УДК 004.056

Копитін Ю.В.
Копытин Ю.В.
Kopytin Y.V.

ВИКОРИСТОВУВАННЯ АВС-АНАЛІЗУ ЗАДЛЯ ОПТИМІЗУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ИСПОЛЬЗОВАНИЕ АВС-АНАЛИЗА ДЛЯ ОПТИМИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

USING THE ABC-ANALYSIS FOR THE OPTIMIZATION OF THE INFORMATION SECURITY SYSTEMS

Анотація. Окреслено можливість використовування методу АВС-аналізу в питаннях захисту інформації. Продемонстровано застосовування АВС-аналізу для вибору комплексу засобів захисту від несанкціонованого доступу.

Аннотация. Показана возможность использования метода АВС-анализа в вопросах защиты информации. Продемонстрировано применение АВС-анализа для выбора комплекса средств защиты от несанкционированного доступа.

Summary. The article shows the possibility to use the method of ABC-analysis for the information protection. It demonstrates the way ABC-analysis can be used to select a trusted computing base against an unauthorized access.

Інформаційні ресурси держави чи то суспільства в цілому, а також окремих організацій та фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і потребують захисту від різноманітних за своєю сутністю дій, які можуть призвести до втрати захищуваної інформації, а також несанкціонованих і незумисних впливів на неї. Тому останнім часом багато досліджень присвячують проблемі захисту інформації.

Тематику даної статті зумовлено:

– зростанням збитків, пов'язаних із втратою ресурсів внаслідок недоліків системи захисту інформації;

– збільшенням обсягу коштів, які необхідно витратити на створення та модернізацію систем захисту інформації;

– проблемами вибору засобів захисту (серед безлічі можливих), адаптованих до сучасних умов [1] та з оптимальним рівнем захищеності [2], який задовольняє політиці безпеки в системі.

Зауважимо, що абсолютно безпечних систем не існує [3]. Витрат на інформаційну безпеку уникнути неможливо, але їх можна звести до оптимального рівня, за якого система безпеки гарантуватиме належний рівень захищеності, а витрати на неї не будуть призводити до збитків. Саме тому питання вибору оптимальних систем захисту інформації набуває ще більшої ваги.

Проте задача вибору оптимальних систем захисту інформації досліджено недостатньо.

Мета статті – показати доцільність практичного застосовування методу АВС-аналізу [4] для вибору оптимальних, ефективних та економічно обґрунтованих систем захисту інформації.

Найбільш поширеним, простим, наочним та з достатнім ступенем вірогідності методом аналізу задля виявляння першопричин виникнення проблем є метод АВС-аналізу, одним з варіантів графічної інтерпретації якого виступає діаграма Парето.

1897 року італійський економіст і соціолог Вільфредо Парето виявив математичну залежність, яка показує, що блага розподіляються нерівномірно. Його відкриття називали по-різному, у тому числі засадою Парето, законом Парето, правилом 80/20, засадою найменшого зусилля, засадою дисбалансу. Ця ж теорія була графічно проілюстрована 1907 року американським економістом Максом Отто Лоренцо. Обидва вчених показали, що в більшості випадків найбільша частка благ (доходів) належить невеликій кількості людей. 1921 року графічне зображення даних, запропоноване Лоренцо, набуло назви «кривої Лоренцо». Саме цим терміном прийнято називати зображення лінії, представленої на сучасних схемах АВС-аналізу.

Метод АВС-аналізу можна застосовувати практично в будь-яких галузях діяльності з метою виявлення першочергових проблем, які треба розв'язувати, шляхом визначення їхньої пріоритетності.

Загальний алгоритм здійснення АВС-аналізу [5] передбачає таку послідовність дій:

1) визначаємо мету аналізу;

2) визначаємо об'єкти аналізу;
3) визначаємо чинники для диференціювання об'єктів аналізу;
4) формуємо інформаційний масив для аналізу;
5) оцінюємо об'єкти аналізу за виокремленими чинниками;
6) ранжуємо показники;
7) здійснюємо поділ об'єктів на групи;
8) графічно інтерпретуємо результати аналізу.

Зазначимо, що низка авторів пропонують іншу послідовність кроків алгоритму. На нашу думку, наведений вище алгоритм є найбільш зручним.

У питаннях захисту інформації даний алгоритм можна використати у такий спосіб:

На першому етапі чітко визначаємо мету аналізу. Наприклад: вибір оптимального набору засобів захисту, які будуть використовуватимуться для забезпечення безпеки об'єкта. Слід зазначити, що неправильно визначена мета може негативно вплинути на результати аналізу.

