

# Перспективи Розвитку та Вдосконалення Розподіленої Системи Моніторингу Державних Інформаційних Ресурсів

Надія Казакова, Олексій Фразе-Фразенко  
кафедра комп'ютерних та  
інформаційно-вимірювальних технологій  
Одеська державна академія технічного  
регулювання і якості  
Одеса, Україна  
kaz2003@ukr.net

Іван Копиченко  
Фонд Східна Європа  
Одеса, Україна  
ikopychenko@egap.in.ua

## Perspectives of Development and Improvement of Distributed Monitoring System of the State Information Resources

Nadiia Kazakova, Oleksii Frazhe-Frazenko  
dept. of computer, information  
and measurement technologies  
Odesa State Academy of Technical Regulation and Quality  
Odesa, Ukraine  
kaz2003@ukr.net

Ivan Kopychenko  
Eastern Europe Foundation  
Odesa, Ukraine  
ikopychenko@egap.in.ua

*Анотація*—У межах вирішення проблеми підвищення ефективності розгалужених систем електронного урядування розглянуті питання впровадження систем централізованого моніторингу ресурсів та активів інформаційної інфраструктури. Окреслені ключові заходи щодо розвитку національної системи електронного документообігу, наведено аналіз особливостей та пропозиції впровадження сучасних систем моніторингу для підвищення рівня захищеності систем електронного урядування. З метою запобігання зміні структурованих даних подій, що містяться в базі даних системи моніторингу, запропоновано використовувати технологію Blockchain. Показано актуальність використання наведених технологій для підвищення ефективності функціонування систем електронної взаємодії органів виконавчої влади.

*Abstract*—Within a solution of the problem of increase in efficiency of branched electronic control systems questions of the information infrastructure resources and assets centralized monitoring systems implementation of are considered. The main priority directions and perspectives of electronic control and electronic democracy development in Ukraine are given. Key

actions for development of national electronic document management system are specified, the analysis of features and the sentence of modern monitoring systems implementation for increase in level of systems of electronic control security is provided. It is noted that efficiency of response to any events found by a monitoring system including incidents of information security, now more depends on quality of expert evaluation that allows to speak about need of further automation and adaptation to events which has to simplify acceptance process the decision by the administrator. For the purpose of structured data change prevention of the incidents which are contained in the monitoring system database it is offered to use Blockchain technology. Relevance of the specified technologies use for increase in efficiency of executive authorities interaction electronic systems functioning is shown.

*Ключові слова*—інформація; електронний документообіг; моніторинг, автоматизація; державний інформаційний ресурс, інформаційна безпека

*Keywords—information; electronic document flow; monitoring; automation; state information resource; information security, executive authorities; blockchain; electronic democracy.*

## I. ВСТУП

Одним із головних питань підвищення ефективності державного управління в Україні є удосконалення впроваджених у цей процес сучасних інформаційних систем, що забезпечують електронну взаємодію органів виконавчої влади та моніторинг коректності функцій управління підпорядкованими об'єктами.

Враховуючи складність програмно-апаратного забезпечення систем електронної взаємодії ієрархічних компонентів системи управління, автоматизовані системи повинні забезпечувати централізований моніторинг параметрів, що впливають на виникнення неприпустимих помилок у процесі обміну даними між керуючими суб'єктами.

Виходячи зі сказаного, метою досліджень, пов'язаних із підвищенням ефективності державного управління в Україні є пошук шляхів удосконалення сучасних автоматизованих систем на основі впровадження до їх архітектури нових функцій моніторингу параметрів, на основі яких оцінюється коректність виконання функцій управління.

## II. ОСНОВНА ЧАСТИНА

В 2016-2017 роках урядом України в якості пріоритету розвитку держави як сучасної Європейської країни був обраний розвиток електронного урядування та електронної демократії. Серед них можна виділити наступні напрямки:

- модернізація публічних послуг (впровадження нових та оптимізація вже існуючих електронних адміністративних послуг, інструменти електронної ідентифікації, залучення громадян та розвиток відкритих даних);
- управління розвитком е-урядування (базова IT-інфраструктура, ефективне управління);
- модернізація публічного управління (електронна взаємодія реєстрів, електронний документообіг, е-урядування базовими галузями).

За минулий рік Україна зробила великий прорив у питаннях розвитку правових засад стосовно інструментів електронного урядування та їх використання. Протягом 2017 року активно розвивалось підґрунтя для вирішення проблеми електронної взаємодії державних реєстрів, а саме було:

- проведено аудит державних електронних інформаційних ресурсів;
- розроблено дорожню карту інтероперабельності даних до 2020 року;
- впроваджено систему електронної взаємодії державних електронних інформаційних ресурсів (Трембіта), створеної на базі естонської системи X-Road;

- розроблено порядок організації електронної взаємодії державних електронних інформаційних ресурсів.

