МЕТОДИ ТА СИСТЕМИ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Анна Чунарьова, Андрій Чунарьов

Національний авіаційний університет

ЧУНАРЬОВА Анна Вадимівна, к.т.н.

Рік та місце народження: 1987 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: доцент кафедри комп'ютеризованих систем захисту інформації кафедри з 2012 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 55 наукових публікацій, серед яких наукові статті та патенти на корисні моделі.
E-mail: chunariova@gmail.com

ЧУНАРЬОВ Андрій Вадимович

Рік та місце народження: 1992 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет
Посада: студент кафедри комп'ютеризованих систем захисту інформації з 2009 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 38 наукових публікацій, серед наукові статті та патенти на корисні моделі.
E-mail: chunariov@ukr.net

Анотація. *У даній статті проведено аналіз сучасних методів та систем виявлення несанкціонованого доступу в сучасних інформаційно-комунікаційних системах та мережах. В результаті проведено аналізу виділені переваги та недоліки застосування існуючих методів та систем. Виділені найбільш ефективні з точки зору підвищення захисту інформації та забезпечення протидії загрозам, як навмисним та і випадковим.*

Ключові слова: *захист інформації, несанкціонований доступ, атака, інформаційно-комунікаційна система та мережа, уразливість.*

Сучасні інформаційно-комунікаційні системи та мережі передачі даних є основою розвитку інформаційного суспільства, а саме вони здійснюють зберігання, передачу й обробку інформації. Тому важливим атрибутом функціонування сучасних інформаційно-комунікаційних системах та мережах (ІКСМ) з умов забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів є здійснення процесів захисту інформації від несанкціонованого доступу (НСД). Під захистом інформаційного об'єкту розуміється регулярне використання засобів і методів, вживання заходів і здійснення заходів з метою забезпечення комплексної безпеки інформації з метою забезпечення базових властивостей інформаційних ресурсів. На сьогодні розгалужені інформаційні мережі функціонують під управлінням різних операційних систем, на перше місце виходить завдання управління всім різноманіттям захисних механізмів. Базовим підходом до вирішення цієї проблеми є використання **систем та методів виявлення НСД.** Застосування даних методів та систем унеможливить НСД та зловживання інформаційними ресурсами в сучасних ІКСМ.

Постановка задачі. Під поняття системи виявлення НСД будемо розуміти безліч різних програмних і апаратних засобів, що аналізують порядок використання інформаційних ресурсів, що захищають, і, у разі виявлення яких-небудь підозрілих або просто нетипових подій, здатні здійснювати певні самостійні дії з виявлення, ідентифікації і усунення причин, що їх викликали. Системи виявлення атак відрізняються принципом функціонування, методом виявлення несанкціонованої дії, реалізацією виявлення атаки в часі тощо. **Метою** даних досліджень є проведення аналізу методів та систем виявлення вторгнень на основі протидії несанкціонованому доступу в сучасних ІКСМ.

Класифікація методів виявлення НСД в ІКСМ. Всі методи виявлення НСД можна розділити на два класи: методи виявлення аномалій і методи виявлення зловживань. Методи першого класу базуються на наявності готового опису нормальної поведінки спостережуваних об'єктів, і будь-яке відхилення від нормальної поведінки вважається порушенням.

Методи виявлення НСД засновані на описі відомих порушень або атак: якщо спостережувана поведінка деякого об'єкту співпадає з описом відомої атаки, поведінка об'єкту вважається атакою. Далі представлено класифікацію методів виявлення НСД (рис.1).

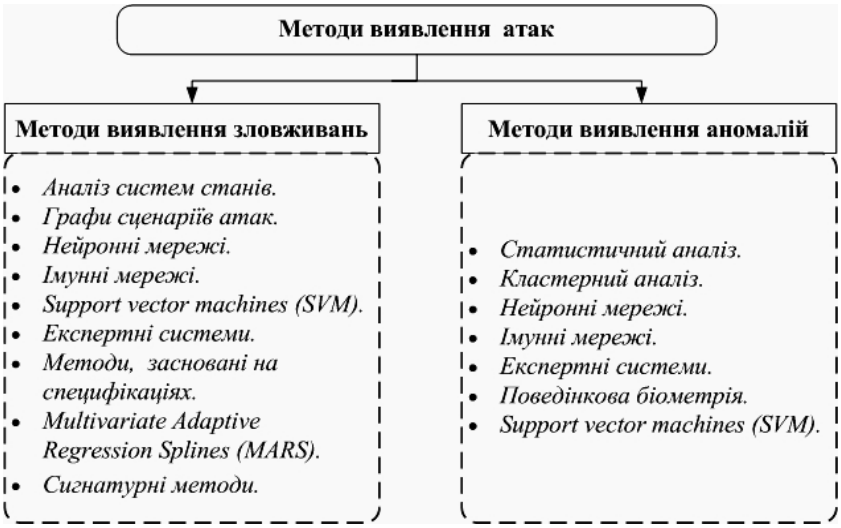

Рис. 1. Класифікація методів виявлення НСД в сучасних інформаційних системах та мережах

