УДК 004.03, 681.3

Довгий С. О. , член-кореспондент НАН України, докт. техн. наук, проф.,
(Тел.: +380 (44) 245 87 97). E-mail: itelua@kv.ukrtel.net)
Лебідь О. Г. , канд. техн. наук (Тел.: +380 (44) 244 78 13). E-mail: itelua@kv.ukrtel.net)
(Інститут телекомунікацій і глобального інформаційного простору)

Копійка О. В., докт. техн. наук, с.н.с. (Тел.: +380 (44) 249 29 23. E-mail: okopiyka@gmail.com)
Ковальчук Ю. П., аспірант (Тел.: +380 (44) 248 85 72. E-mail: yuriu.kovalchuk@gmail.com)
Ройко О. О., аспірантка (Тел.: +380 (44) 249 29 23. E-mail: o.azarh@gmail.com)
(Державний університет телекомунікацій)

ЗАХИЩЕНИЙ ДОСТУП КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ СУПРОВОДЖЕННЯ БЮДЖЕТНОГО ПРОЦЕСУ

Довгий С. О., Лебідь О. Г., Копійка О. В., Ковальчук Ю. П., Ройко О. О. Захищений доступ користувачів інформаційно-аналітичної системи супроводження бюджетного процесу. У статті розглянуті підсистеми інформаційно аналітичної системи супроводження бюджетного процесу: «Моніторинг та аналіз процесу підготовки та виконання бюджету», «Сховище даних» та «База первинних даних» та варіанти формування архітектури системи безпеки для захищеного доступу користувачів. Архітектура системи безпеки забезпечує необхідний рівень захисту ІТ активів шляхом опису підходів щодо організації та формуванню вимог до персоналу , процесів і технологій. Завдання безпеки ІТ полягає у забезпеченні захисту цінної інформації і забезпечення її доступності авторизованим користувачам.

***Ключові слова*:** моніторинг та аналіз процесу підготовки та виконання бюджету, сховище даних, база первинних даних, архітектура системи безпеки, захист і управління цифровими даними

Довгий С. А., Лебедь А. Г., Копейка О. В., Ковальчук Ю. П., Ройко О. А. Защищенный доступ пользователей информационно-аналитической системы сопровождения бюджетного процесса. В статье рассмотрены подсистемы информационно-аналитической системы сопровождения бюджетного процесса: «Мониторинг и анализ процесса подготовки и исполнения бюджета», «Хранилище данных" и "База первичных данных" и варианты формирования архитектуры безопасности для защищенного доступа пользователей. Архитектура системы безопасности обеспечивает необходимый уровень защиты ИТ активов путем описания подходов к организации и формированию требований к персоналу, процессов и технологий. Задача безопасности ИТ заключается в обеспечении защиты ценной информации и обеспечения ее доступности авторизованным пользователям.

***Ключевые слова*:** мониторинг и анализ процесса подготовки и исполнения бюджета, хранилище данных, база первичных данных, архитектура системы безопасности, защита и управление цифровыми данными

1. Вступ. Система державних фінансів посідає ключове місце в системі державного управління. Принципи та механізми її побудови, розподіл функцій та повноважень між суб'єктами виступають, з одного боку, чинником соціально-економічного розвитку країни, з іншого – інструментом державного регулювання [1, 2].

Головною складовою системи управління державними фінансами є бюджетний процес, реалізація якого в Україні на поточний час не відповідає сучасним світовим вимогам до бюджетної системи і потребує модернізації.

Забезпечення ефективності функціонування бюджетної системи на рівні сучасних світових вимог передбачає:

– досягнення якісно нового рівня стратегічного бюджетного планування, визначення середньострокової податково-бюджетної стратегії, взаємоузгодженої із середньостроковими проектами соціально-економічного розвитку держави та її регіонів, секторів економіки та сфер економічної діяльності;

– вдосконалення методології прогнозування дохідної і видаткової частин державного та зведеного бюджетів на середньо- та довгостроковий періоди відповідного до макроекономічного прогнозу розвитку економіки та стратегії соціально-економічного розвитку країни;

– упорядкування процедур складання та затвердження бюджету;

– розширення застосування програмно-цільового методу бюджетування, що забезпечуватиме досягнення середньострокових стратегічних завдань та цілей;

– удосконалення механізму стратегічного та поточного планування видатків бюджету на інвестиційну та інноваційну діяльність, підвищення економічної ефективності капіталовкладень та покращення впровадження і підвищення відсотку виконання схвалених капітальних проектів;

– зменшення диспропорції в соціально-економічному розвитку окремих регіонів шляхом удосконалення системи між бюджетних відносин, а також розподілу функцій та повноважень між центральним та місцевими бюджетами;

– удосконалення системи бюджетної класифікації та гармонізація з міжнародними стандартами;

– удосконалення системи державних закупівель;

– удосконалення управління грошовими коштами та державним боргом з підвищенням його ефективності.