Наступною, але не менш значимою подією для України став розвиток та модернізація національної системи електронного документообігу, основна мета якої полягає в оптимізації міжурядової взаємодії та зменшити час на обробку документів держслужбовцями.

Серед ключових заходів, щодо розвитку національної системи електронного документообігу можна виділити наступні:

- запровадження електронного документообігу в системі центральних органів виконавчої влади, обласних державних адміністрацій, деяких районних державних адміністрацій та державних підприємств стратегічного значення;
- прийняття постанови Кабінету Міністрів України від 18.08.2017 №608 «Деякі питання підготовки проектів актів законодавства в електронній формі»;
- розроблено інструкцію щодо документування управлінської інформації в електронній формі та організації роботи з електронними документами;
- модернізовано системи електронного документообігу в пілотних центральних органах виконавчої влади в рамках реформи державного управління.

Відповідно до даних, наведених у Звіті Голови Державного агентства з питань електронного урядування за 2017 рік, бюджет, виділений на розвиток системи електронної взаємодії державних інформаційних ресурсів в 2018 році виріс в 2 рази, порівняно із минулим роком, а бюджет на систему електронної взаємодії органів виконавчої влади – майже в 6 разів.

Все це говорить про те, що на сьогодні в Україні актуальним є підвищення якості інструментів інформаційних систем для використання у роботі державних органів та приватних підприємств. З цієї причини великого значення набувають теоретичні та прикладні розробки в напрямку вдосконалення Системи електронної взаємодії органів виконавчої влади, зокрема, створення та оптимізація роботи підсистеми моніторингу шляхом впровадження відповідних технологій у якості додаткового функціоналу.

Далі слід розглянути особливості та пропозиції впровадження сучасних систем моніторингу для підвищення рівня захищеності систем електронного урядування.

Одним з головних питань в цьому процесі є організація процесу моніторингу компонентів, що використовуються під час роботи систем електронної взаємодії з метою підвищення ефективності їх роботи[1].

Враховуючи складність використовуваного програмно-апаратного забезпечення систем електронної взаємодії імовірність виникнення непоміченої критичної помилки є

великою. Саме тому в системі має бути реалізований центральний моніторинг, який має представляти комплексне рішення, яке поєднує у собі легку масштабованість, продуктивність та зручність використання [2].

До основних задач, які покладаються на систему централізованого моніторингу системи електронної взаємодії належать [1]:

- моніторинг мережі і додатків;
- виявлення проблем із віртуалізацією та операційними системами;
- аналіз мережевих проблем;
- аналіз захоплених даних додатків і потоків;
- пошук кореневої причини інциденту або проблеми.

Для ефективною реалізації викладених вище задач програмне забезпечення, яке реалізує функціонал системи центрального моніторингу, повинно надавати інструменти: збирання даних; сповіщення про події; зберігання даних; візуалізації.

Збирання даних може бути реалізовано за допомогою протоколу SNMP (SimpleNetworkManagementProtocol, простий протокол мережевого управління), агентів моніторингу та інтелектуального інтерфейсу IPMI.

За допомогою протоколу SNMP також можна стежити за станом апаратних засобів, включаючи блоки живлення, вентилятори, використання пам'яті тощо. Моніторинг за протоколом SNMP не потребує встановлення на об'єкті, який підлягає контролю, додаткового програмного забезпечення. Для моніторингу достатньо щоб пристрій підтримував протокол SNMP.

Метод використання агентів моніторингу дозволяє збирати більш розширене коло відомостей. Однак цей метод вимагає встановлення спеціального програмного забезпечення, яке реалізує функціонал агента.

IPMI (IntelligentPlatformManagementInterface) – це інтелектуальний інтерфейс управління платформою, який призначений для автономного моніторингу та управління функціями, вбудованими безпосередньо в апаратне і вбудоване програмне забезпечення серверних платформ.

Система моніторингу повинна здійснювати сповіщення адміністратору про події. Зберігання даних призначено для накопичення відомостей про події з метою їх подальшого аналізу.

Візуалізація потрібна для зручної обробки даних моніторингу адміністратором та передбачає наявність графічного інтерфейсу.

