УДК 621.396

Любарський С.В., Шаціло П.В.

ДОСЛІДЖЕННЯ АРХІТЕКТУРИ СИСТЕМИ ОПЕРАТИВНОГО АУДИТУ ПОДІЙ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Анотація:

У статті розглядаються формальний і неформальний (класифікаційний) підходи до оцінки інформаційної безпеки інформаційних систем.

Аннотация:

В статье рассматриваются формальный и неформальный (классификационный) подходы к оценке информационной безопасности информационных систем.

Abstract:

The article deals with the formal and anformal (classification) approach to evaluating security of information systems.

Порушення безпеки інформаційної системи (ІС) органу управління розглядається як інцидент безпеки інформаційно-аналітичного процесу управління об'єктами управління через втрату конфіденційності, цілісності, доступності інформаційних ресурсів. Особливо актуальним постає питання забезпечення конфіденційності інформації та цілісності даних в технологіях передачі інформації, що базуються на відкритих стандартах функціонування інформаційних систем та мереж.

Аналіз захищеності є основним елементом таких видів робіт, що взаємно перетинаються, як атестація, аудит та обстеження безпеки ІС.

Основою формального опису систем захисту традиційно вважається модель системи захисту з повним перекриттям, в якій розглядається взаємодія "області загроз", "області, що захищається" (ресурсів ІС) і "системи захисту" (механізмів безпеки ІС).

Перевагою формального підходу є те, що він дозволяє отримати точні кількісні оцінки різних показників захищеності ІС. Однак через обмеженість формального підходу, практична реалізація якого представляється справою досить складною і малоефективною, напрошується висновок про перевагу використання класифікаційного підходу, що є основним методом аналізу захищеності і використовується на практиці.

При класифікаційному підході замість точних кількісних оцінок захищеності ІС передбачається використовувати характеристики категоріювання об'єктів ІС: порушників (за цілями, кваліфікацією), інформації (за важливістю і рівню секретності), засобів захисту (за важливістю контурів захисту і особливістю обчислювальних ресурсів, що використовуються). Такий підхід не дозволяє отримувати точні значення показників ефективності засобів захисту, проте дає можливість класифікувати ці системи і порівнювати їх між собою. В основі класифікаційних методик, що набули поширення, лежать критерії оцінки інформаційної безпеки ІС, що встановлюють класи і рівні захищеності. Методики та концепції оцінки безпеки, а також набір критеріїв у достатньому обсязі міститися в міжнародних стандартах *ISO* 15408 та *ISO* 17799 (*BS* 7799).

Інформаційний аудит посідає ключову роль в загальній системі аудиту рівня інформаційної безпеки ІС [1].

Підсистеми реєстрації подій безпеки є на сьогоднішній день важливими і невід'ємними компонентами систем забезпечення інформаційної безпеки практично в будь-якій мережевій операційній системі, а відповідно, і в будь-якій мережевій інформаційній системі. Реєстрацію подій безпеки також часто називають аудитом подій безпеки (АПБ). Можливості реєстрації подій безпеки реалізовані в мережевих операційних системах (ОС) і прикладному програмному забезпеченні (ПЗ). Однак, відчутний ефект від використання засобів аудиту досягається лише тоді, коли зареєстровані дані про події безпеки можуть бути оперативно проаналізовані. Тільки в цьому випадку стає можливим своєчасне виявлення шкідливих впливів на елементи мережевої інформаційної системи – комп'ютери, програмне забезпечення, дані, що передаються і зберігаються та інше.

Наявність підсистем реєстрації подій безпеки є однією з основних вимог, що має місце у всіх сучасних стандартах та керівних документах з інформаційної безпеки ІС [2]. Зазначені стандарти також визначають класи подій, що підлягають реєстрації. Вимоги до наявності засобів реєстрації подій безпеки відносяться до технічних вимог, тому вони, як правило, виконуються розробниками базового ПЗ мережевих інформаційних систем.