Зрозуміло, що усі зазначені результати можуть бути досягнуті лише на новому рівні законодавчого, методологічного та інформаційного забезпечення.

Рівень методологічного та наукового забезпечення підготовки та виконання Державного бюджету України має домінуючий вплив як на стан розвитку фінансово-економічної структури держави в цілому, так і на переважну більшість складових державотворення: соціальний захист, оборону, безпеку, охорону здоров'я, освіту, науку, тощо.

2. Постановка задачі. Насамперед йдеться про надання керівництву Комітету, Секретаріату та народним депутатам принципово нових можливостей щодо вирішення різноманітних моніторингових та аналітичних задач, які будуть розв'язувати на усіх етапах бюджетного процесу з набагато меншими витратами часу [1].

Саме для вирішення цього завдання були розроблені на першому етапі створення ІАС підсистеми «Моніторинг та аналіз процесу підготовки та виконання бюджету», "Сховище даних" та "База первинних даних".

Підсистеми націлені на розв'язання:

– задач, що вирішуються під час розгляду та прийняття проекту Закону про Державний бюджет України на наступний рік;

– задач моніторингу та первинного аналізу доходної частини Державного бюджету України;

– задач моніторингу та первинного аналізу видаткової частини Державного бюджету України;

– задач моніторингу та первинного аналізу виконання Державного та місцевих бюджетів.

При реалізації підсистем вирішувалась ще одна вкрай важлива задача – побудови захищеного доступу користувачів інформаційно-аналітичної системи супроводження бюджетного процесу. Саме вирішенню цієї задачі присвячена ця стаття.

3. Задачі забезпечення безпеки при управлінні бюджетним процесом. Завдання безпеки ІТ-ресурсів полягає у забезпеченні захисту цінної інформації і забезпечення її доступності авторизованим користувачам. Невиконання завдання безпеки може призвести до:

– видалення або зміни інформації;

– крадіжки інформації або сервісу;

– порушення бізнес операцій.

Пропонується Архітектура безпеки, яка забезпечує необхідний рівень захисту ІТ активів шляхом опису підходів щодо організації та формуванню вимог до персоналу, процесів і технологій [3...9].

ІТ інфраструктура повинна відповідати стандарту British Standard 7799 і його розвитку International Organization for Standardization (ISO) Standard 17799 [10]. Політики організації, розроблені відповідно до даних стандартами можуть надати необхідний рівень вимог до персоналу, процесів і технологій для забезпечення коректного використання ІТ активів авторизованими користувачами.

Архітектура безпеки розробляється на базі трьох компонентів:

1. Процес дисципліни управління ризиками.
2. Зонування мережі.
3. Ешелонний захист.

ІТ-активи. Особливу важливість і цінність для роботи Організації мають ІТ-активи, які включають, але не обмежуються ними, два компоненти: *дані* (інформація, інформаційний сервіс) та *рівні*.

Архітектура безпеки забезпечує для Даних (або інформації) захист:

1. Конфіденційності. Захист він несанкціонованого доступу та використання інформації.

2. Цілісності. Захист від неавторізованої, ненавмисного модифікації або пошкодження інформації.

3. Доступності. Корпорація повинна надавати інформацію чи сервіси вчасно, в межах часових рамок певних клієнтом.

Рівні представляють собою набір вузлів або пристроїв, які мають однотипну функціональність і можуть розглядатися як один логічний компонент.

Персонал. Основні принципи безпеки, що відносяться до персоналу:

1. Створюються і використовуються політики безпеки.
2. Персонал має достатню кваліфікацію для захисти ІТ-активів з якими він працює.
3. Персонал знає про політиків і їх зміни.
4. Існують механізми аутентифікації користувачів і авторизації їх дій з даними.
5. Адміністратори і комісії мають можливість аудиту дій і контролю виконання політик.