На сьогодні у світі наявна велика кількість платних та безкоштовних систем моніторингу. До найбільш відомих відносяться: Cacti, GFI Webmonitor, Nagios, Naumen Network Manager, Zabbix. У [3, 4] наведено порівняння особливостей використання деяких з цих систем. З урахуванням визначених технологій та методів, доцільним

буде розглянути передумови використання саме системи Zabbix для вирішення завдань, поставлених за мету даного дослідження.

Zabbix надає широкую множину функцій для здійснення якісного моніторингу, зокрема:

- централізований та простий у використанні веб-інтерфейс;
- система працює на більшості UNIX-подібних операційних системах, включаючи Linux, AIX, FreeBSD, OpenBSD та Solaris;
- агенти Zabbix здатні працювати під керуванням більшості UNIX-подібних операційних систем та систем родини Microsoft Windows;
- контроль пристроїв за SNMP (SNMPv1, SNMPv2c, SNMPv3) та IPMI;
- відстеження програм Java за допомогою розширень Java Management (JMX);
- контроль за віртуальними системами vCenter або vSphere за допомогою VMware API;
- вбудований графічний та інші можливості візуалізації;
- сповіщення, що дозволяють легко інтегруватися з іншими системами;
- гнучка конфігурація, включаючи шаблони.

Архітектура Zabbix представлена на рис. 1.

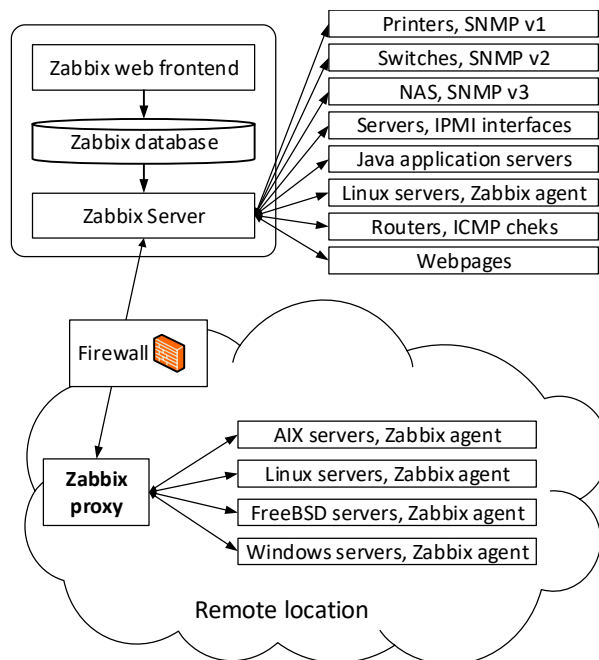


Рис. 1. Архітектура системи моніторингу Zabbix

Сервер Zabbix може контролювати одночасно велику кількість пристроїв. При цьому є можливість контролювати віддалені пристрої шляхом встановлення

Zabbix Proху, який має бути відділений від основного серверу брандмауером. Усі компоненти Zabbix написані мовою програмування С.

### III. ПРОПОЗИЦІЇ ЩОДО СТВОРЕННЯ ПІДСИСТЕМИ ЦЕНТРАЛІЗОВАНОГО МОНІТОРИНГУ

З метою здійснення моніторингу всіх програмних та апаратних (в тому числі віртуальних) компонентів системи електронної взаємодії у доповіді запропоновано створити підсистему централізованого моніторингу, яка повинна включати:

- сервер моніторингу, який періодично отримує і обробляє дані від агентів системи моніторингу та/або SNMP-подій обладнання/серверів, аналізує їх і сповіщає адміністраторів у випадку позаштатних ситуацій;
- агент системи моніторингу, що повинен запускатись на всіх серверах системи електронної взаємодії, та може працювати в двох режимах роботи: в активному режимі (запитує список необхідних параметрів і посилає їх сам до серверу моніторингу) і пасивному режимі (чекає запитів від сервера моніторингу);
- система керування базами даних для зберігання зібраних даних, конфігурації, подій тощо;
- HTTP сервер (Apache і PHP), що забезпечує веб-доступ адміністраторів для здійснення моніторингу та адміністрування.

Підсистема повинна інформувати відповідних адміністраторів про позаштатні ситуації виявлені в процесі моніторингу компонентів, шляхом передачі відповідних сповіщень.

Компоненти підсистеми централізованого моніторингу побудованого на Zabbix дозволяють реалізацію:

1. Створення карти мережі із візуальним відображенням стану серверів майданчику, маршрутів проходження, зв'язків серверів та їх стану, стану дзеркал серверів системи та можливістю перегляду всіх тригерів, що спрацювали на вузлах.

2. Забезпечення відображення вільного місця на всіх дисках із відображенням інформації про загальне/зайняте/вільне місце.