На другому етапі визначаємо об'єкти, які підлягають аналізу. В якості об'єктів виступають: приміщення, які підлягають захисту; процеси (діяльність), які відбуваються в приміщенні; засоби захисту, які використовуються чи плануються задля використовування для забезпечення безпеки, тощо.

На третьому етапі визначаємо чинники, на підставі яких відбуватиметься диференціювання об'єктів аналізу. В якості чинників виступають: потенційні загрози та їхні типи; потенційні уразливості об'єкта, що захищається; необхідні витрати для побудови (модернізації) системи захисту; ймовірні ризики здійснення атаки на ресурс; вплив на виробничу здатність системи, що захищається; величина прибутку тощо.

На четвертому етапі формуємо інформаційний масив для аналізу. Для цього збираємо усі відомості за чинниками, що аналізуються. Наприклад: збираємо інформацію про потенційні загрози об'єктові, що захищається.

На п'ятому та шостому етапах проводимо: оцінювання внеску кожного об'єкта за чинником, що аналізується, до загального результату; ранжування об'єктів в порядку зменшення значення виокремленого чинника; обчислення наростаючої підсумкової частки об'єкта щодо сумарної кількості об'єктів у відсотках та внесок об'єкта до сумарного результату у відсотках.

На сьомому етапі здійснюємо поділ здобутих результатів на групи. Даний поділ можна здійснювати за допомогою: емпіричного методу, методу суми, методу дотичних та ін. Вибір методу здійснимо далі. Кількість груп при проведенні АВС-аналізу може бути довільною. Найбільш поширено здійснювати поділ на три групи (А: В: С). Цим і зумовлено назву методу (ABC-Analysis). Зазначимо, що: групу А складає незначна кількість чинників з високим рівнем питомої ваги за обраним показником (наприклад: ресурси, які мають найбільшу ймовірність ризику здійснення атаки); групу В – середня кількість чинників з середнім рівнем питомої ваги; групу С – величезна кількість чинників з незначною величиною питомої ваги.

Головний сенс дослідження у рамках АВС-аналізу зводиться до того, що максимальний ефект досягається за розв'язування завдань (проблем), що належать до групи А. В табл.1 наведено можливі варіанти поділу на групи [6].

Отже, на даний момент немає чіткого визначення границь груп у выдсотковому співвідношенні за ступенем впливу.

Таблиця 1 – Границі груп

Автор	Група А, %	Група В, %	Група С, %
Д.Дж. Бауерсокс	80	15	5
Уотерс	70	20	10
В.В.Глухов	65	20	15
J. Shapiro	60	20	20

Емпіричний метод передбачає поділ об'єктів на групи на підставі усереднених результатів раніш проведених досліджень. Найбільш поширений варіант передбачає такі границі: 80 % внеску об'єкта до сумарного результату поміж групами А і В та 95 % – поміж В і С. Потім знаходимо відповідні значення частки об'єктів із сумарної кількості у відсотках. Перевага методу полягає в його простоті, а недолік – в тому, що усереднені значення не завжди відповідають певній ситуації [5].

Метод суми передбачає виокремлювання груп за сумою частки об'єктів *(ЧО)* із сумарної кількості у відсотках та внеску об'єкта *(ВО)* до сумарного результату у відсотках. Границя груп А та

В знаходиться в точці, де сума $ЧО_A$ та $ВО_A$ дорівнюватиме 100%. Границя груп В та С – в точці, де сума $ЧО_B$ та $ВО_B$ дорівнює 145%. Зауважимо, що існують й інші варіанти визначання границь груп. Переваги методу: більш гнучкий, ніж емпіричний метод, та оптимальніш відтворює певну ситуацію; може бути легко завтоматизований. Суттєвих недоліків немає [5].

Диференційний метод передбачає, що: до групи А належать об'єкти, в яких значення чинника в 6 разів і більше перевищує середнє значення чинника; до групи С – об'єкти, значення чинника за якими удвічі та більше разів менше за середнє значення чинника; до групи В – уся решта об’єктів. Перевага методу полягає в його простоті, а недолік – часто призводить до некоректних результатів через невизначеність вибору коефіцієнтів. Можливий випадок, що з аналізованих об'єктів взагалі неможливо виокремити групу А [5].

