ISSN 2411-1031. Information Technology and Security. January-June 2016. Vol. 4. Iss. 1 (6)

УДК 004.056.53

ОЛЕКСІЙ МІСНІК,
МИХАЙЛО АНТОНІШИН

СИСТЕМА МОНІТОРИНГУ ДОСТУПНОСТІ ДЕРЖАВНИХ ВЕБ-РЕСУРСІВ

Постійне підвищення ролі інформаційних технологій призводить до відмовляння від традиційного документообігу на користь електронного. Зі зростом його обсягів зростає і зацікавленість електронними документами з боку різноманітних осіб і численних хакерських угруповань, спецслужб інших країн. Найбільшого деструктивного впливу зазнають державні веб-ресурси. Для унеможливлення такого впливу забезпечується непорушність насамперед їх цілісності та доступності. Для постійного контролювання доступності державних веб-ресурсів пропонується система моніторингу на основі рішення Nagios. Тоді як процес пошуку доменних імен державних веб-ресурсів автоматизовано за допомогою скриптової мови програмування Bash. Завдяки цьому стало можливим забезпечення постійного контролювання доступності державних веб-ресурсів і швидке інформування про початок атаки на них або їх технічні несправності.

Ключові слова: інформація, доступність, веб-ресурс, програмне забезпечення, моніторинг, система моніторингу, Nagios.

Постановка проблеми. Сучасний світ характеризується постійним підвищенням ролі інформаційних технологій. Все більше інформації зберігається в електронному вигляді. Багато організацій, а іноді навіть цілі країни, відмовляються від традиційного документообігу на користь електронного. Тому зі зростом обсягів ”електронних” документів зростає і зацікавленість ними з боку різноманітних осіб і численних хакерських угруповань, спецслужб інших країн. Зокрема, найбільшого деструктивного впливу зазнають державні веб-ресурси. Для унеможливлення такого впливу забезпечується непорушність насамперед їх цілісності та доступності. Зокрема, постійне контролювання доступності державних веб-ресурсів здійснюється шляхом впровадження нових комплексних підходів [1-9]. Їх використання дозволяє забезпечити, по-перше, постійний моніторинг доступності державних веб-ресурсів; по-друге, швидке інформування про початок атаки або технічні несправності; та, по-третє, обробляння великого обсягу вхідних даних за результатами моніторингу. Це досягається завдяки розробленню та впровадженню систем моніторингу доступності державних веб-ресурсів.

Аналіз останніх досліджень і публікацій. Системи моніторингу доступності державних веб-ресурсів досліджуються в [1-5]. Зокрема, в [2] виконано їх порівняння за сформованими ознаками. При цьому не враховуються важливі для функціонування таких системи критерії стабільності їх роботи (функціонування, експлуатування) та швидкості конфігурування [2, 3, 5]. Водночас відсутні настанови щодо вибору програмного забезпечення таких систем і, як наслідок, виокремлення серед них кращих і гірших [2, 3, 5, 6-9].

Тому **метою даної роботи** є підвищення оперативності реагування на втрату доступності державного веб-ресурсів завдяки розробленню системи їх моніторингу.

Виклад основного матеріалу дослідження. Доступ до державних веб-ресурсів здійснюється громадянами в будь-який час. При цьому забезпечується непорушність властивості доступності. Для своєчасного реагування на втрату означеної властивості пропонується система моніторингу доступності державних веб-ресурсів. Означена система орієнтована на вирішення таких завдань:

- визначення початку атаки ”відмова в обслуговуванні”;
- відображення технічних проблем серверів на яких функціонує веб-ресурс;
- відображення проблем програмного наповнення веб-ресурсу.

В усіх випадках виникають проблеми зі забезпеченням доступності державних веб-ресурсів. Тому виокремимо випадки порушення означеної властивості, а саме [1-5]:

1. Атака на відмову в обслуговуванні (Denial of service attack) [4] або розподілена атака на відмову в обслуговуванні (Distributed Denial Of Service Attack, DDOS) – це атаки на державний веб-ресурс з метою унеможливити його доступність.

Одним із найпоширеніших методів даного типу атак є насичення ”жертви” великою кількістю зовнішніх запитів (часто “безглуздих” або ”неправильно сформованих”). Таким чином “жертва” не може відповісти на запити користувачів, або відповідає настільки повільно, що стає фактично недоступною. В кінцевому випадку це призводить до відмови державного веб-ресурсу через:

− припинення роботи програмних засобів або до витрати фізичних ресурсів, та, як наслідок, припинення роботи апаратних засобів;

− зайняття каналів зв’язку між користувачами та ”жертвою”, внаслідок цього якість зв’язку перестає відповідати вимогам.

Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою. DDoS-атаки поділяються на локальні та віддалені [1, 4]. До локальних відносяться форк-бомби та програми, що відкривають велику кількість файлів або можуть ініціалізувати циклічні алгоритми. Це призведе до значних витрат обчислювальних ресурсів.

Віддалені DDoS-атаки поділяються на два види [1]:

− віддалена експлуатація помилок в програмному забезпеченні з метою доведення його до неробочого стану;

− Flood – надсилання на адресу ”жертви” великої кількості безглуздих (рідше, осмислених) пакетів.

Метою флуду може бути канал зв’язку або ресурси персонального комп’ютера. У першому випадку потік пакетів займає усю смугу пропускання і не дає ”жертві” можливості обробляти легальні запити. У другому – ресурси персонального комп’ютера захоплюються за допомогою багаторазового і дуже частого звернення до якого-небудь сервісу, що виконує складну, ресурсоємну операцію. Це може бути, наприклад, тривале звернення до одного з активних компонентів (скрипту) веб-сервера. Сервер витрачає всі ресурси на оброблення запитів, що атакують, а користувачам доводиться очікувати на обслуговування [1, 4-5].

Нині в традиційному виконанні (один ”атакуючий” – одна ”жертва”) залишається ефективним лише перший вид атак. Класичний flood неефективний тому, що при сьогоднішній ширині смуги пропускання, рівні обчислювальних потужностей і розповсюдженому використанні різних анти-DoS прийомів у програмному забезпеченні (наприклад, затримки при багаторазовому виконанні типових дій одним клієнтом), ”атакуючий” не здатний завдати будь-якого збитку. Але якщо ”атакуючих” наберуться сотні, то внаслідок їх дій сервер стане недоступним [2-5].

Розподілена атака типу ”відмова в обслуговуванні” (DDoS), зазвичай здійснюється за допомогою великої кількості ”зомбованих” машин, може призводити до унеможливлення доступу до, навіть, найстійкіших серверів. Тому єдиним ефективним захистом при цьому є організація розподіленої системи серверів (кластера).

Існують два варіанти такої організації DDoS атак [1]:

− ботнет – зараження певного числа комп’ютерів програмами, які в певний момент часу починають здійснювати запити до сервера, що атакується.

− флешмоб – домовленість великої кількості користувачів мережі Інтернет почати здійснювати певні типи запитів до сервера, що атакується.

Небезпека більшості DDoS-атак – в їх абсолютній прозорості та ”повсякденності”. Адже якщо помилка в програмному забезпеченні завжди може бути виправлена, то повна витрата ресурсів – явище майже буденне. З ним стикаються багато адміністраторів, коли ресурсів машини (смуги пропускання каналу) стає недостатньо, або веб-сайт піддається следшот-ефекту. І, якщо обмежувати потік даних і ресурси для всіх користувачів, то можна врятуватися від DDoS, але у той же час, втратити велику частину користувачів.

2. Серверні приміщення, окрім власного обчислювального устаткування, відображаються сукупністю інженерних систем – канали зв'язку, електроживлення, охолодження, пожежогасіння, контроль доступу та інше. Несправності можуть виникати в будь-якій з цих підсистем, і бути, наприклад, причиною каскаду несправностей в інших, залежних підсистемах. Також чималу частку збоїв викликає "людський фактор".

Можливі технічні проблеми серверів на платформі яких функціонує веб-ресурс, а саме:

- вихід з ладу жорсткого диску та блоку живлення;
- виведення з ладу RAID контролерів;
- виведення з ладу електронних компонентів: процесорів, системних плат, модулів пам'яті, материнської плати;
- перегрів серверу з причини виведення з ладу вентиляторів;

3. Програмні проблеми, що призводять до непрацездатності сервера:

- помилки у роботі веб-ресурсу, що носять "серверний" характер. Наприклад: "503", "504", "413";
- використання не стабільних версій програмного забезпечення;
- не правильне конфігурування сервісів.

