2) оперативна аналітична обробка (On-Line Analytical Processing, OLAP);

3) інтелектуальний аналіз даних (Data Mining).

Інформаційно-аналітичні системи, які створюються в розрахунку на безпосереднє використання особами, що приймають рішення, надзвичайно прості в застосуванні, але жорстко обмежені у функціональності. Такі системи називаються статичними інформаційними системами керівника. Вони містять у собі наперед завдані безлічі запитів і, будучи достатніми для повсякденного огляду, не здатні відповісти на всі питання, які можуть виникнути при прийнятті рішень. Результатом роботи такої системи, як правило, є багатосторінкові звіти, після ретельного вивчення яких у аналітика з'являється нова серія питань. Однак кожен новий запит, не передбачений при проектуванні такої системи, повинен бути спочатку формально описаний, закодований і тільки потім виконаний. Час очікування в такому випадку може бути неприйнятним. Таким чином, зовнішня простота статичних систем планування і прийняття рішень, за яку активно бореться більшість замовників інформаційно-аналітичних систем, обертається катастрофічною втратою гнучкості.

Отже, динамічні системи орієнтовані на обробку нерегламентованих запитів аналітиків до даних. Робота аналітиків з цими системами полягає в інтерактивній послідовності формування запитів та вивчення їх результатів. Оперативна аналітична обробка даних забезпечує багатомірний статистичний аналіз, тобто представлення аналізованих фактів як функцій від великого числа характеризують їх параметрів.

Нестеренко О.В.,
д.т.н., доцент,
Нетесін І.Є.,
к.ф.-м.н.,
Поліщук В.Б.,
к.т.н.,
Шушпанов Є.Б.,
Державне підприємство «Український науковий центр розвитку інформаційних технологій»

ЗАСТОСУВАННЯ ВІЛЬНОГО/ВІДКРИТОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ ОРГАНІВ ДЕРЖАВНОГО УПРАВЛІННЯ

Істотне значення на сучасному етапі набувають рішення з формування програмного середовища всієї ІТ-сфери органів державного управління. Якість, надійність, безпека, врешті-решт вартість створення інфраструктурних елементів суттєво визначаються програмними засобами, що застосовуються. На цьому витку технологічного розвитку з новою силою постає питання вибору між так званим пропрієтарним (комерційним) і відкритим, або таким, що вільно розповсюджується, програмним забезпеченням.

В наш час комп'ютерні мережі (КМ) є основним комунікатором людини з людиною та з зовнішнім світом, життєво необхідним елементом забезпечення базових потреб людства, а процеси, що відбуваються в цій сфері, мають характер глобальних суспільних явищ. Усе більше взаємодія органів державного управління (ОДУ) та громадян відбувається за посередництвом ІКТ, і саме від стабільності їх функціонування та розвитку залежить створення передумов для сталого зростання економіки країни. Хмарні обчислення, мобільні і соціальні технології, великі дані та Інтернет руйнують старі інфраструктурні моделі і вимагають від ОДУ трансформації процесів прийняття рішень і впровадження технологічних інновацій.

Це висуває нові виклики ОДУ та державним службовцям. Громадяни зараз очікують з'єднань он-лайн з урядовими агенціями в безпечному, безшовному і надійному середовищі.

З іншого боку, працівникам ОДУ потрібно співробітничати з багаточисельними географічно розподіленими інфраструктурними елементами в реальному часі [1].

Крім того, за існуючими оцінками, на ринок буде випускатися усе більше безпровідних пристроїв. Службовці держструктур використовуватимуть чимало з цих пристроїв і інтеграція їх в мережу державних органів при підтримці її поточних рівнів безпеки і доступності є непростим завданням [2].

Перед ОДУ в цих умовах постають такі завдання, як підвищення ефективності своєї роботи за рахунок спільного використання IT-інфраструктури і сервісів для зниження витрат; поліпшення обслуговування громадян за рахунок надання сервісів в потрібний час, в потрібному місці і найбільш зручним для користувачів способом; підвищення рівня суспільної безпеки і безпеки в цілому при виконанні щоденних та екстрених завдань; забезпечення безперебійної роботи державних органів під час різних несприятливих умов та надзвичайних ситуацій.

Водночас у сфері ОДУ існує низка бар'єрів, що знижують ефективність і продуктивність IT-інфраструктури, зокрема КМ, при виконанні поставлених завдань. Серед цих бар'єрів можна виділити питання, пов'язані з широким розповсюдженням пропрієтарного (невільного, закритого) програмного забезпечення (ПЗ), що багато в чому впливає на масштаби неліцензійного використання ПЗ в країні [3]. Останнім часом представники державного сектора багатьох країн приходять до розуміння, що в умовах, коли виконання усе більшого числа державних функцій залежить від ПЗ, держава вже не може собі дозволити покладатися на добру волю постачальника пропрієтарного ПЗ з недоступним вихідним кодом, у якому можуть міститися критичні помилки, що довго не виявляються, або навмисно впроваджені «закладки». У зв'язку із цим суттєво зростає актуальність реалізації державної політики в сфері інформатизації в напрямку рівноправного, поряд з пропрієтарним ПЗ, використання ПЗ, що відкрите та вільно розповсюджується (ВПЗ) для ефективного і надійного функціонування КМ ОДУ.