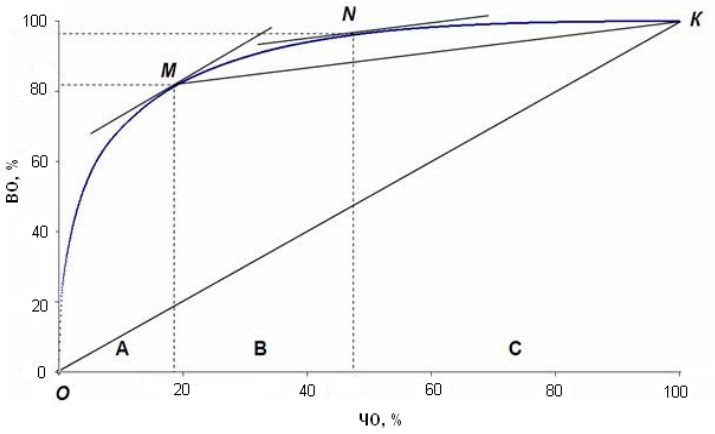

Рисунок 1 – Метод дотичних

Метод дотичних полягає в поділі об'єктів аналізу на групи за допомогою дотичних до кривої АВС аналізу (рис. 1). Для визначення границь груп: сполучують початок і кінець кривої прямою ОК; проводять дотичну до кривої, паралельну до ОК; точка дотику М поділяє групи А і В. Далі сполучують точки М і К та проводять дотичну до кривої, паралельну до МК. Точка дотику N поділяє групи В і С. Перевага методу полягає в його гнучкості, простоті та наочності, а недолік – складність автоматизації [5].

Проаналізувавши різні методи проведення АВС-аналізу, зупинімося на методі «суми», позаяк він є: більш гнучким за емпіричний метод та оптимальніше відтворює певну ситуацію; є одним з найпростіших і може бути легко автоматизований. Інші методи є більш складними у застосовуванні.

На останньому етапі задля оптимального відображення здобутих результатів здійснюємо їхню інтерпретацію шляхом побудови графіка. Такий графік називається кривою Парето, кривою Лоренцо чи АВС-кривою [7]. Позаяк АВС-аналіз проводиться за методом суми, то на осі абсцис відкладаються значення ЧО у відсотках, а на осі ординат відкладається значення суми ЧО та ВО у відсотках. На рис. 2 наведено графічну інтерпретацію методу суми.

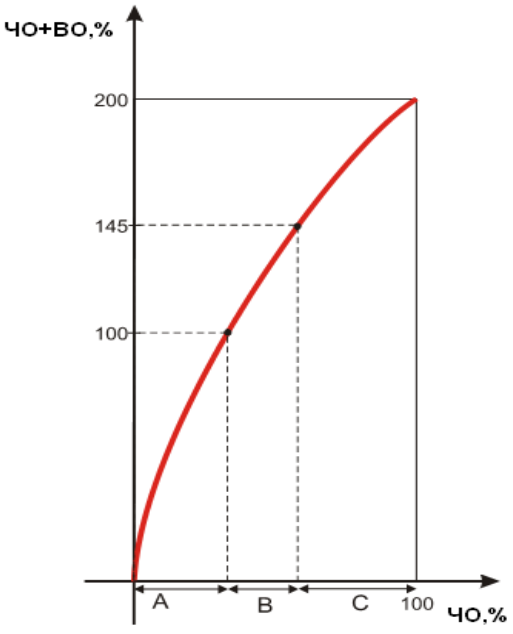

Рисунок 2 – Графічна інтерпретація методу суми

Далі виконуються етапи та стадії створювання системи захисту, передбачені чинними нормативно-правовими документами у сфері захисту інформації.

Переваги методу АВС-аналізу:

1. АВС-аналіз є точний та простий у використовуванні дозволяє правильно виявляти головні причини проблеми задля їхнього ефективного розв’язування**.**

2. АВС-аналіз може бути досить легко автоматизований. Теоретичні методи знаходять практичні втілення у програмних продуктах, одним з яких є продукт компанії КонСі.

Недолік методу АВС-аналізу: за нечітко поставленої мети (крок 1 алгоритму) можливі помилкові висновки.

Отже, сформулюємо метод АВС-аналізу стосовно питань захисту інформації: визначивши чинники, які призводять до найбільших порушень політики інформаційної безпеки, оптимізуємо витрати на забезпечення інформаційної безпеки та зменшимо потенційні збитки, які можна понести внаслідок недосконалості системи інформаційної безпеки, шляхом посилення заходів, спрямованих на боротьбу з цими чинниками та зменшення заходів, направлених проти менш пріоритетних чинників.