Регулярний аналіз зареєстрованих подій безпеки зазвичай відносять до організаційних заходів, що є основною причиною недостатньої уваги розробників ПЗ до проблем організації оперативного аналізу подій безпеки в мережі. Іншими словами, для того, щоб атестувати програмне забезпечення мережевої інформаційної системи на відповідність вимогам стандартів безпеки зазвичай достатньо реалізувати в ній лише засоби реєстрації подій безпеки.

Облік типових обсягів даних про події безпеки, а саме сотні і тисячі записів про події безпеки в день на одному комп'ютері, дозволяє стверджувати, що при відсутності спеціальних програмних засобів, аналіз цих подій стає малоефективним. З цієї причини і обслуговуючий персонал мережевих інформаційних систем часто зневажливо ставиться до завдань аналізу зареєстрованих даних про події безпеки.

Все це значною мірою знижує ефективність визначення ступеня захищеності ІС і не дозволяє виявити помилки й недоліки в реалізації політики безпеки мережевої інформаційної системи до того, як вони будуть використані у зловмисних цілях.

Засоби керування доступом, що існують в програмному забезпеченні кожної мережевої інформаційної системи, часто не можуть забезпечити безпеку в повній мірі, оскільки вони не призначені для запобігання некваліфікованим або зловмисним діям з боку користувачів. Своєчасний аналіз подій безпеки дозволяє оперативно реагувати на небезпечні ситуації, що виникають унаслідок недостатньо чіткого розмежування доступу і вживати заходів протидії.

Процес аналізу зареєстрованих подій безпеки характеризується необхідністю вирішення наступних основних завдань [2]:

– об'єднання подій, отриманих з різних джерел, наприклад, зареєстрованих на різних комп'ютерах мережевого інформаційного середовища;

– усунення надмірності даних про події безпеки;

– пошук подій, що відповідають певним умовам;

– класифікація зареєстрованих подій безпеки за ступенем важливості і інформативності;

– оперативне оповіщення персоналу, відповідального за безпеку, про факти виявлення особливо важливих подій, особливо у разі автоматичної „обробки подій”;

– виявлення взаємозв’язків між подіями безпеки.

Своєчасне вирішення цих завдань дозволяє оперативно виявляти недоліки та вразливості політики безпеки та системи забезпечення інформаційної безпеки [3], а також виявляти користувачів мережевих інформаційних систем, що зловживають доступом до інформації та мережевих ресурсів або проводять шкідливу діяльність по відношенню до системи. Це, в свою чергу, дозволяє оперативно вживати заходів протидії, спрямовані на усунення небезпеки і виключення можливостей її виникнення в майбутньому. У підсумку, проведення таких заходів призводить до досягнення основної мети використання засобів захисту інформації, підвищенню рівня інформаційної безпеки в комп’ютерній мережі і мережевих інформаційних системах.

Розробка структури системи оперативного мережевого моніторингу подій безпеки (СМСБ) і розподіл функцій між її компонентами повинні проводиться з урахуванням основних вимог до системи.

Можна сформулювати такі вимоги, що впливають на структуру системи оперативного аудиту подій безпеки ІС:

1. Система повинна обробляти дані про події безпеки, що витягнуті з журналів аудиту множини комп’ютерів в мережі.

2. Результати обробки подій безпеки повинні зберігатися в єдиній базі даних подій безпеки.

3. Функції системи повинні розподілятися між компонентами, що функціонують на різних комп’ютерах мережі.

Пропонована структура системи, яка задовольняє зазначеним вимогам, показана на рисунку 1.