Аналіз систем станів. У даній групі методів функціонування системи, що захищається, представляється через безліч станів і безліч переходів між ними, тобто у вигляді орієнтованого графа. Суть методу виявлення атак полягає в тому, що частина шляхів в такому графі позначаються як неприпустимі; кінцевий стан кожного такого шляху вважається небезпечним для системи, що захищається. Процесом виявлення атаки є побудова частини графа станів системи і спостережуваних переходів між ними, і пошук в отриманому графі відомих неприпустимих шляхів. Виявлення послідовності переходів, що приводить в небезпечний стан, означає успішне виявлення атаки [1]. Даний метод є гібридним з погляду рівня спостереження за системою, верифікуємим, стійким, має низьку обчислювальну складність (лінійну щодо довжини траси спостережуваних переходів і числа станів), але не є адаптованим.

Графи сценаріїв атак. Даний метод заснований на основі використання методів формальної специфікації. На вхід системи верифікації подається кінцева модель інформаційної системи, що захищається, і деяка формальна властивість коректності її роботи, яка виконується тільки для дозволеної поведінки системи. Дану властивість коректності ділить вся безліч поведінок ділиться на два класи - допустимої поведінки, для якої властивість коректності виконується, і неприпустимої, для якої вона не виконується. Відмінність даного методу від звичайних систем верифікації полягає в тому, що їх завдання, полягає в тому, що потрібно знайти один контрприклад з множини неприпустимої поведінки, а в запропонованому методі будується повний набір таких прикладів для конкретної системи, що захищається, що дає на виході опис можливих шляхів атаки [2]. Із-за високої обчислювальної складності даний метод може бути використаний для пошуку уразливостей проектування систем і інших складних для виявлення уразливостей. Даний метод для завдання виявлення атак в реальному часі непридатний.

Нейронні мережі. Оскільки завдання виявлення атак можна розглядати як завдання розпізнавання образів (або завдання класифікації), то для її вирішення також застосовуються нейронні мережі. Для цього функціонування системи, що захищається, і зовнішніх об'єктів, що взаємодіють з нею, представляється у вигляді траєкторій в деякому числовому просторі ознак [3]. Як метод виявлення зловживань, нейронні мережі навчаються на прикладах атак кожного класу і, надалі, використовуються для розпізнавання приналежності спостережуваної поведінки одному з класів атак. Основна складність у використанні нейромереж полягає в коректній побудові такого простору ознак, який дозволив би розділити класи атак між собою і відокремити їх від нормальної поведінки. Крім того, для класичних нейронних мереж характерне довге навчання, при цьому час навчання залежить від розміру навчальної вибірки [11]. Найбільш часто для виявлення НСД нейронні мережі використовуються на мережному і вузловому рівнях, є адаптивними та мають низьку обчислювальну складність. При цьому вони не є верифікуємими і стійкими, як правило, тільки в межах тієї мережі, в якій вони навчалися, що істотно обмежує застосування даного методу (тільки забезпечується локальна стійкість).

Імунні мережі

Також як і нейронні мережі, імунні мережі є механізмом класифікації і будуються по аналогії з імунною системою живого організму. Основна перевага імунних мереж полягає в можливості отримання «антитіл» до невідомих атак. Використання даного методу вимагає вирішення системи диференціальних рівнянь в режимі виявлення, що дає високу обчислювальну складність порядку при використанні методу Рунге-Кутта [12]. Дана група методів застосовується для мережного і вузлового рівнів ІКСМ.

Support vector machines (SVM)

SVM – це метод уявлення і розпізнавання шаблонів, який дозволяє формувати шаблони в результаті навчання. Даний метод вимагає невеликої

кількості даних для навчання і дозволяє обробляти вектори ознак великої розмірності, що корисно для підвищення точності систем виявлення атак і зниження тимчасових витрат на навчання і перенавчання. Метод застосовний як для виявлення зловживань, так і для виявлення аномалій. SVM має такі ж переваги і недоліки для вирішення завдання, як і нейронні мережі, тобто є адаптивним, але неверифікуємим.

