхідності отримання відповідей на ряд важливих питань: чи доступна інформація в системі в кожен момент здійснення бізнес-процесів; чи забезпечене розмежування доступу до інформації відповідно до встановлених повноважень користувачів; чи забезпечена точність, достовірність і своєчасність інформації в системі? Відповіді на ці та ряд інших важливих питань при моніторингу ІБ можуть бути отримані як результат роботи з оцінки параметрів якості комплексної системи забезпечення ІБ, тобто моніторингу, аналізу та оцінки ризиків ІБ [11].

Формулювання цілей статті та постановка завдання

Зважаючи на викладене, можна вважати, що існує необхідність у синтезі способу управління інформаційною безпекою, який дозволив би не тільки впорядкувати процеси моніторингу та адміністрування безпеки ІС, але й автоматизувати адаптивну реакцію механізмів їх безпеки на негативні інформаційні впливи, які в них можуть виникати. *Метою статті* є синтез способу автоматизації процесу адаптації ІС до інцидентів ІБ.

Аналіз досліджень і публікацій

Останнім часом питання реагування на інциденти ІБ достатньо широко обговорюються у науковому співтоваристві. Так, у роботах Б.М. Герасимова та П.В. Хусаїнова розглядаються шляхи вирішення питань щодо інформаційної підтримки виявлення інцидентів ІБ при централізованій обробці подій. Ними освітлена актуальна науково-практична задача підвищення ефективності роботи оператора системи централізованої обробки подій, тобто адміністратора ІБ, в процесі управління інцидентами і підхід до її вирішення за рахунок інформаційної підтримки оператора. Як видно, відповідальність за вироблення рішень покладається на людину, що, як зазначалося, не є досить оперативним та результативним процесом. О.М. Атаманов у своїх роботах вирішує завдання синтезу системи динамічної ітеративної оцінки ризиків ІБ з врахуванням зазначеного вище недоліку. Так, ним синтезовано методику, яка дозволяє динамічно класифікувати значення спостережуваних параметрів АІС на групи ризику і, на цій основі, проводити оцінку апостеріорної ймовірності реалізації загроз ІБ на підставі даних спостережень з урахуванням виконаного розбиття.

Дослідження в галузі моніторингу та аналізу ризиків ІБ проводилися також й іншими вченими, серед яких можна виділити Г.А. Остапенка, Д.А. Котенка, І.Л. Алфьорова, О.Г. Кашенка, М.В. Тимоніна, Я.М. Алгулієва, О.Н. Назарова, Д.О. Карпєєва, А.О. Сидорова, О.Г. Лисенка, О.В. Львова, Г.А. Кустова, В.О. Хорошко, О.С. та А.О. Петрових, О.Г. Корченка, О.С. Маркова, Г.Ф. Конаховича, О.К. Юдіна, О.О. Скопу, Т.Р. Peltier, С. Kairab, С. Alberts, G. Brjndeland, A. Papoulis, N.E. Fenton, M. Neil, M. Taylor, F.V. Jensen та ін. Аналіз багатьох опублікованих ними робіт показує, що відкритими залишаються питання оцінки ймовірності реалізації загроз в умовах нестачі статистичних даних та питання використання суперечливих даних, які тісно пов'язані з автоматизацією процесу отримання кількісної оцінки ризику ІБ в реальному часі.

Щодо практичної реалізації методів автоматизації процесів адаптації АІС до інцидентів ІБ, то у відкритому друці їх, на жаль, описано надзвичайно мало. Так, відомі системи та способи, в основному, засновані на використанні зворотного зв'язку для класифікації елементів впливів на ІБ з метою запобігання несанкціонованого розсилання електронної пошти. Вони базуються на принципах навчання у межах виборки електронних листів, що генеруються за випадковою схемою, яка імітує найбільш типові приклади поштових розсилок [12]. Проте таке рішення не забезпечує достатню об'єктивність оцінки при класифікації елементів саме у силу випадковості навчальної вибірки. Крім того, зазначений підхід є лише окремим випадком застосування зворотного зв'язку до

вирішення задачі класифікації та не надає загального підходу до управління ІБ на рівні ІС і створенню автоматичного управління безпекою ІС.