З огляду на це проведемо оцінку їх функціоналу для визначення системи, яка задовольнятиме встановленим потребам (див., наприклад [6-9], табл. 1). Системи моніторингу існують на ринку телекомунікацій багато років і стрімко розвиваються з розвитком галузі в цілому. Запропоновані системи моніторингу схожі за функціям, надають майже однаковий мінімальний набір можливостей [1-9]:

- моніторинг мережі;
- групування пристроїв мережі;
- автоматичне виявлення загроз;
- гнучке конфігурування сервісів;
- візуалізування даних і доступ через веб-інтерфейс;
- події та реакція на них у вигляді оповіщень та виконання команд;
- можливість розширення існуючої функціональності через додаткові плагіни;
- зберігання конфігурації та історії моніторингу в БД;
- створення карт мережі і керування доступом.

Найбільш функціональними є системи моніторингу, порівняння яких представлено в табл. 1.

Таблиця 1 – Порівняння систем моніторингу доступності веб-ресурсу

Назва	Діаграми	Мова	Агент	SNMP	Метод зберігання даних	Текстові конфігураційні файли
Cacti	Так	PHP	Ні	Так	RRDtool, MySQL, PostgreSQL	НІ
Nagios	Так	C	Так	Плагін	MySQL	Так
Zabbix	Так	Java	Підтри мується	Так	Oracle, MySQL, PostgreSQL, IBM DB2, SQLite	Ні
NOC	Так	Python	Так	Так	PostgreSQL, MongoDB	Ні

Як бачимо з табл. 1, існують системи моніторингу як з відкритим кодом, так і платні, що програмуються мовами C, Java, Python і PHP. Разом з тим, для моніторингу доступності державних веб-ресурсів обрано систему контролювання стану обчислювальних вузлів і служб – Nagios (див. рис. 1). Це обумовлено такими перевагами [7]:

- налаштування зберігаються у файлах конфігурації;
- простий формат файлу. Можливо легко конфігурувати з використанням будь-яких самописних утиліт;
- велика кількість плагінів для розширення функціоналу;

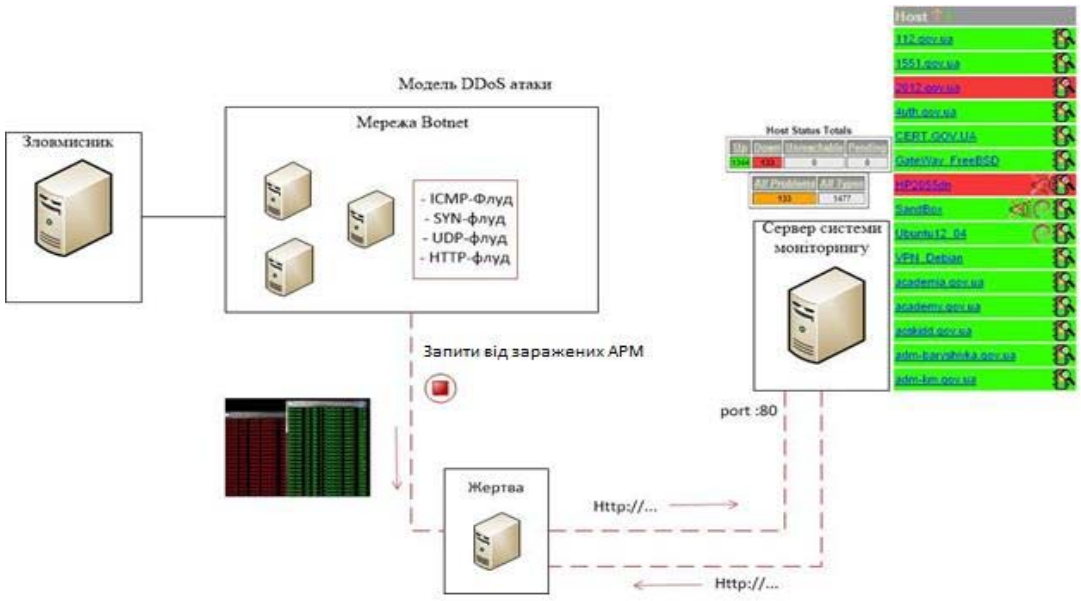

Рисунок 1 – Робота системи моніторингу

Водночас побудова системи моніторингу доступності державних веб-ресурсів пов'язана з такими складнощами конфігурування [2]:

- відсутність офіційного переліку державних веб-ресурсів;
- велика кількість не працюючих доменних імен;
- поява нових домен імен, інформація про які нікому не відома.

