УДК 004.056.5(045)

Чунарьова А.В., к.т.н.

СУЧАСНІ МЕТОДИ АУДИТУ ТА МОНІТОРИНГУ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ

Інститут комп'ютерних інформаційних технологій Національного авіаційного університету

В статті проведено класифікацію та аналіз існуючих методів аудиту та моніторингу інформаційних потоків інформаційно-комунікаційних систем та мереж, що дозволило формувати критерії оцінки якості систем моніторингу

Вступ

Для вирішення більшої частини проблем, які виникають при функціонуванні інформаційних мереж, використовують системи моніторингу й управління. Цей клас рішень забезпечує інвентаризацію й розширену діагностику комп'ютерних мереж; постійний контроль функціонування використовуваного мережного устаткування, прикладних систем і мережних сервісів; збір статистики й візуалізацію ключових показників продуктивності й операційних параметрів мережної інфраструктури; оптимізацію навантаження на мережне устаткування й сервери; фіксацію інцидентів; аналіз впливу ризиків на бізнес-процеси, і критично важливі додатки; локалізацію причин інциденту і його автоматичне усунення, або повідомлення відповідальних за його усунення осіб. Використання подібних систем дозволяє організації здійснювати про активний моніторинг доступності, стану й продуктивності компонентів мережі передачі даних, аналізувати й оптимізувати їхнє завантаження, а також прогнозувати виникнення позаштатних ситуацій.

Аудит автоматизованих інформаційних систем – це перевірка матеріально технічних ресурсів організації, зокрема компонентів інформаційно-комунікаційних систем та мереж (ІКСМ), систем безпеки на предмет їх відповідності встановленим вимогам та стандартам. Основними завданнями аудиту є: оцінка поточного стану інформаційної безпеки; ідентифікація та ліквідація вразливостей; мінімізація збитків від потенційно реалізованих загроз; відповідність державним, національним та міжнародним стандартам. Нормативним документом з цих питань виступає НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Функціональними критеріями за документом є: конфіденційність; цілісність; доступність; спостереженість [1]. Дані критерії надають базу для розробки або модернізації ІКСМ, у яких мають бути реалізовані функції захисту інформації та порівняльну шкалу для оцінки надійності діючих механізмів захисту інформації. Окрім функціональних критеріїв захищеності існують таки критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації [1]. Наступним документом, що регламентує порядок проведення аудиту та визначення слабких місць ІКСМ є міжнародний стандарт *ISO/IEC* 15408 «Загальні критерії оцінки безпеки інформаційних технологій». Стандарт описує інфраструктуру, у якій користувачі (замовники) комп'ютерної системи описують вимоги, розробники описують характеристики з безпеки комп'ютерної системи, а експерти (аудитори) визначають, чи задовольняє комп'ютерна система критеріям [2]. Важливу роль у роль у стандартизації критеріїв, яким повинна відповідати ІКСМ грає асоціація *ISACA*. Даною асоціацією створено стандарт COBIT «Контрольні об'єкти інформаційних та суміжних технологій». Стандарт вводить 5 основ-

них об'єктів, що являються ресурсами інформаційних технологій [3-4]: дані, додатки, технології, обладнання, люди. Та на відміну від державного нормативного документу НД ТЗІ 2.5-004-99, описуються такі критерії оцінки інформації: ефективність, продуктивність, конфіденційність, цілісність, надійність, придатність, узгодженість.

Частина стандарту, що зосереджена на порядку проведення аудиту, орієнтована на аудиту IT–процесів. COBIT складається з високорівневих цілей контролю, що охоплюють всі параметри інформаційних систем, враховують життєвий цикл та специфічні задачі ІКСМ.

Постановка задачі

Метою статті є класифікація та аналіз існуючих методів аудиту та моніторингу інформаційних потоків ІКСМ; формування критеріїв оцінки якості систем аудиту та контролю інформаційних потоків; формування вимог для створення методів та підсистем аудиту і контролю окремих функціональних елементів ІКСМ.