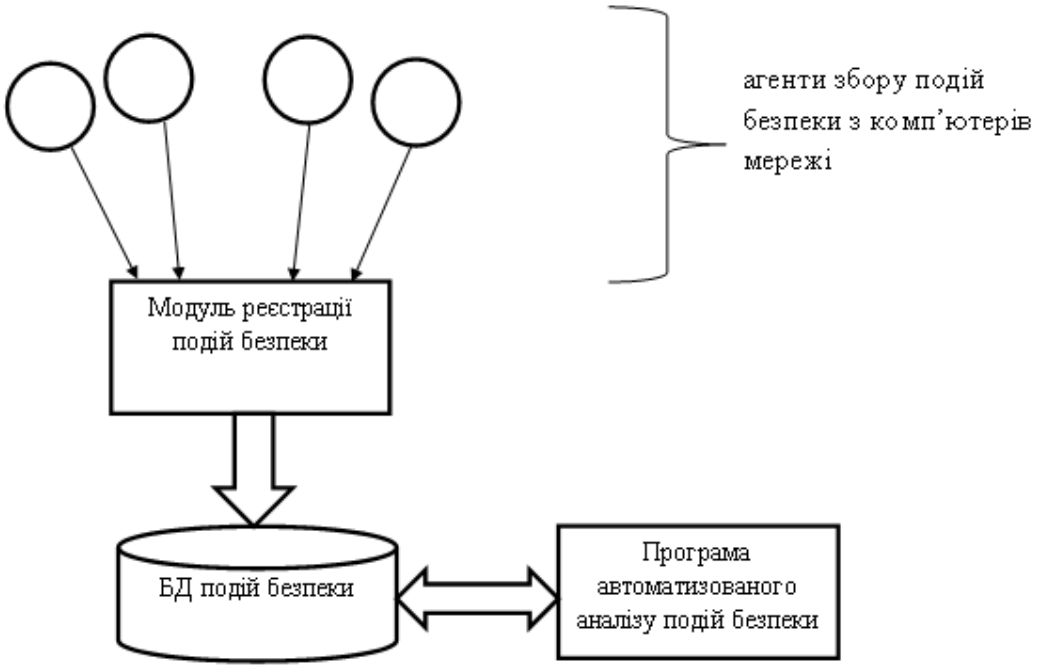

Рис. 1. Структура системи мережевого моніторингу подій безпеки

Можна виділити наступні основні компоненти такої системи:

– агенти збору подій безпеки;
– модуль реєстрації подій безпеки;
– база даних подій безпеки (БДПБ);
– програма автоматизованого аналізу подій безпеки.

Програма автоматизованого аналізу подій безпеки дозволяє адміністратору безпеки аналізувати дані про події безпеки, що зберігаються в базі даних подій безпеки. Події заносяться в БДПБ модулем реєстрації подій безпеки. Дані про події потрапляють в модуль реєстрації подій безпеки від агентів збору подій безпеки з комп'ютерів мережі, які витягують дані з журналів аудиту комп'ютерів мережі і направляють їх для обробки модулю реєстрації подій безпеки.

У сервері подій безпеки для обробки запитів агентів та отримання даних про події безпеки використовуються окремі серверні потоки. Кількість серверних потоків M не обов'язково має дорівнювати кількості N комп'ютерів в мережі, у якій функціонують агенти. Для нормальної роботи системи практично завжди достатньо і меншого числа серверних потоків, тобто $M < N$.

Серверні потоки більшу частину часу знаходяться в стані очікування запитів на підключення клієнтів, в якості яких виступають агенти системи. Коли надходить запит на підключення, один з серверних потоків, що чекає, переводиться в активний стан. Потім цей потік встановлює з'єднання з клієнтом і приймає від нього дані про оброблені події безпеки. Якщо всі серверні потоки зайняті і жоден з них не може обробити запит клієнта, то клієнт переводиться в стан очікування до тих пір, поки який-небудь з серверних потоків не звільняється і не увійде у стан очікування запитів на підключення.

Коли серверний потік отримує дані про нові події безпеки від будь-якого агента системи, він аналізує поле *Class* і виконує останній етап обробки подій безпеки в системі – подає сигнали оповіщення для подій-тривог за допомогою модуля оповіщення і зберігає події в архівну та оперативну бази даних події безпеки. Завершивши обробку отриманої партії подій безпеки серверний потік повертається в стан очікування підключень клієнтів.