Ці складнощі дозволяє подолати використання системи моніторингу Nagios. Зокрема, на її основі налагоджено моніторинг доступності державного домену gov.ua. При цьому процес пошуку доменних імен державних веб-ресурсів було автоматизовано за допомогою скриптової мови програмування Bash. Знайдено більше 3000 доменів державних веб-ресурсів, але більше 1000 з них були непрацездатні або не несли ніякої інформації для користувача [2-5]. Тому перед створення конфігураційного файлу введено перевірку на працездатність веб-ресурсів і тільки після цього проходить створення конфігураційного файлу. Скрипти автоматизації вище викладеного алгоритму з описом роботи функцій.

Даний код виконує пошук державних доменів веб-ресурсів:

Лістинг 1

```
v="$(theharvester -d gov.ua -l 200 -b all)"
echo "$v" > harvesting_result
o="$( cat harvesting_result | sed '1,/----------/ d' )"
echo "$o" > harvesting_result_redaction1
```

Наступний код фільтрує знайдені домени та видаляє повторні записи.

Лістинг 2

```
cat harvesting_result_redaction1 | grep gov.ua | sed 's/ /\n/g' | grep gov.ua | sed 's/\t/\n/g' | sed 's/:/\n/g' | grep gov.ua | grep -v "@" | grep -v "href" | grep -v "value" | tr -d \" | tr -d \' | sed 's|.*\/||' | sed -r 's/\/.+//' | tr -d \/ | sort -u > harvesting_result_redaction2
cat all_domains harvesting_result_redaction2 | sort  | uniq | tr '[A-Z]' '[a-z]' | uniq
```

Цим фрагментом коду відображається створення файлу, що містить знайдені домени державних веб-ресурсів:

Лістинг 3

```
sort harvesting_result_redaction2 > harvesting_result_redaction2.sort
sort all_domains > all_domains.sort
comm -13 all_domains.sort harvesting_result_redaction2.sort > newdomains
```

Для створення конфігураційного файлу потрібно відібрати тільки працюючі домени, тому використовується команда перевірки знайдених доменних імен на працездатність:

curl -Is http://cert.gov.ua | head -1

Усіма доменами повертається відповідь, що записується у файл робочих доменів

HTTP/1.1 200 OK

Даний код показує, як проходить створення хостового конфігураційного файлу системи моніторингу доступності державних веб-ресурсів

Лістинг 4

```
define host{
    use                 generic-host_http
    host_name               a@a
    alias                 a@a
    address                 a@a
    contact_groups          admin_gov
    }
```

Після створення конфігураційного файлу потрібне перезавантаження системи моніторингу, для впровадження змінених конфігураційних файлів у роботу (див. рис. 2).