Відомі також теоретичні способи синтезу та аналізу систем управління ІБ (наприклад, [13]). Однак розв'язки, які пропонуються, спрямовані на побудову лише загальних математичних моделей систем моніторингу та управління ІБ та на моделювання процесів, які в них відбуваються. При цьому практичні особливості забезпечення ІБ в ІС в них не розглядаються.

Найбільш відомим розв'язком щодо моніторингу та управління ІБ є [14]. Документ описує безперервність забезпечення ІБ на основі організації процесного підходу, який включає етапи створення, впровадження, експлуатації, постійного контролю, аналізу, підтримки в робочому стані та поліпшення систем захисту інформації (СЗІ). Однак у зазначеному джерелі регулюється лише циклічність процесу моніторингу та управління та регламентується необхідність оцінки та адаптації СЗІ на рівні організації та не пропонується ніяких реалізацій для обслуговування ІС.

Сказане підтверджує основні уявлення більшості вчених про те, що існуючі методики погано адаптуються до змін, які вносяться в АІС, так як у випадку виникнення таких змін потрібне повторення всіх етапів процедури моніторингу системи.

Виклад основного матеріалу

В основу синтезу способу автоматизації процесу адаптації ІС до інцидентів ІБ покладемо матеріали [12, 15...18]. Згідно до зазначених джерел, спосіб може базуватися на адаптивному параметричному управлінні безпекою ІС, в основі технічної реалізації якого лежить система, яка передбачає використання інформації про поточну конфігурацію системи безпеки. Як вже зазначалося в огляді першоджерел, її основним схемотехнічним рішенням є система зі зворотним зв'язком про інциденти ІБ. Спосіб повинен включати процедури моніторингу з метою отримання оцінки конфігурації АІС, а також можливості адаптації конфігураційних параметрів її СЗІ до порушень, які можуть виникнути в процесі експлуатації. Адаптація повинна відбуватися за рахунок автоматизації процедур фіксації конфігурації СЗІ АІС, оцінки її безпеки та надання керуючих впливів на конфігураційні параметри безпеки. Це дозволить спростити процес управління ІБ, а при автономних реалізаціях та впровадженні системи управління ІБ до складу таких ІС – повністю автоматизувати процес адаптації ІС до інцидентів безпеки. Т.ч. можуть бути створені захищені АІС, які володіють властивостями самоадаптації, що приведе до скорочення експлуатаційних витрат на обслуговування ІС та їх відновлення після інцидентів ІБ, забезпечить безперервність та гарантованість безпеки, а також поліпшить керуваність та ефективність забезпечення безпеки ІС в цілому.

Покладемо, що розв'язок поставленого завдання може бути забезпечено тим, що при синтезі способу, функціональні завдання якого приведені вище, необхідно задати умови для безпеки конфігурації ІС. Для кожної умови необхідно зазначити відповідний ступінь критичності її порушення, перераховуючи при цьому ознаки безпечної конфігурації, тобто вказуючи безпечні по складу та значеннях множини суб'єктів, об'єктів, їх атрибутів безпеки та ін., наявність яких свідчить про безпеку ІС. Також слід визначити шкалу ступенів критичності порушень для створених умов ІБ, ранжируючи умови безпеки по зазначеній шкалі [19, 20]. Необхідним є задання для кожної умови ІБ ступеню критичності порушення, а по шкалі ступенів критичності – визначення границі критичності між критичними та некритичними порушеннями ІБ. Вважатимемо викладене початковим етапом синтезу методу, який розглядається.

Після цього, згідно [15], необхідно визначити загальну функцію порушення ІБ, яка буде індикатором порушення заданих умов безпеки конфігурації. Вона може бути представлена у вигляді логічного виразу або функції, заданої у полі функцій порушень умов ІБ згідно з раніше введеними ступенями критичності порушень. За цим фіксується факт впливу на поточну конфігурацію безпеки ІС при здійсненні доступу суб'єкта до

об'єкта. Також фіксується поточна конфігурація безпеки ІС, включаючи множини суб'єктів, об'єктів, їх атрибутів безпеки за складом та значеннями.