ВПЗ відкрило нову епоху у розробці та використанні ПЗ для компаній і, зокрема, для ОДУ, що пов'язане з появою стабільної, безпечної та масштабованої операційної системи Linux, під керуванням якої вже працюють мільйони комп'ютерів у різних країнах. За цей час чимало країн зробили суттєві кроки в напрямку освоєння та впровадження ВПЗ в державних установах, і їх досвід має стати дуже важливим й для нашої країни. Тому одним з основних завдань проведеного дослідження є огляд ВПЗ, що є можливою альтернативою пропрієтарному ПЗ для забезпечення функціонування КМ ОДУ України.

ОС Linux може бути з успіхом використаною як основа інфраструктури ОДУ, зокрема серверів різного призначення. Як свідчить практика, у цій сфері Linux є достойним конкурентом інших ОС, або перемагає їх, особливо що стосується усіх мережних спеціалізацій серверів.

Як відомо, безпечний, зашифрований тунель між комп'ютером локальної мережі і зовнішньою мережею встановлює технологія VPN. Є декілька різних реалізацій VPN, але найбільш відомим є OpenVPN. Це, як випливає з назви, повністю відкрита система; вона використовує для з'єднання бібліотеку OpenSSL. Однією з найуніверсальніших утиліт для аналізу мережевого трафіку (sniffer) є WireShark.

Децентралізованою системою авторизації на сайтах є Mozilla Persona, заснована на протоколі BrowserID. Посилений захист надає двохфакторна автентифікація. Одне з цікавих двохфакторних рішень – це сервіс DuoSecurity, що підтримує автентифікацію для VPN, сайтів, облікових записів Unix (SSH) і т.ін.

Системою для збору всіх уразливостей, дір в безпеці, систем сканування і робочих навантажень є Metasploit Framework. Web-додатки – найласі шматочки для хакреського злому. Проект Open Web Application Security (OWASP) створив утиліту WebGoat, яка демонструє потенційні уразливості в цій області.

Важливим є підхід комплексного вирішення проблем захисту. Таким open source проектом є Security Enhanced Linux (SELinux). Основу SELinux складають три технології: мандатне керування доступом; ролевий доступ (RBAC); система типів (доменів). Модель

безпеки SELinux вирішує головним чином лише проблеми керування доступом користувачів до об'єктів ОС. Для вирішення проблем порушення цілісності виконуваного коду розроблені розширення безпеки Linux, що дозволяють мінімізувати наслідки атак, а саме система PAX та Bastille Linux.

Для інфраструктурних рішень використовується додаток Asterisk IP-PBX, що працює на Linux і FreeBSD і призначений для створення рішень комп'ютерної телефонії. Серверною платформою, що використовує мову програмування Javascript, є Node, або Node.js, що призначена для створення масштабованих розподілених мережевих застосувань, таких як веб−сервер. Проект Linux-HA (High-Availability Linux) призначений для забезпечення високої доступності на основі кластерізації для Linux, FreeBSD, OpenBSD, Solaris і ОС MacX, та який покриває проблеми надійності, доступності і обслуговуємості. Головним програмним продуктом проекту є Heartbeat - мобільна програма кластерного управління, що розповсюджується за GPL-ліцензією.

Для програмно-технологічної інфраструктури ОДУ, яка використовує ВПЗ, у тому числі продукти Linux, постає завдання забезпечення співіснування Linux з існуючим обладнанням – від десктопів до серверів. На сьогодні найпотужнішим та безпечним засобом централізованого керування усіма ресурсами є Novell ZENworks Linux Management.

Таким чином, існує чимало продуктів ВПЗ, які можуть застосовуватись в інфраструктурних рішеннях ОДУ, зокрема для підвищення рівня інформаційної безпеки КМ. Для підтвердження їх працездатності ряд технічних рішень, що використовують ВПЗ, проходить апробацію в рамках модернізації локальної мережі та веб-вузла Міністерства освіти і науки України.

Література

1. Нестеренко, О.В. Безпека інформаційного простору державної влади. Технологічні основи / О.В. Нестеренко. – К.: Наук. думка, 2009. – 352с.
2. Нестеренко, О.В Проблеми формування національної інформаційної інфраструктури та забезпечення її безпеки / О.В. Нестеренко // Реєстрація, зберігання і обробка даних. – 2010. – Т. 12 , №2. – С. 216-226.
3. Будько, Н.Н. Вільне програмне забезпечення: український вибір / Н.Н. Будько, О.В. Нестеренко, І.Є. Нетесін. – К.: Альтерпрес, 2011 . – 400 с.

***Домрачев В.М**., к.ф.-м.н., доцент,*
***Грабарєв А.В.,** к.е.н.,*
***Скляренко О.В.,** к.ф.-м.н., доцент,*
Європейський університет, м. Київ, Україна

КІБЕРБЕЗПЕКА ТА ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ

Досліджено сучасні інструменти інтелектуального аналізу даних, які застосовуються в процесі роботи правоохоронних органів США та надані відповідні рекомендації для запровадження їх в Україні.

Сучасний стан економіки України, вплив агресії з боку Росії та останні події на світовому фінансовому ринку потребують особливої уваги з боку правоохоронних органів та працівників інформаційної безпеки. До вирішення задач інформаційної підтримки кримінального аналізу та кібербезпеки підключились такі відомі комп'ютерні компанії як IBM (Cognos Express, SPSS), Microsoft, SAS та інші.

Так, компанія SAS активно пропонує на ринку інструменти SAS Enterprise Miner та SAS Fusion Center, які дозволяють вирішувати багато задач пов'язаних з запобіганням кіберзлочинності, зокрема пошуку злочинців, які через платіжну мережу здійснюють фінансові шахрайства у банках. Аналіз параметрів злочинів методами інтелектуальної