4. Процес дисципліни управління ризиками. Архітектура безпеки включає в себе один процес, що базується на дисципліні Управління Ризиками Безпеки – Security Risk Management Discipline (SRMD) (Рис. 1). Процес складається з чотирьох послідовних кроків:

1. Визначення та оцінка ІТ-активів.
2. Ідентифікація Ризиків безпеки.
3. Аналіз ризиків.
4. Розробка та зменшення ризиків.

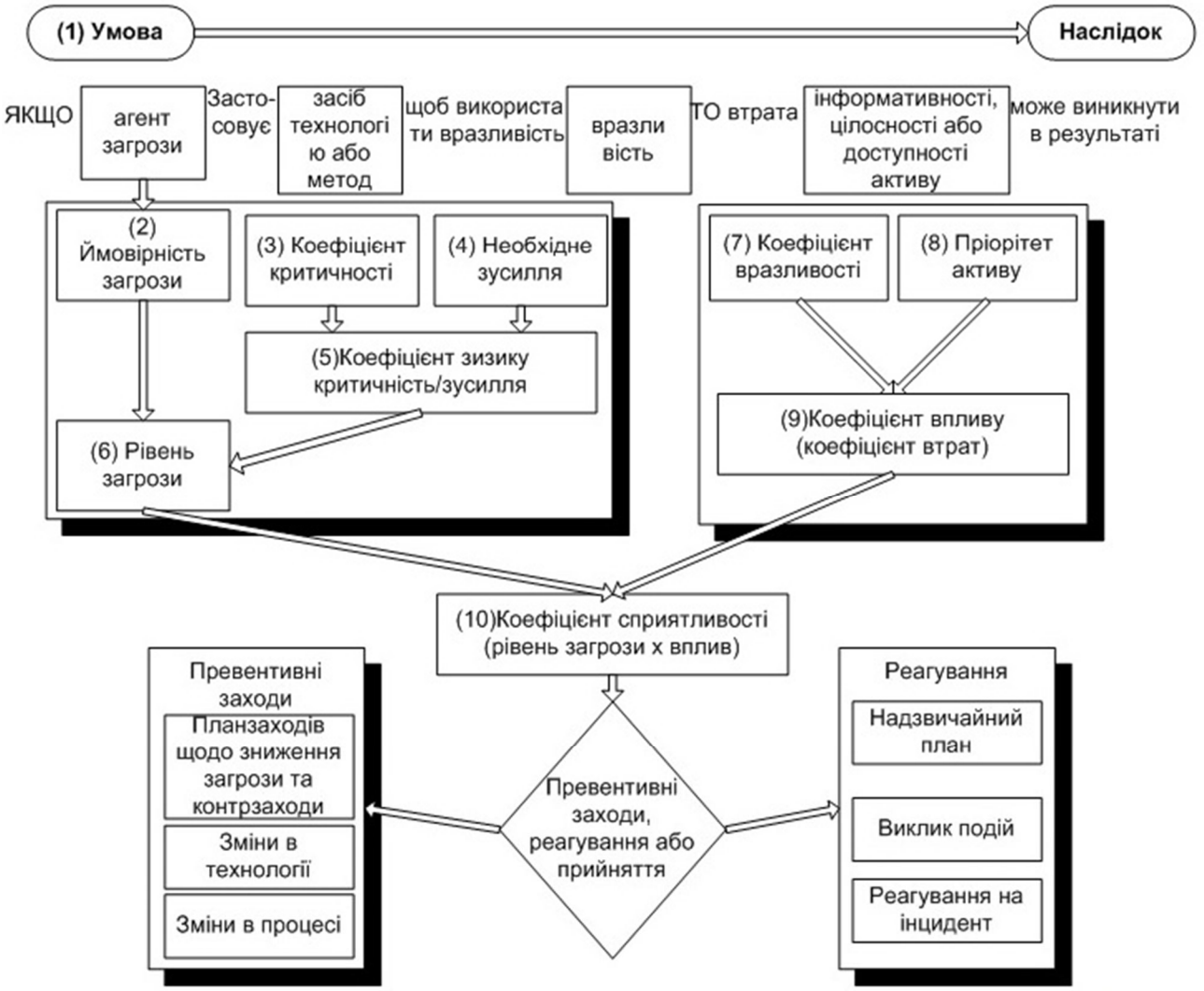

Рис. 1. Методика управління ризиками

Крок 1. Визначення і оцінка IT-активів. Визначення активів включає в себе класифікацію даних, використовуваних в Підсистемах.