3. Покращення візуального сприйняття процесів у системі, особливо, що стосується критичних процесів. Додавання на комплексних екранах таких елементів моніторингу: графік відображення мережевого навантаження на сервери системи, індикатори статусу операцій на майданчику серверів, індикатори статусу дзеркала серверів, індикація об'єму дисків із журналами серверів, графік індикації навантаження процесорів та кількості процесів, індикація кількості клієнтських підключень у вигляді графіку та ін.

4. Забезпечення моніторингу стану серверів та мережевих зв'язків, а також стан мережевих адаптерів.

5. Моніторинг Крипто-серверу (стан мережевого підключення, вільне місце на диску С та стан системної служби тощо)

6. Виведення інформації по будь-яким параметрам для всіх вузлів мережі продуктивного майданчику (ZabbixGrapher).

7. Створення відображення простою системи.

Приклад реалізації системи моніторингу на базі Zabbix наведено на рисунку 2.

Спираючись на сучасні практики з модернізації електронних державних систем, впроваджених в Україні, та з метою запобігання зміни структурованих даних подій, що містяться в базі даних системи моніторингу, пропонується також використовувати технологію Blockchain.

Blockchain – (англ. ланцюжок блоків) технологія збереження даних у вигляді послідовних записів (блоків), де кожний наступний запис містить посилання на попередній.

Ключовими особливостями даної технології є:

- Незмінність даних – не можливе внесення змін у запис бази даних після моменту його внесення;
- Децентралізація – забезпечення розподілу, збереження та синхронізації даних між ланками ланцюга;
- Розумні контракти – можливість програмування умов проведення транзакцій та автоматичний контроль цих умов.

Blockchain є сучасною технологією розподільних даних, ідея якої полягає у функціонуванні без централізованого керівництва. Використання Blockchain забезпечує можливість функціонування систем без посередників, що дозволяє підвищити швидкість транзакцій, суттєво зменшити витрати та запобігти корупції. Захист даних здійснюється за допомогою потужних криптографічних алгоритмів.

В якості прикладів використання технології Blockchain в національних державних системах можна привести СЕТАМ (Система електронних торгів арештованим майном міністерства Юстиції України) та систему обробки та зберігання відомостей Державного земельного кадастру.

В першому випадку дана технологія була запроваджена за підтримкою Державного агентства з питань електронного урядування та використовується для збереження відомостей про ставки (можливість перевірити що ставку не було змінено або додано «заднім числом»)

У випадку з Державним земельним кадастром технологію Blockchain було запроваджено загальними зусиллями Міністерства агрополітики України, Державним агенством з питань електронного урядування та Transparency International Україна з метою збереження даних про виписки з реєстру.

## ВИСНОВКИ

Наведено основні пріоритетні напрямки та перспективи розвитку електронного урядування та електронної демократії в Україні. Розглянути особливості та пропозиції впровадження сучасних систем моніторингу для підвищення рівня захищеності систем електронного урядування.

Беручи до уваги всі вищенаведені особливості та переваги впровадження системи централізованого моніторингу із використанням системи Zabbix, можна відзначити безумовну перспективність його використання. Однак, слід зазначити, що рішення по реагуванню на будь-які події, в тому числі інциденти інформаційної безпеки, в системі приймає Адміністратор на підставі власного досвіду та отриманих знань. Це дає змогу говорити про необхідність подальшої автоматизації та адаптації до подій [5-7], яка повинна спростити процес прийняття рішення по адекватному реагуванню на змінення стану системи.

Відповідно до проведеного аналізу стану модернізації електронних державних систем, впроваджених в Україні також виявлено необхідність реалізації технології Blockchain для запобігання зміні структурованих даних подій, що містяться у базі даних системи моніторингу.