Розглянемо приклад використовування АВС-аналізу в питаннях вибору оптимального комплексу засобів захисту (КЗЗ) від несанкціонованого доступу. В даному разі під оптимальним розуміється такий комплекс, який забезпечує захист від найбільш актуальних на даний момент уразливостей. Зазначимо: наведений приклад демонструє потенційну можливість використання АВС-аналізу в питаннях захисту інформації. Для вибору найбільш оптимального КЗЗ необхідно здійснити комплексний всебічний аналіз, проаналізувавши всі можливі чинники, що впливають на результат.

Для розв'язання поставленої проблеми проведемо АВС-аналіз методом суми, на базі статистики уразливостей ОС за другий квартал 2008 року, наведеної в [8], та зведемо його результати у табл. 2. Зазначимо, що у [8] опубліковано 188 уразливостей, здобутих на підставі 85-ти повідомлень від різних виробників.

Таблиця 2 – АВС-аналіз уразливостей операційних систем

Тип уразливості	Кількість уразливостей за даними [8]	Частка фактора у сумі значень фактора за даними [8], %	Наростаюче значення ВО, %	Наростаюче значення ЧО, %	Сума ЧО та ВО,%	Група
Відмова в обслуговуванні	52	27,66	27,66	11,11	38,77	A
Компрометація системи	48	25,54	53,2	22,22	75,42	A
Підвищення привілеїв	44	23,41	76,61	33,33	109,94	A
Обхід обмежень безпеки	18	9,57	86,18	44,44	130,62	B
Спуфінг- атака	11	5,85	92,03	55,55	147,58	B
Розкриття важливих даних	7	3,72	95,75	66,66	162,41	C
Розкриття системних даних	4	2,13	97,88	77,77	175,65	C
Неавторизована зміна даних	2	1,06	98,94	88,88	187,82	C
Міжсайтовий скриптинг	2	1,06	100	100	200	C

На рис. 3 представлена АВС-крива, яка графічно інтерпретує поділ уразливостей на групи.

Виходячи з результатів, поданих в табл. 2, першочерговими є механізми КЗЗ, які протидіють таким дразливостям, як: відмова в обслуговуванні, компрометація системи та підвищення привілеїв. Дані уразливості належать до групи А. Забезпечення захисту від трьох основних типів уразливостей знизить потенційну можливість скористатися 144 уразливостями зі 188-ми, що у відсотковому співвідношенні становить 76,61 % усіх можливих уразливостей.

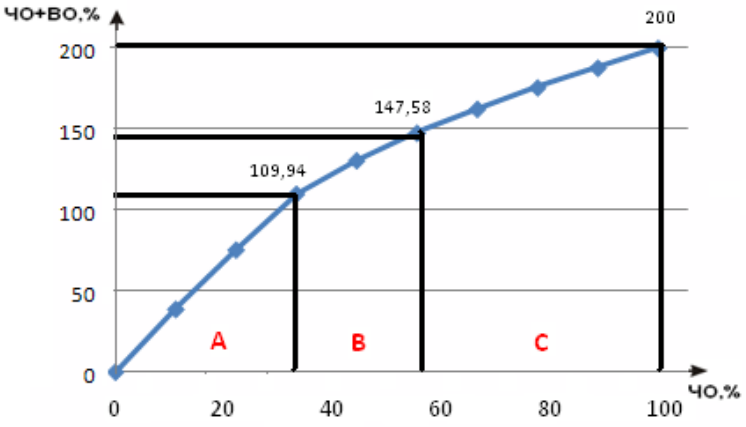

Рисунок 3 – Графічна інтерпретація АВС-аналізу

До відмови в обслуговуванні належать уразливості, які дозволяють зловмисникові порушити коректну роботу і вплинути на програмний додаток або ОС. До компрометації системи належать уразливості, які дозволяють користувачеві виконати довільний код на цільовій системі з привілеями користувача або вразливої служби. До підвищення привілеїв належать уразливості, які дозволяють локальному користувачеві отримати привілеї іншого облікового запису в системі.

Задля протидії щодо відмови в обслуговуванні застосовують механізм контролю цілісності, який захищає виконувані файли від модифікування. Задля протидії атакам, пов'язаним з компрометацією системи, КЗЗ застосовують механізм створення замкненого програмного середовища. Задля протидії підвищенню рівня привілеїв – механізм ідентифікації та автентифікації.