Наступний етап – оцінка виконання умов безпеки конфігурації системи. При цьому обчислюється логічне значення загальної функції інциденту з порушення безпеки та по ньому визначається наявність порушення умов безпеки конфігурації. Крім того, встановлюється, чи є необхідність виконання тих чи інших дій щодо впливу на ІС з метою її адаптації до даного порушення безпеки. У випадку, якщо порушення умов безпеки конфігурації не зафіксоване та адаптацію ІС виконувати не потрібно, то вище вказані дії повторюються, починаючи з моменту фіксації впливу на конфігурацію безпеки системи. У випадку, коли порушення умов безпеки конфігурації зафіксоване і, відповідно, необхідна адаптація ІС, то необхідно встановити, які умови безпеки конфігурації порушені. Це надасть можливості виробити керуючі впливи на конфігурацію безпеки з метою адаптації ІС до виявлених порушень. При цьому по кожній з умов, шляхом порівняння множин поточних та заданих в умовах безпеки суб'єктів, об'єктів та атрибутів безпеки, виявляють відсутні елементи цих множин та/або некоректно задані та/або відсутні значення конфігураційних параметрів безпеки. Далі по кожному з порушених умов безпеки конфігурації, призводять конфігурацію безпеки ІС у відповідності до встановлених умов, додаючи виявлені на попередньому етапі відсутні елементи та/або значення, та/або видаляючи надлишкові, та/або змінюючи некоректні. Всі дії періодично повторюють, починаючи з етапу фіксації елементу впливу на конфігурацію безпеки системи.

Рішення щодо технічної реалізації завдання, яке вище розглянуто, пропонується в [15]. Взявши його за основу технічної системи адаптивного параметричного управління безпекою ІС, встановимо, що вона може включати модулі, які виконують наступні функції (див. далі рис. 1 та рис. 2): фіксацію конфігурації безпеки; опис умов безпеки; оцінку виконання умов безпеки; фіксацію впливу з одночасним відслідковуванням факту здійснення доступу суб'єкта до об'єкта. Останній з заначених модулів повинен бути пов'язаний з модулем фіксації конфігурації безпеки у який він передає сигнал про те, що відбувся вплив на конфігурацію безпеки. У модулі фіксації конфігурації безпеки, який спрацьовує при надходженні сигналу про вплив від модуля фіксації впливу, повинен бути додатково передбачений збір повної інформації про поточну конфігурацію безпеки ІС. У модулі опису умов безпеки, призначеному для зберігання ознак безпечної конфігурації, необхідно додатково передбачити функції визначення шкали ступенів критичності порушень для створених умов безпеки конфігурації, а також їх ранжирування по обраній шкалі. Тут же повинно проводитися визначення межі між критичними та некритичними порушеннями безпеки та синтез загальної функції порушення безпеки, яка є індикатором порушення умов безпеки конфігурації для заданого набору умов. Модуль оцінки виконання умов безпеки сполучується з модулем фіксації конфігурації безпеки та модулем опису умов безпеки. Він призначений для оцінки виконання умов безпеки конфігурації системи на основі зафіксованих конфігураційних параметрів безпеки та умов безпеки конфігурації ІС шляхом обчислення логічного значення загальної функції порушення безпеки. Якщо така загальна функція прийме дійсне значення, то відбудеться включення модуля управління безпекою. Модуль оцінки виконання умов безпеки виконує зазначену оцінку шляхом обчислення логічного значення загальної функції порушення безпеки і, якщо вона приймає дійсне значення, то ініціює роботу пов'язаного з ним модуля управління безпекою. Після цього виконується основна дія: модуль управління безпекою, пов'язаний з модулем оцінки виконання умов безпеки, виконує здійснює адаптацію ІС шляхом вироблення керуючого впливу на її конфігурацію безпеки.