Класифікація засобів моніторингу ІКСМ

Різноманіття засобів, що використовуються для контролю та аналізу ІКСМ поділяються на декілька класів:

1. *Системи керування мережею* – централізовані програмно-апаратні системи, що збирають дані про стан вузлів та комунікаційних пристроїв мережі, дані про трафік, що циркулює у мережі. Особливістю даних систем є, те що вони в автоматичному або напівавтоматичному режимах виконують дії з керування мережею – увімкнення або відімкнення портів приладів, зміна змісту маршрутизуючих таблиць, правил брандмауерів, тощо[7-8].

2. *Засоби керування системою* – виконують функцію, що аналогічні до систем керування мережею, але по відношенню до комунікаційного обладнання. Також вона здатна виконувати найпростіший аналіз мережевого трафіка.

3. *Вбудовані системи діагностики та управління* – дані системи реалізуються шляхом використання програмних модулей у комунікаційне обладнання. Вони направлені на виконання функцій діагностики та керування лише над одним пристроєм. На даний час вбудовані системи також виконують роль *SNMP*-агентів, що постачають дані для систем керування мережею.

4. *Аналізатори протоколів* – програмні або програмно – апаратні системи, що виконують лише функції моніторингу та аналізу трафіку. Характеристикою аналізатора є здатність до виявлення певного числа протоколів. Аналізатори встановлюють логічні умови з метою перехоплення пакетів для визначених протоколів.

5. *Експертні системи* – даний вид систем акумулює людські знання про виявлення причин аномальної роботи мережі та можливих способах повернення мережі до нормального режиму функціонування. Експертні системи часто реалізуються у вигляді підсистем засобів моніторингу та систем керування мережею. Функціональною основою складних експертних систем є так звані бази знань, що володіють елементами штучного інтелекту [5].

Далі розглянемо найбільш поширені методи проведення моніторингу доступності та цілісності інформаційних потоків. До основних методів моніторингу відносяться: активний моніторинг, пасивний моніторинг, моніторинг мережі базований на маршрутизації, моніторинг за аномальною поведінкою.

Активний моніторинг. Суть активного моніторингу полягає у передачі в інформаційну мережу пакетів з метою вимірювання параметрів між двома кінцевими точками корпоративної мережі. Вимірюються такі параметри: доступність, маршрут, затримка пакетів, зміна порядку пакетів, втрата пакетів, пропускна здатність каналу. Базовими інструментами, що здатні допомогти у вимірюванні вищезгаданих параметрів є *ping*, що вимірює затримки та втрату пакетів, *traceroute*

– допомагає побудувати топологію мережі. Ці інструменти використовують *ICMP* пакети. Також даний метод аудиту реалізується з використанням інструменту *iperf*, що генерує *TCP* та *UDP* трафік для вимірювання пропускної здатності мережі та втрати пакетів [6]. Недоліком активного моніторингу є те, що згенерований трафік може завантажує мережу під час її експлуатації.

Пасивний моніторинг. На відміну від активного моніторингу, пасивний метод не генерує надлишкового трафіку, та вимірює параметри продуктивності лише в одній точці мережі. Даний метод знайшов застосування у пакетних сніферах. Результати пасивного моніторингу можуть бути досліджені лише постфактум, при цьому ніякого навантаження на мережу не має.

Моніторинг мережі, що базується на маршрутизації. Такі методи зазвичай реалізуються програмно-апаратними засобами мережевих пристроїв.

