УДК 004.7(066)

Ю. М. ІВЧЕНКО (ДІІТ), В. Г. ІВЧЕНКО, О. М. ГОНДАР (ІОЦ Придніпровської залізниці, Дніпропетровськ)

СИСТЕМА МОНІТОРИНГУ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

В статті надана оцінка небезпеці збоїв сервісів та служб корпоративної інформаційно-телекомунікаційної системи Придніпровської залізниці, важливості виконання постійного контролю функціонування основних компонентів системи. Запропоновані класифікація компонентів за категоріями, залежно від функціонального призначення, і програмне забезпечення для контролю компонентів кожної категорії.

Ключові слова: моніторинг корпоративної інформаційної мережі.

Корпоративна мережа Придніпровської залізниці вимагає постійної уваги до себе. Збої апаратного чи програмного забезпечення можуть провести до тяжких наслідків. Значне сповільнення функціонування мережевих сервісів та служб – найменш неприємне з них. Особливо складними є випадки, коли зовсім припиняється функціонування критично важливих служб і додатків, а також коли стають недоступними окремі сегменти мережі або територіально віддалені підприємства.

Від правильної, коректної роботи маршрутизаторів та іншого мережевого обладнання залежить доступність серверів та їх сервісів. Від працездатності серверів (веб-серверів, серверів баз даних, серверів електронного документообігу), в свою чергу, залежить робота важливих додатків і сервісів, які забезпечують функціонування оперативних систем АСК ВП УЗ та АСК ПП УЗ. Вихід з ладу будь-якого з перелічених компонентів може привести до серйозних порушень у роботі інформаційних систем.

Але слід відмітити, що вихід з ладу обладнання або збій в роботі програмного забезпечення не завжди є основними і найбільш небезпечними причинами порушення функціонування інформаційних систем.

Більшою небезпекою є збої, викликані зловмисними діями всередині або ззовні мережі.

Зловмисники, використовуючи вразливості програмного забезпечення чи помилки в конфігурації, можуть виконати безліч деструктивних дій, починаючи з простого виведення з ладу серверів, далі зміни конфігурації мережевого обладнання, порушення роботи мережі, зміни спрямування трафіка, закінчуючи зараженням вірусами та викраданням конфіденційних даних.

Не варто залишати поза увагою також помилки обслуговуючого та керуючого персоналу підчас обслуговування чи зміни конфігурації будь-якої частини інформаційних систем.

Всі перелічені варіанти відмов та порушень в роботі інформаційних систем можуть викликати серйозні матеріальні збитки: затримки вагонів, припинення реалізації квитків, розголошення конфіденційної інформації, втрата довір'я клієнтів тощо.

Оскільки виключити повністю збої апаратного чи програмного забезпечення неможливо, рішення проблеми полягає в постійному контролі стану складових частин інформаційної системи для отримання інформації щодо проблем на ранніх стадіях.

Для досягнення цієї мети, як правило, використовується різноманітне програмне забезпечення, яке контролює роботу серверів, компонентів мережі передачі даних, зміни конфігурацій, а також збирає статистичну інформацію щодо їх функціонування.

Вибір засобів моніторингу залежить від різних факторів. Так можливості моніторингу мережевого обладнання, в значній мірі, визначаються його виробником. Для серверів вирішальним є тип операційної системи та прикладне програмне забезпечення.

Зараз існує значна кількість програмних продуктів для здійснення контролю функціонування інформаційних систем та їх складових.

Класифікуємо компоненти інформаційних систем за категоріями залежно від функціонального призначення та розглянемо програмні продукти, які виконують їх контроль.

Можливо виділити наступні категорії та програмне забезпечення для їх контролю [2]:

Категорії	Компоненти	ПЗ
1	Доступність та зміни конфігурацій мережевого обладнання, збереження резервних копій конфігурацій	Rancid, Nagios
2	Контроль безпеки, наявності вразливостей та помилок конфігурування систем і сервісів	Nessus, Lotus Domino

© Івченко Ю. М., Івченко В. Г., Гондар О. М., 2011

Категорії	Компоненти	ПЗ
3	Статистика стану і завантаження каналів, облік помилок, детальний аналіз трафіку	Cacti, Fluke NetWatch, Fluke Netflow Tracker
4	Контроль функціонування критичних служб і додатків	Nagios
5	Інвентаризація ПЗ серверів та користувачів, контроль встановленого ПЗ	Microsoft System Center Configuration Manager 2007

Програмне забезпечення Rancid проводить моніторинг конфігурації маршрутизаторів, включаючи програмне і апаратне забезпечення (модулі, серійні номери і т. ін.), та використовує Subversion для контролю історії змін.

Nagios – це додаток, що використовується для виконання моніторинга систем і мереж. Він стежить за певними додатками і службами та генерує сповіщання в залежності від поведінки служб, за якими ведеться спостереження.