Експертні системи

Використання експертних систем для виявлення атак заснований на описі функціонування системи у вигляді безлічі фактів і правил виводу, зокрема для атак. На вхід експертна система отримує дані про спостережувані події в системі у вигляді фактів. На підставі фактів і правил виводу система робить висновок про наявність або відсутність атаки [4]. Дана група методів в загальному випадку має дуже велику обчислювальну складність.

Методи, засновані на специфікаціях

У основі даного методу лежить опис обмежень на заборонену поведінку об'єктів в системі, що захищається, у вигляді специфікацій атак. У специфікацію може входити: обмеження на завантаження ресурсів, на список заборонених операцій і їх послідовностей, на час доби, протягом якого застосовні ті або інші обмеження. Відповідність поведінки специфікації вважається атакою [5]. Специфікації використовуються для мережного рівня і є локально стійкими і мають низьку обчислювальну складність.

Multivariate Adaptive Regression Splines (MARS). Один з методів апроксимації функцій, заснований на сплайнах. Аналогічно нейронним мережам і кластерному аналізу MARS оперує в багатовимірному просторі ознак. Поведінка мережних об'єктів відображається в послідовності векторів даного простору. Завдання процедури MARS полягає в побудові оптимальної апроксимації поведінки по заданій історії у вигляді навчальної безлічі векторів, при цьому як апроксимуюча функція використовуються сплайни із змінним числом вершин. В ході «навчання», за допомогою процесу перебору, вибирається оптимальне число вершин для заданої вибірки. Побудований сплайн є «шаблоном» атаки [6]. У режимі розпізнавання спостережувана поведінка відображається в параметричний простір і порівнюється з апроксимуючою функцією.

Сигнатурні методи. Суть даного методу полягає в складанні деякого алфавіту із спостережуваних в системі подій і описі безлічі сигнатур атак у вигляді регулярних виразів (у загальному випадку) в побудованому алфавіті. Як правило, сигнатурні методи працюють на найнижчому рівні абстракції і аналізують безпосередньо дані, що передаються в мережі, параметри системних викликів і записи файлів журналів. У найбільш розвиненому вигляді є реалізацією регулярних виразів над різними трасами (мережний трафік, системні виклики, записи журналів додатків і тому подібне) [7]. Сигнатурні методи примітні тим, що для них добре застосовні апаратні прискорювачі, але при цьому метод не є адаптивним.

Методи виявлення аномалій

Статистичний аналіз. Дана група методів заснована на побудові статистичного профілю поведінки системи протягом деякого періоду «навчання», при якому поведінка системи вважається нормальною. Для кожного параметра функціонування системи будується інтервал допустимих значень, з використанням деякого відомого закону розподілу. Далі, в режимі виявлення, система оцінює відхилення спостережуваних значень від значень, отриманих під час навчання. Якщо відхилення перевищують деякі задані значення, то фіксується факт аномалії (атаки) [8]. Для статистичного аналізу характерний високий рівень помилкових спрацьовувань при використанні в локальних мережах, де поведінка об'єктів не має гладкого, усередненого характеру. Крім того, даний метод стійкий тільки в межах конкретної системи, тобто побудовані статистичні профілі не можна використовувати на інших аналогічних системах.

Кластерний аналіз. Суть даної групи методів полягає в розбитті безлічі спостережуваних векторів – властивостей системи на кластери, серед яких виділяють кластери нормальної поведінки. У кожному конкретному методі кластерного аналізу використовується своя метрика, яка дозволяє оцінювати приналежність спостережуваного вектора властивостей системи одному з кластерів або вихід за межі відомих кластерів [9].

Нейронні мережі. Нейронні мережі для виявлення аномалій навчаються протягом деякого періоду часу, коли вся спостережувана поведінка вважається нормальною. Після навчання нейронна мережа запускається в режимі розпізнавання. За ситуації, коли у вхідному потоці не вдається розпізнати нормальну поведінку, фіксується факт атаки. У разі використання репрезентативної вибірки нейронні мережі дають хорошу стійкість в межах заданої системи, але складання подібної вибірки є серйозним і складним завданням [3]. Класичні нейронні мережі мають високу обчислювальну складність навчання, що затрудняє їх застосування на великих потоках даних.

Імунні мережі. Виявлення аномалій є одним з можливих додатків імунних методів. Оскільки кількість прикладів нормальної поведінки звичайно на порядки перевищує число прикладів атак, використання імунних мереж для виявлення аномалій має велику обчислювальну складність [7].

Експертні системи. Інформація про нормальну поведінку представляється в подібних системах у вигляді правил, а спостережувана поведінка у вигляді фактів. На підставі фактів і правил ухвалюється рішення про відповідність спостережуваної поведінки «нормальному», або про наявність аномалії [10]. Головний недолік подібних систем - висока обчислювальна складність (у загальному випадку). Зокрема при виявленні аномалій.