Simple Network Management Protocol. Даний протокол є протоколом прикладного рівня стеку *TCP/IP*. Його використання надає адміністратору мережі можливості з керування та контролю над пристроями (комутаторами, маршрутизаторами, серверами, модемами, робочими станціями) та додатками у мережі шляхом обміну інформацією між агентами, що встановлені у мережевих пристроях та менеджерами, що встановлені на станціях керування (*Network Management Systems*) [7]. Агенти є програмним забезпеченням, здатним перетворювати дані протоколу *SNMP* у команди керування пристроями, та навпаки. Станції керування є програмним забезпеченням, що здійснюють моніторинг та контроль за керованими пристроями. Обробка всіх даних, отриманих з агентів, виконується на станціях. Станції керування здатні виконувати 4 базові операції: *read* – зчитування значень змінних, що знаходяться у пам'яті керованих пристроїв; *write* – змінює значення змінних; *traversal operations* – накопичення інформації щодо доступних змінних керованого пристрою; *trap* – повідомляє *NMS* про певну подію, що сталася з керованим пристроєм. Недоліком використання *SNMP* у мережі, є те що даний протокол є вразливим, оскільки жодних процедур з аутентифікації користувачів не виконується.

Remote Monitoring (RMON). *RMON* включає в собі різні мережеві монітори та системи для обміну інформацією мережевого моніторингу. Даний метод моніторингу є розширенням *Management Information Database* (*MIB*). На відміну від *SNMP*, коли *NMS* повинна власноруч надсилати запити на отримання інформації, *RMON* дозволяє налаштовувати обробники подій, що будуть спрацьовувати за певних критеріїв. Іншою відміною від *SNMP* є те, що агенти *RMON* збирають та зберігають інформацію самостійно. Агентами можуть бути мережеві пристрої зі вбудованим програмним забезпеченням та комп'ютери. Агенти здатні бачити трафік лише всередині певного сегменту. Роль клієнта виконує станція керування, що взаємодіє з агентами з використанням *SNMP* [6]. Дана технологія функціонує на мережевому рівні та нижче.

Моніторинг за аномальною поведінкою

Суть даного методу полягає у моніторингу стану мережі та виявлення значних відхилень параметрів у порівнянні зі значеннями цих параметрів при стабільному функціонуванні. Наприклад, для виявлення аномальної динаміки мережевого трафіку використовується штучний інтелект та статистичні показники. Для ефективного застосування даного методу, спочатку необхідно зафіксувати контрольні значення важливих параметрів функціонування мережі. Виявлення аномалій запускає модуль для подальшого аналізу трафіку або спричинює повідомлення для аналітика безпеки [5].

Вимоги до засобів аудиту та моніторингу ІКСМ

Базовими вимогами, що ставляться до систем моніторингу є:

– масштабованість та розподіле-

ність. Дані властивості є взаємопов'язаними, оскільки високий рівень здатності до масштабування досягається за рахунок розподіленості системи управління. Під розподіленістю будемо розуміти те, що система може включати декілька серверів та клієнтів. Сервери (менеджери) накопичують дані про поточний стан мережі з встановлених у ній агентів у власній базі даних. Клієнти використовують інтерфейси для доступу до накопиченої інформації серверу;

– відкритість, що дозволяє використовувати систему з різнотипним обладнанням від різних виробників. [8];

– ступінь завантаженості ІКСМ. Функціональні компоненти, що входять до складу систем контролю здатні генерувати трафік для вимірювання показників продуктивності мережі, що впливає на пропускну здатність каналів передачі;

– кількість вузлів, що може аналізуватися та контролюватися системою;

– можливість встановлення клієнтів та серверів на робочі станції з різними операційними системами;

– отримання інформації про динаміку трафіку у режимі реального часу;

– здатність системи до конфігурації контролю окремих програмних додатків;

– наявність централізованого місця накопичення службової інформації, з можливістю індексування для прискорення витягу потрібних даних;

– можливість створення реєстру наявних у мережі програмних та апаратних ресурсів.

Критерії оцінки якості системи аудиту та моніторингу інформаційних потоків

Виділення вимог дозволило сформувати критерії оцінки якості системи аудиту та моніторингу інформаційних потоків: підтримка різних операційних систем; можливість аудиту та контролю різних за призначенням серверів; можливість аудиту та контролю СУБД; виявлення відхилень функціонування мережі від норми (поява незареєстрованих вузлів, втрата зв'язку з окремими вузлами, втрата пакетів, перенавантаження комунікаційних пристроїв); підтримка графічних інтерфейсів для перегляду звітів, можливості конфігурування параметрів налаштувань (табл. 1).