Крім інформації при визначенні виділяються рівні (логічні групи однотипних пристроїв і вузлів).

Оцінка активів включає аналіз:

1. Фізичної вартості компонента IT інфраструктури:
   a) вартість апаратної частини;
   b) вартість програмної частини;
   c) вартість підтримки, експлуатації;
   d) вартість заміни;
2. Бізнес вартості - вартість активу для виконання місії Підсистеми.
3. Непрямої вартості.
4. Конкурентної вартості - вартість активу з точки зору переходу до іншої організації.

Після визначення та оцінки необхідно пріоритезувати IT-активи. Кожному активу присвоюється значення AP (asset priority) відповідно до якого активи упорядковуються. Фактори, що впливають на формування упорядкованого лінійного списку:

1. Вартість активу.
2. Ціна його створення.

3. Ціна його захисту.
4. Ціна його підтримки.
5. Ціна його відновлення.
6. Вартість активу для конкурентів.

Результатом першого кроку процесу буде чотири документи:

1. Список класифікованих даних.
2. Список класифікованих рівнів.
3. Список оцінених активів.
4. Список пріорітезірованих активів.

Крок 2. Ідентифікація ризиків безпеки. Ідентифікація ризиків безпеки опирається на такі терміни:

1. Погроза – потенційна небезпека, людина, річ або подія, яка загрожує безпеці активу.
2. Агент загрози – форма носія загрози – злочинець, хакер, пожежа, землетрус.
3. Уразливість – апаратна, програмна, процедурна точка зручна для здійснення атаки агентом загрози.
4. Метод атаки (exploit).
5. Ризик – значення функції, що зв'язує актив, загрозу, вразливість і метод атаки.

Ідентифікація ризиків включає в себе:

1. Аналіз загроз. Хто загрожує кожному з активів?
2. Оцінка вразливостей. Які у активів є вразливості? Які атаки мали місце в світовій практиці? Які наслідки цих атак?
3. Створення списку ризиків:

a) Визначення ризику у форматі «ЯКЩО агент загрози допомогою методу або інструменту впливає на вразливість, ТОДІ втрата (конфедінціальності, цілісності, доступності) активу може відбитися в результаті».

b) Визначення рівня додатки ризику: рівень даних, додатки, вузла, мережі, фізичного доступу.

c) Визначення критичних чинників (CF) – рівня руйнування активу в разі успішної атаки.

d) Визначення рівня вартості атаки (E) – кількості знань, досвіду, роботи необхідної для виконання атаки.

e) Визначення рівня схильності даного типу атаки (VF) – фактор, який дозволяє пов'язувати різні активи з одним типом атаки.

4. Оцінка ризиків – процес кількісної оцінки ризиків.

Результатом другого кроку процесу будуть три документи:

1. Список загроз і методів їх здійснення;
2. Список вразливостей;
3. Таблиця ризиків.

Крок 3. Аналіз ризиків. На третьому етапі для кожного з виділених ризиків визначаються наступні параметри:

1. Імовірність ризику;
2. Результат ризику (наслідки).

У результаті аналізу всіх отриманих кількісних характеристик ризиків створюється «Основний список пріоритезованих ризиків».

Крок 4. Розробка та зменшення ризиків. У розробку беруться тільки ризики з документа «Основний список пріоритезованих ризиків». Для кожного з описаних ризиків формується стратегія контрзаходів.

Результатом кроку буде один документ: «Стратегія контрзаходів».

5. Зонування мережі. Однією з успішних практик, яка дозволяє успішно аналізувати і зменшувати ризики є зонування мережі. IT інфраструктура логічно ділиться на зони з різними компонентами та вимогами до захисту - приватна зона містить активи, повністю контрольовані; публічна зона, містить активи з якою взаємодіють зовнішні клієнти.

Друга практика зменшення ризиків – Ешелонний захист - припускає, що контрзаходи створюються на п'яти рівнях IT інфраструктури (Рис. 2):

1. Рівень фізичного доступу.
2. Рівень мережі.
3. Рівень вузла.
4. Рівень даних.
5. Рівень прикладних програм.