При збереженні подій в бази даних серверні потоки спільно використовують загальні з'єднання з базами даних. Доступ до глобальних змінних при цьому захищається за рахунок використання таких об'єктів синхронізації як критичні секції.

Процес обробки даних аудиту подій безпеки, що одержуються від кожного з джерел – журналів аудиту комп'ютерів мережі, може бути описаний узагальненим алгоритмом, блок-схема якого представлена на рисунку 2. Згідно з цим алгоритмом, в процесі обробки даних аудиту подій безпеки можна виділити чотири основні етапи [2]:

1. Отримання даних з журналу аудиту.
2. Формалізація даних.
3. Аналіз і фільтрація подій безпеки.
4. Оповіщення персоналу про виявлені загрози і запис подій безпеки в базу даних подій безпеки.

Крім цих етапів у блок-схемі алгоритму відображені також операції управління ходом процесу обробки даних, зміст яких повністю залежить від програмного середовища, в якому функціонує система.

Отримання даних з журналу аудиту полягає у виконанні операції читання даних з файлу журналу аудиту в деякий буфер. Конкретні дії, які необхідно виконати на цьому

етапі залежать від способу організації зберігання подій безпеки в журналах аудиту. Аналіз публікацій показав, що сучасні засоби аудиту подій безпеки використовують два основних підходи для організації зберігання подій безпеки в файлах журналів аудиту – зберігання подій в структурованих файлах і зберігання подій в текстових файлах, де кожний окремий текстовий рядок задає окрему подію. Якщо дані успішно отримані, то далі необхідно формалізувати, тобто перетворити дані до структур, що використовуються в системі для подання подій. Оскільки, лічені дані про події безпеки представлені в такому форматі, в якому вони зберігаються в журналі аудиту, то необхідно їх перетворити до структури, що є зручною для подальшого подання в процесі обробки в системі. Для цього звичайно необхідно виділити з масиву інформації окремі події та значення окремих полів даних структур, які задають події. Алгоритми рішення даного завдання залежать від способу подання подій безпеки при їх зберіганні в журналах аудиту.

Події безпеки, що представлені у внутрішньому форматі системи, потім піддаються аналізу та фільтрації за ступенем важливості [2]. Для цього кожна подія перевіряється на приналежність до різних класів. Умови приналежності подій до класів задаються в системі у вигляді правил фільтрації. Правила фільтрації задають умови, що накладаються на поля даних структури події. Це дозволяють віднести подію до деяких класів. В результаті аналізу подія може бути віднесена до декількох класів одночасно.

Останнім етапом обробки подій безпеки, виділених з кожної чергової порції нових даних журналу аудиту є запис даних про події в таблиці бази даних подій безпеки. На цьому етапі також здійснюється оповіщення обслуговуючого персоналу, відповідального за інформаційну безпеку, про виявлені небезпечні ситуації та загрози за допомогою модуля оповіщення.

Після того, як будуть опрацьовані всі події, що містяться в отриманій порції даних аудиту, до обробки може бути прийнята наступна порція даних, що отрмується будь-яким з агентів системи з відповідного журналу аудиту. Оскільки агенти системи функціонують безпосередньо на контрольованих комп’ютерах мережі, то вони можуть здійснювати отримання чергових порцій даних із журналів аудиту незалежно один від одного.

Такий поділ процесу обробки подій безпеки на етапи має такі особливості:

– дані про події безпеки обробляються порціями;

– кожна порція даних повинні послідовно проходити всі етапи обробки;

– однакові етапи обробки для різних порцій даних (наприклад, отриманих з різних журналів аудиту) можуть виконуватися паралельно;

– витяг даних із журналів аудиту комп’ютерів мережі виконується агентами системи безпосередньо на комп’ютерах мережі і може проводитися одночасно і незалежно;

– наступні етапи обробки подій безпеки можуть проводитися як агентами на комп’ютерах мережі, так і монітором подій безпеки, що є центром обробки подій в системі.