## ЛІТЕРАТУРА REFERENCES

- [1] Послуги по модернізації системи електронної взаємодії органів виконавчої влади (створення та впровадження підсистеми моніторингу, звітності, білінгу електронних документів Системи електронної взаємодії органів виконавчої влади) [Звіт про НДР] (заключн.) / В. В. Корчинський, Н. Ф. Казакова, О. О. Фразе-Фразенко, М. М. Светіков, І. В. Твердохліб, Д. С. Парфьонов, Ю. В. Копитін // ТОВ «Едванс Дейта Інтегрейшн»; кер. В. В. Корчинський. — 0117u005475. — Київ: 2017. — 51 с.
- [2] Гузій, М. М., Станіславова, О. В., & Кадет, М. В. (2009). Аналіз технологій моніторингу комп'ютерних мереж. Науковий журнал, 1(1), 46-50.
- [3] Порівняння систем моніторингу Zabbix і PRTG network monitor [Електронний ресурс] / Режим доступу: <http://it-ua.info/news/2014/09/02/porvnyannya-sistem-montoringu-zabbix--prtg-network-monitor.html>
- [4] Моніторинг подій інформаційної безпеки за допомогою ZABBIX [Електронний ресурс] / Режим доступу: <http://it-ua.info/news/2014/03/12/monitoring-pody-nformacyno-bezpeki-za-dopomogoyu-zabbix.html>
- [5] Казакова, Н. Ф. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки [Текст] / Н. Ф. Казакова, Є. В. Вавілов // Інформаційна безпека. — Луганськ: СНУ ім. В. Даля. — 2013. — №4(12). — С. 49-56. — ISSN 2224-9613.
- [6] Волков, С. Л. Модель експертного оцінювання якісного стану технічної системи [Текст] / С. Л. Волков, Н. Ф. Казакова, С. Д. Асабашвілі // Вісник Національного технічного університету «ХПІ»: Механіко-технологічні системи та комплекси. — Х.: НТУ «ХПІ». — 2017. — № 44. — С. 157-161.
- [7] Щербина, Ю.В. Определение параметров угроз информационным объектам [Текст] / Ю. В. Щербина, Н. Ф. Казакова // V Міжнародн. наук.-практ. конф. «Метрологія, технічне регулювання та забезпечення якості», 8-9 жовтня 2015 р., Одеса, ОДАТРЯ, 2015: матер. конф. — С. 133-137.

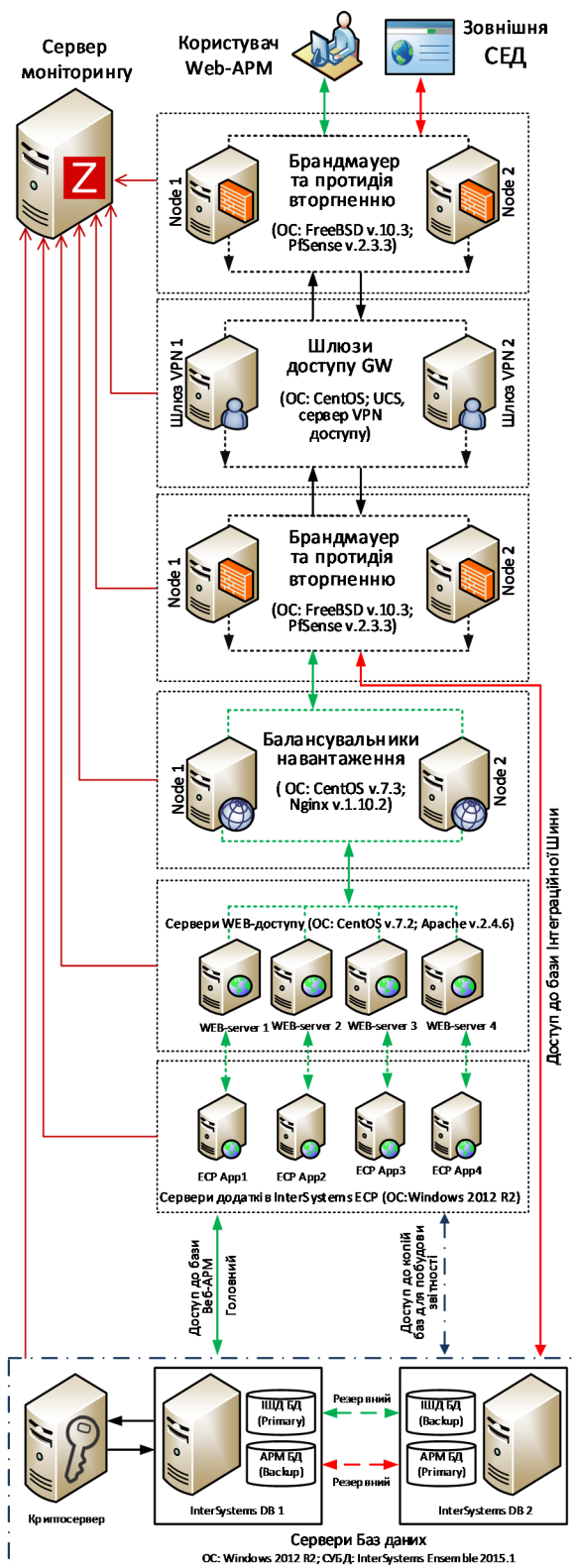


Рис. 2. Приклад реалізації системи моніторингу на базі Zabbix