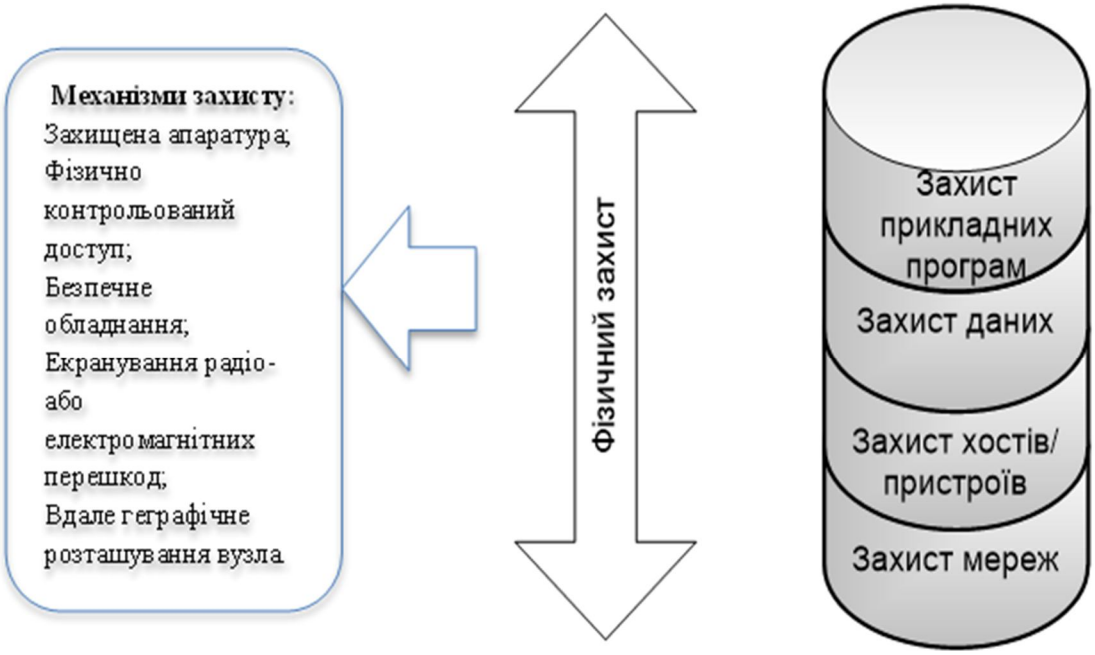

Рис. 2. Рівні ешелонного захисту

Оскільки в більшості випадків для здійснення атаки агенту необхідно використовувати або обійти кілька рівнів розміщення контрзаходів, це дозволяє на всіх рівнях значно зменшити ризик. Як приклад, IT інфраструктура повинна залишатися захищеної при відключенні систем мережевого захисту (firewall).

6. Технології захисту. Кожен компонент IT інфраструктури включає в себе механізми захисту. Список всіх механізмів доцільно виділити в окрему таблицю (Табл. 1).

Табл. 1

Механізми захисту	**Типи ризиків**
Рівень додатків	
HTML content filters	Ідентифікує і реагує на неавторизовані URL рядка.
Рівень даних	
Авторизація (NTFS ACL)	Забороняє доступ до даних для неавторизованих клієнтів.
Шифрування (IPSec, EFS, SSL)	Зменшує ризик прослуховування інформації в мережі і читання даних з носіїв в обхід механізмів авторизації.
Рівень вузла	
Internet Information Services (IIS) 6.0 Hardening	Забезпечує додатковий рівень захисту для сервера пріложенійIIS 6.0, допомагає уникнути помилок при конфігурації.
Windows Server 2003 шаблони безпеки	Призводить систему до базового рівня захищеності, шляхом настройки більш ніж 1200 параметрів.
Рівень мережі	
Firewalls	Мережеві екрани забезпечують інспекцію мережевого трафіку і розташовуються між мережевими зонами.
Internet Protocol Security (IPSec)	Захищає цілісності та конфіденційність мережевого трафіку.
Рівень фізичного доступу	
Контроль фізичного доступу	Контрольований доступ в приміщення та поверхи Корпорації.
Турнікет	Контроль доступу на територію Організації.