Зазначені особливості процесу обробки подій безпеки дозволяють сформулювати наукове завдання синтезу ефективної структури системи моніторингу подій безпеки та ефективного розподілу функцій, що реалізують розглянуті етапи обробки, між монітором подій безпеки та агентами системи.

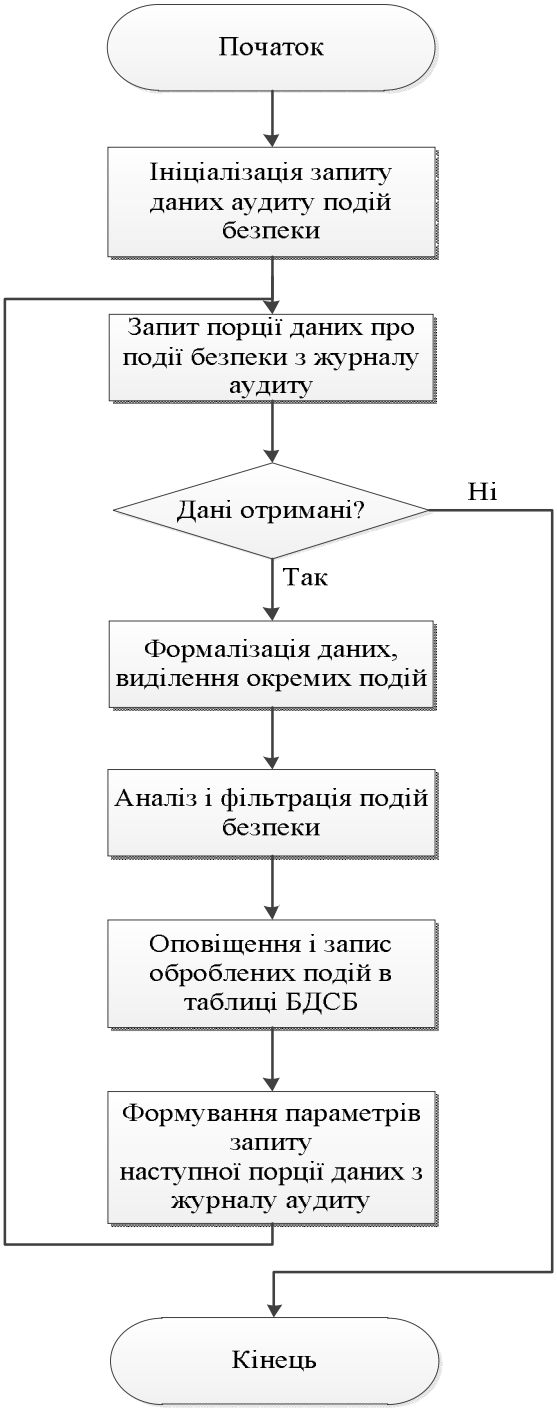

Рис. 2. Узагальнений алгоритм обробки даних аудиту подій безпеки

Необхідно ефективно організувати послідовну чотирьох-етапну обробку кожної порції даних аудиту подій безпеки, ефективно розподіливши функції, що реалізують етапи обробки між кінцевим безліччю агентів системи і єдиним монітором подій безпеки.

Методи і алгоритми програми монітора подій безпеки доцільно розробляти в розрахунку на багатопотокову реалізацію, тобто з урахуванням можливості сучасних мережевих операційних систем і можливе використання багатопроцесорної обчислювальної машини для виконання зазначеної програми. Також доцільно мінімізувати кількість з'єднань з базою даних подій безпеки, оскільки це підвищує ефективність її функціонування [4]. Використання мінімального числа з'єднань з базою даних є обмеженням, що накладаються при розробці можливих варіантів реалізації системи. На рисунку 3 розглянута постановка задачі представлена схематично.