Висновки.

В даній статті проведено класифікацію існуючих методів аудиту та моніторингу; сформовано критерії оцінки якості систем аудити та контролю інформаційних потоків; сформовано вимоги щодо функціонування методів аудиту та контролю окремих елементів ІКСМ.

Виконавши аналіз основних характеристик, за якими порівнюються системи аудиту та моніторингу та значення даних характеристик для найбільш підготовлених корпоративних рішень зроблені наступні висновки:

– у випадку необхідності проведення аудиту необхідною є така функція системи, як можливість побудови топології мережі із занесенням до реєстру всіх можливих ресурсів мережі;

– підтримка популярних та ефективних СУБД є перевагою над тими системами, що використовують для збереження даних бінарні файли, що значно впливає на продуктивність системи;

– підтримка протоколу *SNMP* є значною перевагою, що підвищує ефективність моніторингу та контролю об'єктів мережі;

– в залежності від місця застосування систем моніторингу та контролю, варіюються і операційні системи, що встановлені на об'єктах мережі. Наприклад, на серверах більш промислового призначення зазвичай можуть бути встановлені такі ОС, як *HPUX*, *IBM*, коли в інших випадках переважають *UNIX* – подібні ОС, та ОС *Microsoft Windows*.

Таблиця 1. Порівняння поширених інструментів моніторингу та аудиту за характеристиками

Інструмент моніторингу / Критерії оцінки	OpenView Network Node Manager 4.1	Spectrum Enterprise Manager	NetView forAIX SNMP Manager	Solstice Enterprise Manager
Визначення імені хосту через DNS – сервер	+	+	+	+
Розпізнавання мережевих топологій	Будь – які мережі на TCP/IP	Ethernet, розподілені мережі	Розпізнавання за інтерфейсами пристроїв	Ethernet, розподілені мережі
Підтримка баз даних	Oracle	Файли	Oracle, Sybase	Informix, Oracle, Sybase
Наявність серверів	+	+	+	+
Кількість клієнтів	До 15	Необмежено	30	Необмежено
Підтримка SNMP	+	+	+	+
Підтримка ОС	HPUX, Solaris	HPUX, IBM, Win NT	Win NT	Solaris
Максимальне число вузлів, що обслуговуються	3000	Обмеження відсутнє	Обмеження відсутнє	10000-50000

Можна відзначити, що моніторинг та управління доступу корпоративних мереж є перспективним напрямком розвитку інформаційної інфраструктури та гарантованості надання послуг. Незважаючи на ряд проблем, що виникають при його впровадженні, використання подібних рішень забезпечить значний ріст ефективності використання апаратного й програмного забезпечення й знизить число критичних збоїв та несанкціонованих дій, що особливо важливо для сучасних ІКСМ.

Список літератури

1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

2. ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій».

3. COBIT «Контрольні об'єкти інформаційних та суміжних технологій».

4. Леденко С.А., Чикалев И.А. Международный стандарт COBIT как средство управления бизнесом// Information Security/ Информационная безопасность. – 2007. – № 6. – С. 12-14.

5. Internetworking Technology Handbook : User manual / Jackson C. – Massachusets : Cisco Systems, 2011. – P. 56 -67.

6. Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques / A. Cecil // Computer Systems Analysis. – 2006. – P.4 – 7.

7. Lowekamp B. Using passive traces of application traffic in a network monitoring systems. / B.B. Lowekamp, M. Zangrilli. – IEEE Computer Society, 2004. – P. 73 – 75.

8. Fry C. Security Monitoring / C. Fry, M. Nystrom – Sebastopol : O'Reily Media, 2009. – P.40 – 56, 163 – 170.

Статтю подано до редакції 20.09.2013