Таким чином при реалізації підсистем «Моніторинг та аналіз процесу підготовки та виконання бюджету», "Сховище даних" та "База первинних даних" вирішувалась ще і задача побудови захищеного доступу користувачів інформаційно-аналітичної системи супроводження бюджетного процесу за рахунок механізмів захисту компонентів IT інфраструктури.

7. Висновки. При побудові системи захищеного доступу користувачів інформаційно-аналітичної системи супроводження бюджетного процесу виділяємо наступні критерії для оцінки якості системи:

1. Керованість. Керованість, мабуть, є визначальною властивістю системи безпеки. Некеровану систему безпеки дуже важко захистити. Без використання механізмів моніторингу – потенційні порушення захисту можуть залишитися непоміченими. Без діагностування важче вирішувати питання безпеки.

Підхід із застосуванням зон, прийнятий для системи безпеки, також може використовуватися для її управління. Кожну зону безпеки можна розглядати як область управління, а завдання з управління безпекою можна доручити у разі потреби локальним адміністраторам. На сьогоднішній день для більшості пристроїв захисту існує можливість віддаленого управління, оскільки вони можуть зв'язуватися з консоллю централізованого управління, за допомогою якої виконується моніторинг їх роботи та налагодження конфігурацій.

2. Використання адміністративних ролей. Модель команд MOF пропонує рекомендації для управління IT-службами, створені на основі досвіду успішних організацій різного масштабу, які застосовують IT-технології у своїй діяльності від великих корпоративних IT-відділів до невеликих дата-центрів електронної комерції та постачальників служб додатків .

У MOF визначені кластери ролей, кожен з яких пов'язаний з певним аспектом IT - операція. Ролі кластера Безпеки (Security role cluster) покликані забезпечувати конфіденційність, цілісність і доступність даних організації. Фахівці з безпеки, які виконують ці ролі, приділяють увагу не тільки технічним проблемам, пов'язаним із захистом корпоративної мережі, але й політиці та практиці бізнесу. Мова йде про електронну пошту організації, застосування віддаленого доступу, надання дозволів на використання важливої корпоративної фінансової інформації та особистих даних працівників, а також про такі специфічні питаннях, як забезпечення конфіденційності списку телефонів працівників організації.

Ролі в кластері Безпека виконують такі загальні обов'язки:

– допомога в моніторингу правильності роботи IT-ресурсів;

– виявлення вторгнень і захист від вірусів;

– надання захисту шляхом відмови від обслуговування;

– визначення політик приховування та безпечної передачі даних;

– виконання аудиту та складання звітів про його результати;

– проектування ефективної системи безпеки і системи управління для мережевих доменів;

– тестування та впровадження стратегічних технологій захисту;

– моніторинг та оцінка вразливостей мережі;

– забезпечення швидкого реагування на вторгнення в реальному часі;

– управління інфраструктурою відкритих ключів;

– управління вимогами IP- безпеки;

– управління вимогами перевірки автентичності та доступу;

– управління застосуванням і вимогами політик щодо користувачів (наприклад, політикою застосування паролів);

– управління зовнішніми та фізичними вимогами до безпеки (наприклад, доступом в комп'ютерні лабораторії);

– управління вимогами до безпечного обміну повідомленнями;

– надання поточної технічної підтримки та консультацій з відповідних питань для різних ініціатив з підтримки безпеки в організації.

3. Системне адміністрування. Централізований підхід до адміністрування системи безпеки є досить простим для застосування менеджером з безпеки, оскільки всі завдання зосереджені в одному місці. Однак архітектура системи безпеки може зробити віддалене управління неможливим через певних обмежень безпеки.

Для віддаленого адмістрірованія застосовують засоби трьох типів:

– консоль MMC;

– веб-інструменти;

– засоби сторонніх виробників.

Зазвичай велика частина функцій віддаленого управління здійснюється за допомогою консолі MMC і засобів сторонніх виробників. Веб-інструменти постійно удосконалюються.