У якості конфігурації безпеки ІС, як правило, використовуються множини суб'єктів, об'єктів доступу та їх атрибутів безпеки. Їх склад та значення визначаються типом операційного середовища ІС. У загальному випадку конфігурація безпеки визначається такими конфігураційними параметрами: користувачі та групи користувачів; елементи файлової системи (диски, каталоги, файли, посилання); елементи реєстру (роз-

діли, ключі, параметри, посилання); об'єкти ядра (завдання, процеси, потоки, драйвери, об'єкти синхронізації і т.д.); ресурси загального доступу (каталоги, принтери); програмні сервіси; COM/Dcom-Об'єкти; об'єкти служб каталогів; локальні та глобальні налаштування системної політики безпеки; опції та налаштування безпеки користувацького та спеціального програмного забезпечення; конфігураційні параметри мережних служб; атрибути безпеки суб'єктів та об'єктів доступу, у т.ч. ідентифікатори захисту, привілеї користувачів і груп користувачів, власники об'єктів, списки прав доступу, мітки доступу та цілісності, ієрархічний розподіл суб'єктів, об'єктів, прав доступу, міток доступу та цілісності.

Вище описане, для ілюстрації, пояснюється за допомогою рис. 1 [15]. На ньому представлена загальна схема функціонування. На рис. 2 приведена модульна схема системи на основі якої можлива реалізація розглянутого способу [15].

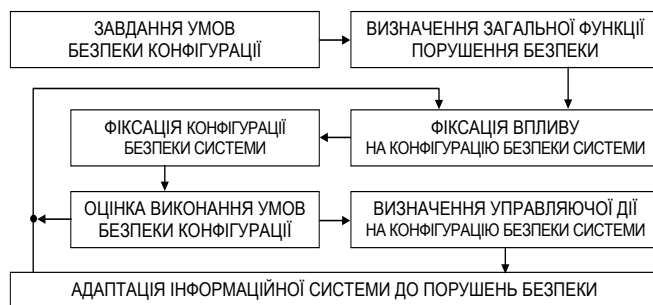


Рис. 1. Загальна схема функціонування способу автоматизації процесу адаптації інформаційних систем до інцидентів інформаційної безпеки

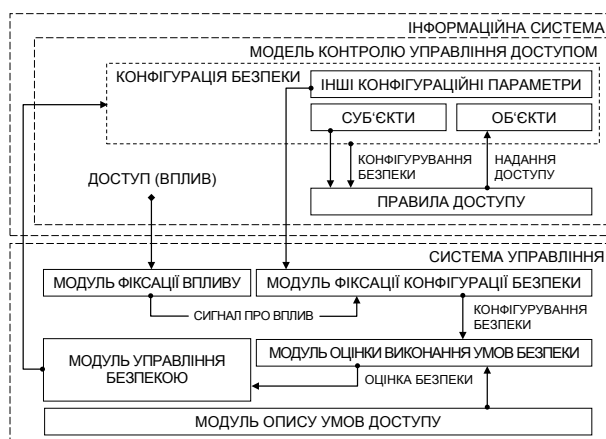


Рис. 2. Модульна схема системи на основі якої можлива реалізація способу автоматизації процесу адаптації інформаційних систем до інцидентів інформаційної безпеки

Як правило, управління безпекою здійснюється людиною-адміністратором. Процес носить назву «адміністрування безпеки». У ході обслуговування ІС адміністратор має за основу тезу про те, що до ІС можна отримати несанкціонований доступ шляхом різних проникнень. У такому випадку для забезпечення ІБ в ІС ним постійно ведеться моніторинг системи з метою пошуку та усунення недоліків і помилок конфігурування безпеки. Спосіб, який розглядається, є альтернативою такому рутинному підходу. Як

видно, він у своїй основі забезпечує безпеку ІС та проходить динамічно відповідно до необхідних умов безпеки в автоматизованому режимі.

Приведемо пояснення окремих використаних термінів.