service nagios3 restart

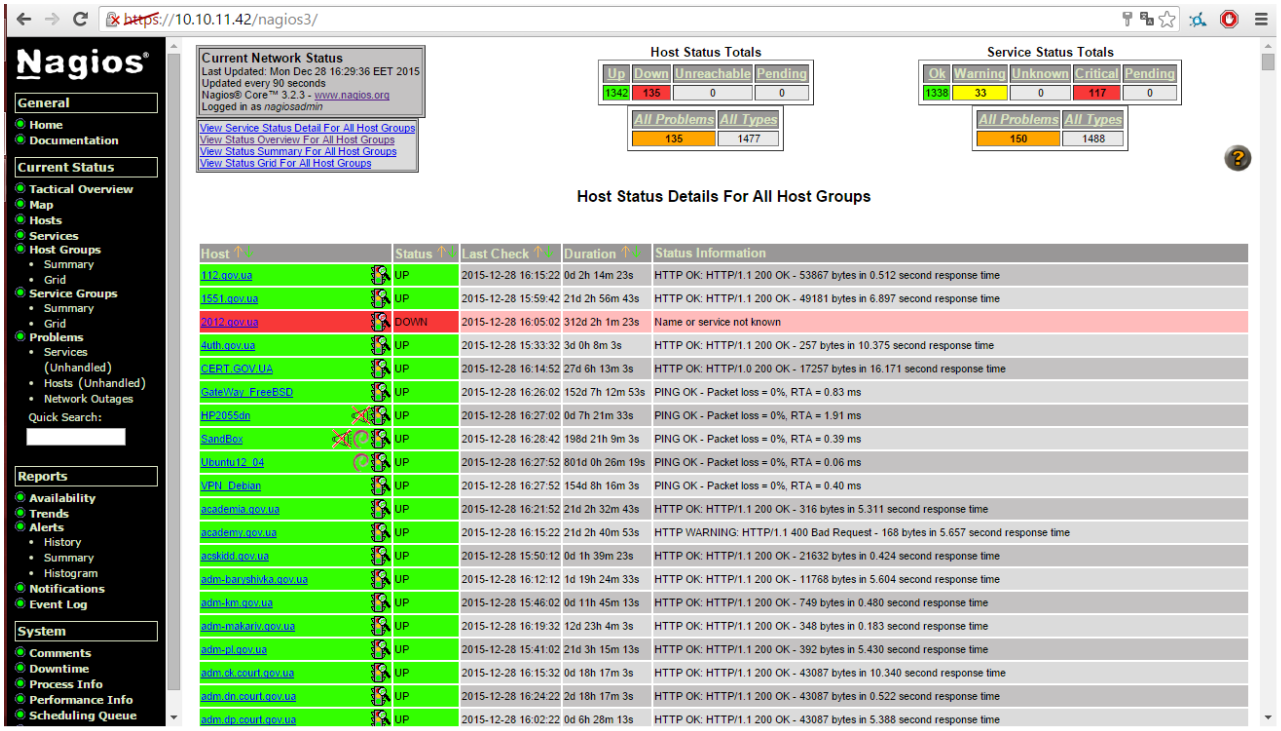

Рисунок 2 – Робота системи моніторингу доступності веб-ресурсів [7]

При втраті доступності державного веб-ресурсу системному адміністратору надсилається повідомлення про стан ресурсу (див. рис. 3).

Рисунок 3 – Приклад відображення відомостей про стан державних веб-ресурсів

Висновки. Розроблено систему моніторингу державних веб-ресурсів на основі рішення Nagios. Зокрема, забезпечено контролювання доступності домену gov.ua. При цьому процес пошуку доменних імен автоматизовано за допомогою скриптової мови програмування Bash. Знайдено більше 3000 доменів державних веб-ресурсів. Однак, більше 1000 з них були непрацездатні або не несли ніякої інформації для користувача. Тому створенню конфігураційного файлу передує введення перевірки працездатності веб-ресурсів. Завдяки цьому забезпечено, по-перше, постійний моніторинг доступності державних веб-ресурсів; по-друге, швидке інформування про початок атаки або технічні несправності; та, по-третє, обробляння великого обсягу вхідних даних за результатами моніторингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] DoS-атака. [Електронний ресурс]. Доступно: https://ru.wikipedia.org/wiki/DoS-атака. Дата звернення: Лют. 3, 2016.

[2] О. С. Высочина, С. И. Шматков, и А.М. Салман, “Анализ систем мониторинга телекоммуникационных сетей”, *Радіоелектроніка, інформатика, управління,* № 2 (23), с. 139-142, 2010.
doi: 10.15588/1607-3274-2010-2-24.

[3] Ю.М. Івченко, В.Г. Івченко, та О.М. Гондар, “Система моніторингу корпоративної інформаційної мережі”, *Вісник Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна*, вип. 36, с. 171-174, 2011.

[4] “DDoS в 100 Гбит/с – репортаж с линии фронта от очевидца”. [Электронный ресурс]. Доступно: http://blogerator.ru/page/ddos-v-100-gbits-reportazh-s-liniifronta-ot-ocevidca. Дата обращения: Янв. 10, 2016.

[5] В. Кордяк, І. Дронюк, та О. Федевич, “Інформаційна технологія моніторингу та аналізу трафіку у комп’ютерних мережах”, *Вісник Національного університету ”Львівська політехніка”. Серія: Комп’ютерні науки та інформаційні технології*, № 826, с. 35-42, 2015.

[6] Zabbix. [Online]. Available: www.zabbix.org. Accessed on: Dec. 15, 2015.

[7] Nagios is the industry standard in IT infrastructure monitoring. [Online]. Available: www.nagios.org. Accessed on: Dec. 15, 2015.

[8] Cacti. [Online]. Available: www.cacti.net. Accessed on: Dec. 15, 2015.

[9] NOC. [Online]. Available: kb.nocproject.org. Accessed on: Dec. 15, 2015.

Стаття надійшла до редакції 18 лютого 2016 року.

REFERENCE

[1] DoS-attack. [Online]. Available: https://ru.wikipedia.org/wiki/DoS-атака. Accessed on: Febr. 3, 2016.

[2] O.S. Vysochina, S.I. Shmatkov, and A.M. Salman, “Analysis of telecommunications networks monitoring systems”, *Radio Electronics, Computer Science, Control,* no. 2 (23), pp. 139-142, 2010.
doi: 10.15588/1607-3274-2010-2-24.