Поведінкова біометрія. Включає методи, що не вимагають спеціального устаткування (сканерів сітківки, відбитків пальців), тобто методи виявлення атак, засновані на спостереження клавіатурного почерку і використання миші. У основі методів лежить гіпотеза про відмінність «почерку» роботи з інтерфейсами введення-виводу для різних користувачів. На базі побудованого профілю нормальної поведінки для даного користувача виявляються відхилення від цього профілю, викликані спробами інших осіб працювати з клавіатурою або іншими фізичними пристроями введення [2]. Поведінкова біометрія має строго локальну стійкість (в межах однієї мережі).

Support vector machines (SVM). SVM застосовний як для виявлення зловживань, так і для виявлення аномалій, при цьому метод має достоїнства і недоліки, аналогічні нейронним мережам.

Класифікація систем виявлення атак

Існують різні підходи до класифікації систем виявлення вторгнень, але в практичній діяльності найчастіше застосовується така класифікація НСД, що враховує принципи практичної реалізації таких систем:

- виявлення атак на рівні мережі;
- виявлення атак на рівні системи (вузла).

Перші системи аналізують мережний трафік, тоді як другі реєстраційні журнали операційної системи або додатку.

Необхідно відмітити, що лише деякі системи виявлення атак можуть бути однозначно віднесені до одного з названих класів. Як правило, вони включають можливості декількох категорій. Проте ця класифікація відображає ключові можливості, що відрізняють одну систему виявлення атак від іншої. Принципова перевага мережних систем виявлення атак полягає в тому, що вони ідентифікують НСД перш, ніж ті досягнуть вузла, що атакується. Ці системи простіші для розгортання в розгалужених ІКСМ, тому що не вимагають встановлення програмного забезпечення на різні платформи, використовувані в організації. Крім того, системи виявлення атак на рівні мережі практично не знижують продуктивності мережі.

Існує і ще одна класифікація систем виявлення атак. Вона ділить системи по тому, коли аналізуються дані - **в реальному масштабі часу** або **після здійснення події**. Як правило, системи виявлення атак на рівні мережі працюють в реальному режимі часу, тоді як системи, що функціонують на рівні вузла, забезпечують автономний аналіз реєстраційних журналів операційної системи або додатків [13]. Переваги і недоліки кожного з підходів залежать від того, як буде застосовуватися система виявлення атак. У разі висококритичних систем, виявлення атак в реальному режимі часу є обов'язковим, оскільки зловмисник може проникнути в систему, зробити все, що необхідно і зникнути протягом декількох хвилин або навіть секунд. Проте і автономний аналіз має чимале значення. Він дозволяє проводити детальне дослідження того, коли і як зловмисники проникли у вашу систему та дозволяє виробити ефективні заходи протидії НСД. Реалізований такий аналіз може бути по-різному. Починаючи від простої генерації звіту з інформацією про всі або вибрані минулі події, і закінчуючи відтворенням в реальному часі всіх дій, здійснених при атаці. Проте необхідно відмітити, що аналіз даних «постфактум» корисний тільки за наявності кваліфікованого персоналу. Необхідний склад персоналу для експлуатації системи виявлення атак дуже важко визначити, оскільки це залежить від об'єму даних, що вимагають аналізу. Важливо, щоб системи виявлення атак підтримували цю можливість, надаючи ефективні засоби управління даними.

Висновок. Використання описаних видів методів та систем виявлення НСД дозволяє посилити політику безпеки і внести велику гнучкість до процесу експлуатації мережних ресурсів ІКСМ. Але будь-які системи те методи мають як і певні переваги, так і деякі недоліки. При аналізі роботи цих засобів виявляється, що більшість з них виконують лише одну або декілька специфічних функцій, які не можуть забезпечити в тій чи іншій мірі комплексності захисту інформації. В результаті проведеного аналізу методів та систем виявлення НСД виділено, що тільки завдяки комбінації декількох методів та систем можна досягти ефективного захисту і забезпечити протидію загрозам, як навмисним та і випадковим.

Література

[1] Koral Ilgun, Richard A Kemmerer, and Phillip A Porras, “State transition analysis: A rule-based intrusion detection approach”. // IEEE Transactions on Software Engineering, 21(3):181–199, March 1995

[2] Sheyner, Oleg “Scenario Graphs and Attack Graphs.” // PhD thesis, SCS, Carnegie Mellon University, 2004.

[3] Смелянский Р.Л., Качалин А.И. “Применения нейросетей для обнаружения аномального поведения объектов в компьютерных сетях”. // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2004.