Безпека також певною мірою залежить від поширення віддаленого програмного забезпечення, зокрема від того, наскільки оперативно відбувається оновлення програмного забезпечення клієнтів віртуальних приватних мереж і антивірусних програм. Системне адміністрування засобів, які використовуються для реалізації безпеки і захисту рівнів, може виявитися складним завданням. Коли в організації прийнята стратегія глибоко ешелованого захисту, це призводить до зростання складності управління середовищем в залежності від значимості компонентів. За умови, що багато різних адміністраторів управляють різними технологіями, застосовуваними в середовищі, внесення змін може призвести до численних випадків неправильного налаштування конфігурацій. Для зменшення такого ризику в середовищі повинні бути введені надійні процеси обміну даними та управління змінами. На ринку з'являються інструментальні засоби для керування політиками безпеки для різних технологій, але поки вони недосконалі.

4. Продуктивність. Продуктивність системи безпеки в першу чергу залежить від того, які технології та обмеження реалізовані в середовищі.

– Фільтрація пакетів на мережевому рівні. Майже у всіх ситуаціях фільтрація пакетів збільшує час їх передачі з вихідного місця до місця призначення. Затримка залежить від способу перевірки пакетів. Наприклад, часті перевірки за допомогою механізму проксі на рівні прикладних програм займають більше часу, ніж проста фільтрація портів, оскільки такий процес вимагає більш глибокого дослідження пакетів.

– Шифрування. Шифрування даних завжди призводить до передачі більшої кількості даних, а також створює додаткове навантаження на процесори пристроїв, що виконують шифрування і дешифрування. Такі навантаження можуть бути переведені на спеціальні засоби апаратного забезпечення.

5. Консолідація. Якою буде система безпеки – розрізненої або консолідованої, визначається архітектурами мереж і програмного забезпечення, які вона підтримує. Полегшення управління системою безпеки є визначальним фактором консолідації серверних і мережевих пристроїв. Але консолідація повинна виконуватися з урахуванням вимог до безпеки даних і структури зон, розробленої для підтримки безпеки.

Консолідуючи служби на меншій кількості серверів, необхідно взяти до уваги наступне:

– Чи забезпечує консолідація автономне адміністрування служб на спільно використовуваному сервері, якщо до цього адміністрування цими службами виконували різні особи?

– Які додаткові ризики (для сервера, на якому вже виконуються ці служби, або для додатків, для яких, існують свої ризики) створює ця нова служба або додаток? Або організація готова погодиться з таким додатковими ризиками?

– Чи не висувають різні вимоги до паролів та/або шифрування програми або служби? Якщо так, то вони не зовсім придатні для консолідації.

– Чи не використовують програми або служби різні облікові записи служб або підвищені пріоритети, які можуть надати нападнику, який отримає несанкціонований доступ до однієї службі, доступ до інформації, виконуваної в інших процесах на тому ж сервері?

6. Стандарти та інструкції. Стандарт ISO 17799 – це прийнятий на міжнародному рівні ряд регуляторних норм, які об'єднують кращі практики у сфері безпеки інформації. Це стандарт створений на основі англійської стандарту BS 7799, який він поступово витіснив.

Література

1. Довгий С. О. Інформаційно-аналітичне супроводження бюджетного процесу / С. О. Довгий, І. В. Сергієнко, О. В. Копійка та ін.]; під ред. С. О. Довгого, І. В. Сергієнко. – К.:ТОВ «Інформаційні системи», 2013. – 420 с.

2. Довгий С. О. Засади регіональної інформатизації / С. О. Довгий, О. В. Копійка, Ю.Т. Черепін. – К.:ВПЦ «ТИРАЖ», 2004. – 304 с.

3. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група BHN, 2005. – 352 с.

4. Копейка О. В. Сетевые службы и службы сетевых устройств в дата-центрах / О. В. Копейка // Системи управління, навігації та зв'язку. – 2013. – №4(28). – С. 98-104.

5. Копейка О. В. Архитектура системы безопасности ИТ-инфраструктуры в дата-центрах / О. В. Копейка // Сучасний захист інформації. – 2014. – №1. – С.48-57.

6. Jew Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010. – 28 p.

7. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric – page 4.

8. Telecommunications Infrastructure Standard for Data Centers // Tia standard TIA-942. Telecommunications industry association. – April 2005. – 135 p.

9. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices // Committee Approval. – January 2011 First Published: March 2011. – 367 p.

10. Информационные технологии – практические правила управления информационной безопасностью // ISO/IEC 17799 международный стандарт ; – 1-е изд. – 2000-12-01. – 87 с.

Дата надходження в редакцію: 09.02.2015 р. Рецензент: д.т.н., проф. Беркман Л. Н.