Отже, на підставі результатів проведеного вище аналізу можна зробити логічний підсумок, що оптимальний КЗЗ має включати механізми контролю цілісності, створювання замкненого програмного середовища й ідентифікації та автентифікації. Слід зазначити, що, захищаючись від атак на ці ключові уразливості за допомогою використовування наведених механізмів, зреалізовується й захист від атак на низку інших, менш імовірних та критичних уразливостей.

Як ***висновок*** зазначимо, що використовування розглянутого методу АВС-аналізу в питаннях захисту інформації дозволяє швидко та зручно визначати механізми захисту, які треба застосовувати задля підтримання належного рівня політики інформаційної безпеки. Тим самим створюються оптимальні, ефективні та економічно обґрунтовані системи захисту інформації, оскільки головні витрати спрямовано на найбільш уразливі місця об'єкта, а інші – зменшуються за умови відсутності порушень політики безпеки. Зокрема , це вибір комплексу засобів захисту, який забезпечує захист від актуальних на даний момент уразливостей.

Використовування методу АВС-аналізу надає можливість надалі:

– обирати оптимальні системи захисту інформації, які забезпечували б захист від актуальних загроз та уразливостей;

– створювати економічно ефективні системи захисту, які гарантуватимуть належний рівень захищеності, а витрати на неї не призводитимуть до збитків, пов'язаних з перевищенням вартості системи величини можливого здобутого прибутку від захищуваної інформації;

– здійснювати зручно та швидко адаптування систем захисту до змінюваних умов.

Отже, для вибору оптимальних, ефективних та економічно обґрунтованих систем захисту інформації доцільно застосовувати метод АВС-аналізу.

Література

1. *Де Гроот М.* Оптимальные статистические решения, *пер. с англ.* / Де Гроот М. – М. : Мир, 1974. – 491 с.
2. *Баутов А.* Экономический взгляд на проблемы информационной безопасности. *[Електронний ресурс]* / Открытые системы – 2002. – № 2. – Режим доступу: http://www.osp.ru/os/2002/02/181118/. – Назва з екрана.
3. *Adi Shamir.* Turing Award lecture *[Електронний ресурс] /* Adi Shamir. – 2004. – Режим доступу: http://www.financialcryptography.com/mt/archives/000147.html. – Назва з екрану.
4. *АВС-анализ [Електронний ресурс].* – Режим доступу: http://www.abc-analysis.ru/. – Назва з екрана.
5. *Фишер Андрей*. Методы выделения групп в АВС анализе *[Електронний ресурс]* / Фишер Андрей. – Режим доступу: http://www.transmap.ru/articles/view/169. – Назва з екрана.
6. *Методы АВС* анализа номенклатурных групп [Електронний ресурс]: (По книге «Модели м методы теории Логистики», Лукинский В.С. и др.). – Режим доступу: http://www.adviss.ru/content/view/45/7/. – Назва з екрана.
7. *Анализ АВС [Електронний ресурс].* – Режим доступу: http://www.basegroup.ru/glossary/definitions/abc_analysis/. – Назва з екрана.
8. *Отчет* по уязвимостям за второй квартал 2008 года [Електронний ресурс] / Валерий Марчук. – Режим доступу: http://www.securitylab.ru. – Назва з екрана.
9. *Цуканова О.А.* Экономика защиты информации *:* учебн. пособие / О.А. Цуканова, С.Б. Смирнов. – СПб.: СПб ГУИТМО, 2007. – 59 с.
10. *Баканов М. И.*Теория экономического анализа [Текст] : учебник / М.И. Баканов, М.В. Мельник, А.Д. Шеремет; под ред. проф. М.И. Баканова. – [5-е изд., перераб. и доп.]. – М. : Финансы и статистика, 2005. – 536 с. : ил. – ISBN 5-279-02718-9
11. *Лукинский В.С.* Модели и методы теории логистики: учеб. пособие [для студентов, аспирантов, преподавателей и специалистов в области логистики] / Лукинский В.С. – [2-е издание]. – И: Питер, 2008 . – 448 с. – ISBN 978-5-91180-139-7
12. *Гаджинский А.М.* Логистика : учебник [для студентов высших и средних специальных учебных заведений] / Гаджинский А.М. – И.:"Дашков и Ко", 2004. – 432 с. – ISBN 5-94798-500-4