[4] Sebring, M., Shellhouse, E., Hanna, M. & Whitehurst, R. Expert Systems in Intrusion Detection: A Case Study. // Proceedings of the 11th National Computer Security Conference, 1988.

[5] Calvin Ko, “Execution Monitoring of Security-critical Programs in a Distributed System: A Specification-based Approach.” // PhD thesis, Department of Computer Science, University of California at Davis, USA, 1996.

[6] Koral Ilgun, Richard A Kemmerer, and Phillip A Porras, “State transition analysis: A rule-based intrusion detection approach”. // IEEE Transactions on Software Engineering, 21(3):181–199, March 1995.

[7] Sandeep Kumar and Eugene H. Spafford, “A pattern matching model for misuse intrusion detection.” // Proceedings of the 17th National Computer Security Conference, pages 11–21, Baltimore MD, USA, 1994.

[8] Debra Anderson, Teresa F. Lunt, Harold Javitz, Ann Tamaru, and Alfonso Valdes, “Detecting

unusual program behavior using the statistical component of the next generation intrusion detection system (NIDES)". // Technical Report SRI-CSL-95-06, Computer Science Laboratory, SRI International, Menlo Park, USA, May 1995.

[9] Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun FelixWu, and CleavelandW Rance, "Architecture design of a scalable intrusion detection system for the emerging network infrastructure." // Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA, April 1997.

[10] Sebring, M., Shellhouse, E., Hanna, M. & Whitehurst, R. Expert Systems in Intrusion Detection: A Case Study. // Proceedings of the 11th National Computer Security Conference, 1988

[11] Herve Debar, Monique Becker, and Didier Siboni, "A neural networkcomponent for an intrusion detection system." // Proceedings of the 1992 IEEE Computer Sociecty Symposium on Research in Security and Privacy,pages 240–250, Oakland, CA, USA, May 1992.

[12] M.P.Zielinski, "Applying Mobile Agents in an Immune-system-based intrusion detection system." // University of South Africa, 2004.

[13] Sheyner, Oleg "Scenario Graphs and Attack Graphs." // PhD thesis, SCS,Carnegie Mellon University, 2004.

УДК 004.056.53 (045)

Чунарева А.В., Чунарев А.В. Методы и системы обнаружения несанкционированного доступа в современных информационно-коммуникационных системах и сетях

Аннотация. *В данной статье проведен анализ современных методов и систем обнаружения несанкционированного доступа в современных информационно-коммуникационных системах и сетях. В результате проведения анализа выделены преимущества и недостатки применения существующих методов и систем. Выделены наиболее эффективные с точки зрения повышения защиты информации и обеспечения противодействия угрозам, как преднамеренным и случайным.*

Ключевые слова: *защита информации, несанкционированный доступ, атака, информационно-коммуникационная система и сеть, уязвимость.*

Chunariova A.V., Chunariov A.V. Methods and systems for the detection of unauthorized access to modern information and communication systems and networks

Abstract. *In this paper, an analysis of modern methods and systems to detect unauthorized access to modern information and communication systems and networks. As a result, the analysis highlighted the advantages and disadvantages of existing methods and systems. Select the most efficient in terms of improving data protection and security to counter threats such as deliberate and accidental.*

Keywords: *information security, unauthorized access, attacks, information and communication system and network, vulnerabilities.*

Отримано *15 березня 2012 року,* затверджено редколегією *04 червня 2012 року*
(рецензент д.т.н., професор О.К. Юдін)

МЕТОДИКА ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ЛОМ. ГРАФІЧНІ МОДЕЛІ ВЗАЄМОДІЇ ЗАГРОЗ ФУНКЦІОНАЛЬНИМ ВЛАСТИВОСТЯМ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЛОМ ІЗ ЕЛЕМЕНТАМИ СИСТЕМИ ЗАХИСТУ

Вячеслав Василенко, Олена Дубчак, Микола Василенко

Національний авіаційний університет

ВАСИЛЕНКО Вячеслав Сергійович, к.т.н., доцент

Рік та місце народження: 1941 рік, с. Євстратівка, Россошанський р-н, Воронізька обл., Росія.
Освіта: Київське вище інженерне радіотехнічне училище ППО, 1971 рік, Харківська інженерна радіотехнічна академія ППО, 1978 рік.
Посада: доцент кафедри комп'ютеризованих систем захисту інформації з 2005 року.
Наукові інтереси: технічний захист інформації.
Публікації: більше 200 наукових публікацій, серед яких навчальні посібники, наукові статті свідотства та патенти на винаходи.
E-mail: bbc1@voliacable.com