[3] Y.M. Ivchenko, V.H. Ivchenko, and O.M. Hondar, “The monitoring system of corporative informational net”, *Bulletin of Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan*, iss. 36, pp. 171-174, 2011.

[4] “DDoS 100 GigaBit - report from the front lines of the witness”. [Online]. Available: http://blogerator.ru/page/ddos-v-100-gbits-reportazh-s-liniifronta-ot-ocevidca. Accessed on: Jan. 10, 2016.

[5] V. Kordyak, V. Dronyuk, A. Fedevych, “Information technology monitoring and traffic analysis in computer networks”, *Bulletin of Lviv Polytechnic National University. Series ”Computer Sciences and Information Technologies”*, no. 826, pp. 35-42, 2015.

[6] Zabbix. [Online]. Available: www.zabbix.org. Accessed on: Dec. 15, 2015.
[7] Nagios is the industry standard in IT infrastructure monitoring. [Online]. Available: www.nagios.org. Accessed on: Dec. 15, 2015.
[8] Cacti. [Online]. Available: www.cacti.net. Accessed on: Dec. 15, 2015.
[9] NOC. [Online]. Available: kb.nocproject.org. Accessed on: Dec. 15, 2015.

АЛЕКСЕЙ МИСНИК,
МИХАИЛ АНТОНИШИН

СИСТЕМА МОНИТОРИНГА ДОСТУПНОСТИ ГОСУДАРСТВЕННЫХ ВЕБ-РЕСУРСОВ

Постоянное повышение роли информационных технологий приводит к отказу от традиционного документооборота в пользу электронного. С ростом его объемов растет и заинтересованность электронными документами со стороны разнообразных лиц и многочисленных хакерских группировок, спецслужб других стран. Наибольшее деструктивное влияние испытывают государственные веб-ресурсы. Для того чтоб сделать невозможным такое влияние обеспечивается сохранность в первую очередь их целостности и доступности. Для постоянного контролирования доступности государственных веб-ресурсов предлагается система мониторинга на основе решения Nagios. Тогда как процесс поиска доменных имен государственных веб-ресурсов автоматизируется с помощью скриптового языка программирования Bash. Благодаря этому стало возможным обеспечение постоянного контролирования доступности государственных веб-ресурсов и быстрое информирование о начале атаки на них или быстрое выявление их технических неисправностей.

Ключевые слова: информация, доступность, веб-ресурс, программное обеспечение, мониторинг, система мониторинга, Nagios.

OLEKSII MISNIK,
MYKHAILO ANTONISHYN

AVAILABILITY GOVERNMENT WEB RESOURCES MONITORING SYSTEM

The constant increase in the role of information technology leads to the denial of the traditional paper workflow for electronic. With the increase used of electronic documents increases and interest for this electronic documents from various people and many hacker groups, also the intelligence services of other countries. The most destructive influence befalls government web-resources. To prevent such exposure is provided primarily inviolability of their integrity and availability. To control the accessibility government web resources used monitoring systems. However, there are no guidelines for the selection of software systems and, consequently, the isolation of their best and worst. Therefore, constant monitoring the availability of government web resources offered to carry through the development of monitoring systems based solution Nagios. This is due to the ability to store settings in configuration files, a simple file format, ease of configuration using any recording tools, and lots of plugins to extend functionality. The process of finding domain names government web resources using automated scripting language Bash. This system is aimed at solving such problems as the definition of early attacks “denial of service” display technical problems on servers which operate a Web resource; mapping software problems working web resource. This will be possible to ensure continuous monitoring of the availability of government web resources and quick information about the beginning of an attack on them or their technical malfunction.

Keywords: information, availability, web resource, software, monitoring, monitoring system, Nagios.

Олексій Ігоревич Міснік, аспірант, Державний заклад “Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут”, Київ, Україна.
E-mail: alexmisnik91@gmail.com.

Михайло Васильович Антонішин, інженер, Національний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації, Київ, Україна.
E-mail: antonishin.mihail@gmail.com.

Алексей Игоревич Мисник, аспирант, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.
Михаил Васильевич Антонишин, инженер, Национальный центр киберзашиты Государственной службы специальной связи и защиты информации, Киев, Украина.

Oleksii Misnik, postgraduate student, State institution "Institute of special communication and information protection of National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.
Mykhailo Antonishyn, engineer, National cyber centre of the State service of special communication and information protection of Ukraine, Kyiv, Ukraine.