Під поняттям «умова безпеки» розуміється логічний критерій, виконання якого свідчить про інформаційну безпеку АІС або будь-якої іншої ІС. Така умова вимагає попереднього завдання. Воно повинне враховувати правила контролю та управління доступом, які реалізовані у моделі безпеки. Так, для операційних систем (ОС) Windows умови безпеки задані розробником ОС та представлені у вигляді шаблонів безпеки, які є стандартом для неї. Для ОС UNIX норми визначаються на основі відкритого алгоритму роботи механізму контролю та управління доступом.

Розглянемо процедуру синтезу керуючого впливу на множину конфігураційних параметрів безпеки з врахуванням умов безпеки.

Люба система має початкову конфігурацію безпеки S . Згідно [15], вважатимемо її безпечною. Можливо, що у деякий наступний момент часу система може змінити конфігурацію на S' . Нову конфігурацію необхідно оцінити згідно до умов безпеки та при необхідності адаптувати її до виявлених порушень безпеки. Для цього для кожної умови безпечної конфігурації необхідно визначити логічну функцію порушення C_i , $i \in Z$, а також відповідний ступінь критичності її порушення в контексті безпеки. Функція C_i приймає значення «істина», якщо відповідна умова безпеки не виконується в даній конфігурації безпеки ІС. Набір таких функцій складає множину C функцій порушень умов безпеки.

Загальна функція порушення, яка ініціалізує порушення умов безпеки для множини C у системній конфігурації S' , як зазначалося вище, представляється у вигляді логічної функції, що задається в базисі ТА-АБО. Така функція повинна бути такою, яка визначається на множині C . Запис функції має вигляд: $F(C) = C_1 \vee C_2 \vee \dots \vee (C_i \wedge C_j \wedge \dots \wedge C_N)$, де i, j та $N \in Z$. Як видно, вона складається з кількох логічних доданків, об'єднаних операцією логічного додавання, і логічних множників, об'єднаних операцією логічного множення. Сам вид функції погоджений зі ступенем критичності порушення, який введений раніше. Це означає, що ті некритичні умови, які все ж таки володіють деяким ступенем критичності, але який є меншим, ніж задана границя критичності по шкалі ступенів критичності, поєднуються логічним множенням, що означає спрацьовування загальної функції порушення безпеки при одночасному порушенні цих умов. Т.ч., для появи повідомлення про порушення безпеки буде достатньо порушення як однієї з критичних умов, так і одночасного порушення кількох або всіх некритичних умов.

Якщо буде виявлено, що загальна функція порушення набула дійсного значення, то система перейде у стан аналізу та пошуку порушеної умови або групи умов і пов'язаних з ними конфігураційних параметрів. Після локалізації порушень синтезуються та здійснюються управляючі впливи на конфігурацію безпеки ІС для переведення її в безпечний стан, який задовольняє встановленим умовам безпеки.

Висновки

Розглянутий спосіб та система на основі якої можлива його технічна реалізація, по багатьом параметрам перевершують можливості існуючих рішень по контролю безпеки АІС, які здійснюють моніторинг або аудит безпеки та сканування уразливостей, і проводять при цьому прямий перебір фіксованої множини контрольованих характеристик не виконуючи при цьому ніяких управляючих впливів на конфігураційні параметри безпеки ІС з метою ліквідації виявлених порушень. Відповідно, розглянутий спосіб параметричного адаптивного управління безпекою дозволяє спростити розв'язок завдання автоматизації адміністрування ІС та процедури контролю за системними конфігураційни-

ми параметрами безпеки, систематизувати реакції на порушення безпеки, що надає можливості автоматизації виконання операцій по оцінці безпеки системної конфігурації та надання своєчасних впливів в ІС з метою запобігання порушень безпеки.