Сумісне використання програмного забезпечення Rancid і Nagios дозволяє проводити постійний контроль змін конфігурацій мережевого обладнання, мати актуальний набір резервних копій файлів конфігурацій, отримувати оперативні повідомлення про недоступні вузли мережі передачі даних. Це дозволяє контролювати спроби несанкціонованих змін конфігурацій маршрутизаторів, оперативно виявляти і виправляти помилки адміністраторів мережі передачі даних при виконанні змін конфігурацій мережевого обладнання. У випадку, якщо зміни конфігурації приводять до відмови в роботі вузлів мережі, програмне забезпечення Nagios, що здійснює контроль за доступністю вузлів, сповістить про це відповідальних співробітників.

Nessus – це програма для автоматичного пошуку відомих вразливостей в захисті інформаційних систем. Вона спроможна виявити види ураження, які найбільш часто трапляються, наприклад:

- наявність вразливих версій служб або демонів;
- помилки в конфігурації (наприклад, відсутність необхідності авторизації на SMTP-сервері);
- наявність паролів за замовчанням, пустих або слабких паролів.

Програма має клієнт-серверну архітектуру, що значно розширює можливості сканування.

IBM Lotus Domino Server – сервер додатків системи Lotus Notes, базово надає ряд сервесів (нереляційна СУБД, сервер каталогів, поштовий сервер, web-сервер) і може використовуватися для побудови корпоративних систем електронного документообігу, колективної роботи, інших додатків. Він має в своєму складі великий набір модулів. Основними з яких є поштовий сервер, http-сервер, сервер баз даних.

На Придніпровські залізниці за допомогою Nessus і Lotus Domino розроблена система перевірки параметрів безпеки серверів і мережевого обладнання. Система складається з трьох компонентів:

1. Nessus-сервер – програма для автоматичного пошуку відомих дірок в захисті інформаційних систем;

2. Плановик завдань, який безпосередньо виконує перевірку серверів і мережевих служб, запускає клієнт Nessus з заданими параметрами за розкладом;

3. База даних «Безпека» (Lotus Domino) є сховищем сканера Nessus з відстеженням появи та усунення критичних вразливостей на серверах, які скануються. База налагоджена таким чином, що при виявлені критичних вразливостей автоматично надсилає повідомлення з описом і рекомендаціями співробітнику відповідальному за супроводження даного сервера.

Використання даного комплексу дозволяє проводити аналіз захищеності систем та вузлів мережі, прогнозувати появу порушень безпеки, контролювати процес усунення виявлених вразливостей.

Cacti – веб-додаток, який дозволяє будувати графіки за допомогою RRDtool. Cacti збирає статистичні дані за певний інтервал часу і відображає їх у графічному виді. Переважно використовуються стандартні шаблони для відображення статистики щодо завантаженості процесора, надання оперативної пам’яті, кількості запущених процесів, використання вхідного/вихідного трафіка каналів зв’язку.

Дане програмне забезпечення використовується для контролю завантаженості та кількості помилок каналів зв’язку в мережі передачі даних (виділених аналогових, супутникових каналів, волоконно-оптичних ліній зв’язку).

Диспетчерська система NetWatch – це засіб управління з веб-інтерфейсом, який надає можливість контролю стану мережевих пристроїв у форматі, що відповідає вимогам усіх рівнів технічної компетенції.

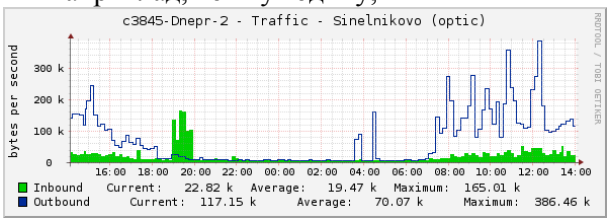
Унікальний інтерфейс Netwatch представляє новий функціональний рівень управління мережею і виконує огляд мережевих ресурсів з використанням інтернет-технологій. Висококласна презентаційна складова продукту дозво-

ляє більш широкій аудиторії спостерігати і оцінювати стан мережі та параметри, з якими вона працює. Замість надання технічно-орієнтованих графіків і діаграм Netwatch представляє інформацію у зручному форматі, зображаючи мережу у вигляді зрозумілої схеми, з нескладним доступом до додаткової інформації. Система дозволяє легко інтегрувати звіти, набори даних та компоненти інших управляючих систем.

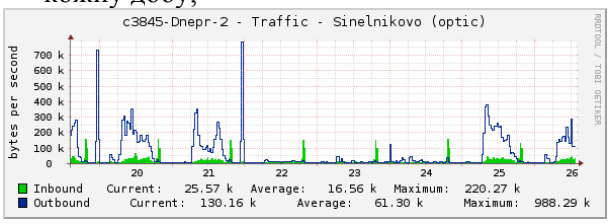
Набір перелічених програмних продуктів використовується для побудови системи контролю якості каналів зв'язку, їх завантаженості, доступності вузлів мережі передачі даних. На базі даної системи створено web-портал, з розділами, які контролюють стан основних вузлів мережі та каналів зв'язку, компонентів мережі щодо кожної станції. Для контролю рівня помилок та стану резервних виділених аналогових каналів зв'язку створені розділи порталу для кожної дирекції залізниці, які виконують цей контроль спільно з програмним забезпеченням Cacti.