Література

1. Скопа, О. О. Інтелектуальні автономні системи: концептуальні положення створення та функціонування [Текст] / О. О. Скопа, Є. В. Вавілов // Бионика интеллекта. – 2013. – № 1(80). – С. 35-40. – ISSN 0555-2656.
2. Грабовський, О. В. Скорочення випробувань надійності ІВС за рахунок її функціональної надмірності [Текст] / О. В. Грабовський, Н. Ф. Казакова // Технологічний аудит та резерви виробництва. – 2013. – №2/1(10). – С. 24-27. – ISSN 2226-3780.
3. Казакова, Н. Ф. Методи оцінки надійності систем телекомунікацій з резервом [Текст] / Н. Ф. Казакова // Праці УНДІРТ. – 2003. – №. 2. – С. 34. – ISSN 1562-2541.
4. Казакова, Н. Ф. Надійність функціонування морських супутникових систем телекомунікацій [Текст] / Н. Ф. Казакова // Збірник наукових праць Українського державного морського технічного університету. – 2002. – № 7(385). – С.109-115. – ISSN відсутній.
5. Панфилов, И. П. Надежность работы линии связи, состоящей из основного и резервного каналов [Текст] / И. П. Панфилов, А. А. Скопа // Радиотехника. – 2002. – № 128. – С.91-96. – ISSN 0485-8972.
6. Скопа, О. О. Обслуговування резервних систем зв'язку [Текст] / О. О. Скопа // Наукові праці ДонДТУ. Серія: Обчислювальна техніка та автоматизація. – 2002. – № 38. – С.89-91. – ISSN 2077-6780.
7. Грабовський, О. В. Візуалізація структури показників якості інформаційно-вимірювальних систем [Текст] / О. В. Грабовський, С. Л. Волков, О. О. Скопа // Метрологія та прилади. – 2013. – №2. – С. 69-74. – ISSN 2307-2180.
8. Скопа, О. О. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем [Текст] / О. О. Скопа, Н. Ф. Казакова // Системи обробки інформації : Безпека та захист інформації в інформаційних системах. – 2009. – № 7(79). – С.48-54. – ISSN відсутній.
9. Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15(204). – Ч.1. – С.59-62. – ISSN 1998-7927.
10. Казакова, Н. Ф. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки [Текст] / Н. Ф. Казакова, Е. А. Плешко, К. Б. Айвазова // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2013. – № 15(204). – Ч.1. – С.172-181. – ISSN 1998-7927.
11. Скопа, О. О. Безпека фінансового ринку та фінансової стабільності як суспільне благо [Текст] / О. О. Скопа, О. О. Йона // Вчені записки університету «КРОК». Серія: Економіка. – 2012. – № 32. – Т.1. – С.117-122. – ISSN відсутній.
12. Пат. № 2331913 (19) RU (11) 2 331 913 (13) C2 (51) МПК G06F 1/00 (2006.01). Контур обратной связи для предотвращения несанкционированной рассылки / Раунтвэйт Р. Л., Хекерман Д. Э., Мер Д. Д. [та ін.] ; заявник та патентообладач Майкрософт Корпорейшн. – RU 2331913 C2 ; заявл. 25.02.2004 ; опубл. 20.08.2008, Бюл. 23.
13. Ким Д. П. Теория автоматического управления. Т.1. Линейные системы. – М. : Физматлит, 2003. – 288 с. – ISBN 5-9221-0379-2, 5-9221-0534-5.
14. Стандарт ИСО/МЭК 27001: 2005. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования [Электронный ресурс] / Портал : Федеральное агентство по техническому регулированию и метрологии. – Режим доступа \www/ URL: expert.gost.ru/ID/DOC/27001.pdf. – Заголовок з контейнера, доступ вільний, 27.02.2014.
15. Пат. № 2331913 РФ, (19) RU (11) 2 399 091 (13) C2 (51) МПК G06F 21/00 (2006.01) G06F 12/14 (2006.01) H04L 9/32. Способ адаптивного параметрического управления безопасностью информационных систем и система для его осуществления / Зегжда Д. П., Зегжда П. Д., Калинин М. О. ; заявник та патентообладач ООО «НеоБИТ». – RU 2399091 C2 ; заявл. 27.11.2008 ; опубл. 10.09.2010, Бюл. 25.
16. Скопа, А. А. Политика предупреждения угроз информационной безопасности в практической деятельности Одесского филиала ОАО «Укртелеком» [Текст] / А. А. Скопа, Н. Ф. Ка-