NetFlow Tracker – це програмне рішення для збору та аналізу NetFlow-інформації, яку надає обладнання Cisco. Програмне забезпечення встановлюється на сервері і дозволяє акумулювати дані, а також надавати звіти про мережевий трафік в реальному масштабі часу (до 14 діб), та забудь-який період часу з різним рівнем деталізації (від 1 хвилини).

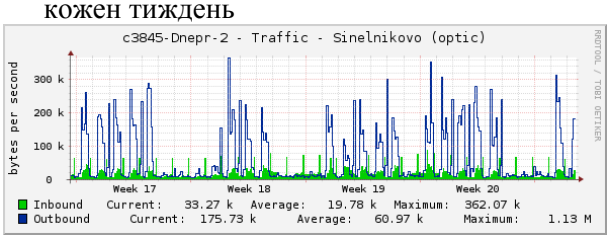
Наприклад, кожну годину,



кожну добу,



кожен тиждень



NetFlow Tracker використовується в корпоративні мережі Придніпровської залізниці для збору деталізованої статистики щодо трафіка маршрутизаторів Cisco в найбільш важливих вузлах мережі передачі даних (Дніпропетровськ, Кривий Ріг Головний, Запоріжжя, Сімферополь, Джанкой) в безперервному режимі. При необхідності є можливість проведення тимчасового контролю інших вузлів мережі, їх більше 100, у разі зниження якості передачі даних в мережі.

Використання програмного рішення NetFlow Tracker разом з ПЗ NetWatch дозволило підняти рівень контролю інформації, яка передається в мережі передачі даних, на якісно новий рівень і значно скоротити час на визначення причин порушення нормальної її роботи. Це дає можливість підвищити надійність функціонування мережі передачі даних разом з резервування обладнання у вузлах [1].

Незважаючи на порівняно нетривалий термін експлуатації даного програмного забезпечення, його ефективність вже підтверджена у випадках виявлення причин збоїв в роботі мережі та їх усунення. Більш того, функціональні можливості NetFlow Tracker дозволяють проводити налагодження оперативного контролю та журналу повідомлень, якщо кількість небажаної або неслужбової інформації перевищить рівень, визначений адміністративною політикою. Це дає можливість здійснювати контроль активності та знаходити її джерело навіть в тих випадках, коли після її виникнення пройшов досить значний час.

Microsoft System Center Configuration Manager 2007- програмний пакет для керування IT-ресурсами підприємства (серверами та робочими станціями під управлінням операційних систем Windows).

Основні можливості: інвентаризація програмного та апаратного забезпечення; розповсюдження програмного забезпечення; управління оновленнями операційних систем та прикладного програмного забезпечення; оцінка вразливості клієнтів; моніторинг використання програмного забезпечення; віддалене управління; розгортання образів операційних систем; управління мобільними пристроями; управління гетерогенними системами.

Важливість даного програмного пакета важко перебільшити, тому що у поточний час кількість робочих станцій, що підключені до мережі, обчислюється тисячами, і вона неухильно зростає.

Використання розглянутих програм дозволяє не тільки оперативно усувати збої у функціонуванні інформаційних систем, а також і запобігати їх виникненню.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Івченко, Ю. М. Інтеграція мережевого обладнання АСК ВП УЗ та АСК ПП УЗ, підключення його до ЄМПД [Текст] / Ю. М. Івченко, В. Г. Івченко, О. М. Гондар // Вісник Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна. - Вип. 29. – Д. : Вид-во Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазаряна, 2009. – С. 143–146.
2. Ивченко, Ю. Н. Система мониторинга информационной сети Приднепровской ж.д. [Текст] / Ю. Н. Ивченко, В. Г. Ивченко, О. Г. Гондар // Тези доп. Міжн. наук-практ. конф. «Сучасні інформаційні технології на транспорті, в промисловості та освіті» (13–14.05.2010 р., Дніпропетровськ). – Д., 2010. – С. 12–13.

Надійшла до редколегії 02.09.2011.
Прийнята до друку 05.09.2011.

Ю. Н. ИВЧЕНКО, В. Г. ИВЧЕНКО, О. Н. ГОНДАР

СИСТЕМА МОНИТОРИНГА КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ

В статье оценена опасность сбоев сервисов и служб корпоративной информационно-телекоммуникационной системы Приднепровской ж.д., важности осуществления постоянного контроля функционирования основных компонентов системы. Предложены классификация компонентов системы по категориям, в зависимости от функционального назначения, и программное обеспечение для контроля компонентов каждой категории.

Ключевые слова: мониторинг корпоративной информационной сети.

YURIY IVCHENKO, VALENTINA IVCHENKO, OLEG GONDAR

SYSTEM OF MONITORING OF THE CORPORATE INFORMATIVE SYSTEM

The danger of failures of services and services of the corporate informatively-telecommunication system of Pridneprovskoy railway is appraised in the article., to importance of realization of permanent control of functioning of basic components of the system. Offered classification of components of the system on categories, depending on the functional setting, and software for control of components of every category.

Keywords: monitoring of corporate informatively network.