- закова, С. Т. Сорока // Вісник Національного технічного університету «ХПІ». Тематичн. випуск: Нові рішення в сучасних технологіях. – 2012. – №17. – С.42-47. – ISSN 2224-0349.
17. Рубежанський, Ю. С. Использование политики предупреждения инцидентов в практической деятельности Центра обработки данных Одесского филиала ОАО «Укртелеком» [Текст] / Ю. С. Рубежанський, С. Т. Сорока, Н. Ф. Казакова // Наукові записки Міжнародного гуманітарного університету. – 2009. – № 16. – С.122-127. – ISSN 2307-1745/
 18. Казакова, Н. Ф. Алгоритм действий дежурного персонала при сбоях и событиях в системе информационной безопасности Одесского филиала ОАО «Укртелеком» [Текст] / Н. Ф. Казакова, С. Т. Сорока // Вісник УНДІЗ. – 2009. – №2. – С.14-15. – ISSN відсутній.
 19. Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (проміжн.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразенко, А. В. Мінін, О. О. Йона, Є. В. Вавілов, К. Б. Айвазова // ОНУ ; кер. О. О. Скопа. – 0112U007713. – Одеса, 2013. – 236 с.
 20. Грабовський, О. В. Розробка методу оцінювання якості інформаційно-вимірjuвальних систем на основі використання генетичних алгоритмів [Текст] : дис. ... канд. техн. наук / О. В. Грабовський. – Одеса, 2013. – 219 с.

Надійшла до редколегії 10.11.2013

Рецензент: проф., д.т.н. Дядичев В.В.

Н.Ф. Казакова, Е.В. Вавилов

АВТОМАТИЗАЦИЯ ПРОЦЕССА АДАПТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ К ИНЦИДЕНТАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматривается способ осуществления мониторинга и аудита безопасности информационных систем с целью установления и автоматической ликвидации выявленных инцидентов информационной безопасности. Способ позволяет упростить решение задачи администрирования информационной безопасности и процедуры контроля за системными конфигурационными параметрами безопасности, систематизировать реакции на нарушения безопасности и автоматически синтезировать соответствующие управляющие решения.

Ключевые слова: информационная безопасность, автоматизированная информационная система, инцидент, информационное воздействие, управляющее решение, администрирование

N.F. Kazakov, E.V. Vavilov

AUTOMATION OF THE PROCESS OF ADAPTATION OF INFORMATION SYSTEMS FOR INFORMATION SECURITY INCIDENTS

This article discusses a method of monitoring and auditing information systems security. The method allows you to set and automatically eliminate information security incidents. The method simplifies the administrative tasks of information security. The method simplifies the procedures for monitoring the system security configuration parameters. On the basis of this method is possible to conduct systematization reactions to security breaches. As a result, possible automatic synthesis of control decisions.

Keywords: information security, automated information system, incident information influence, control solution, administration

ІНФОРМАЦІЙНА БЕЗПЕКА

Східноукраїнський національний університет
імені Володимира Даля

Науковий журнал
№ 4 (12) 2013

Відповідальний секретар випуску
Технічний редактор
Оригінал-макет

*Петров О.С.
Кліпаков М.В.
Кліпаков М.В.*

Підписано до друку 21.10.2013.
Формат 70х108 ¹/₁₆. Папір офсетний.
Умов. друк. арк. 12,16. Обл.-вид. арк. 16,75.
Наклад 100 прим. Видавничий № 2946. Замовлення №1251. Ціна вільна

Видавництво
Східноукраїнського національного університету
імені Володимира Даля

Свідоцтво про реєстрацію: серія ДК № 1620 від 18.12.03 р.

Адреса видавництва: 91034, м. Луганськ, кв. Молодіжний, 20 а,
Телефон (0642) 41-34-12. Факс (0642) 41-13-60.
E-mail: izdat.snu@gmail.com, <http://publish.snu.edu.ua>.

Надруковано у видавництві «НОУЛІДЖ»
Свідоцтво про реєстрацію серія ДК №2884 від 26.06.2007
91051, м. Луганськ, кв. Якіра, 3/316,
тел. (050) 475-35-13, e-mail: nickvnu@gmail.com