Для знаходження ефективного рішення даної задачі необхідно розглянути всі можливі варіанти рішення і оцінити їх за допомогою деяких показників ефективності. Оскільки дана система відноситься до засобів забезпечення інформаційної безпеки, то для неї особливо важливо забезпечити високу відмовостійкість [5]. Оскільки основним завданням системи мережевого аудиту подій безпеки є оперативне виявлення небезпечних ситуацій і загроз, то доцільно обрати в якості критеріїв ефективності системи наступні характеристики:

– середній час обробки подій в системі;
– ймовірність виходу системи з ладу.

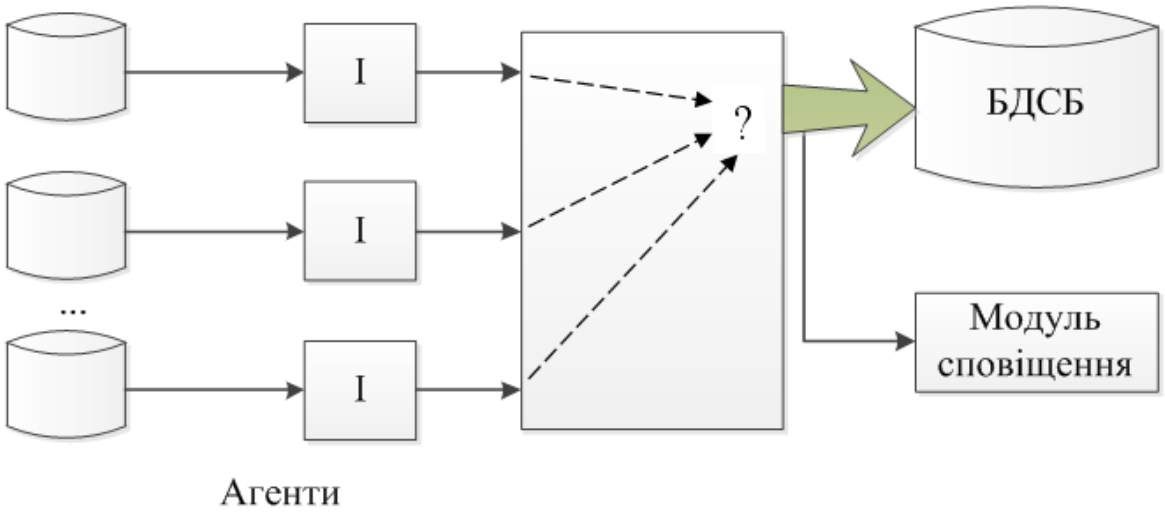

Рис. 3. Ефективний розподіл функцій обробки подій безпеки

Безліч джерел даних і, фактично, єдиний приймач результатів обробки призводить до того, що в системі буде неминуча комутація даних, що паралельно оброблюються протягом деяких початкових етапів і послідовно – протягом деяких заключних етапів. Для здійснення такої комутації необхідно використання буферної черги з синхронізацією доступу до неї.

З урахуванням вищесказаного та без урахування поділу функцій обробки між монітором і агентами, можливі чотири варіанти організації обробки подій безпеки, що показані на рисунках 4-7. На схемах використовуються такі позначення етапів обробки подій безпеки:

– „I” – отримання даних про події безпеки;
– „Ф” – формалізація даних про події безпеки;
– „А” – аналіз подій безпеки;
– „С” – збереження результатів і оповіщення.

Схеми організації обробки подій безпеки показані на рис. 4-7.

У схемі „*А*” отримання даних із журналів аудиту виконується паралельно, а наступні етапи обробки виконуються послідовно. Жирна вертикальна лінія позначає синхронізацію елементів системи при комутації етапів обробки, що виконуються різними елементами системи. Такими елементами є процеси і потоки компонентів системи.

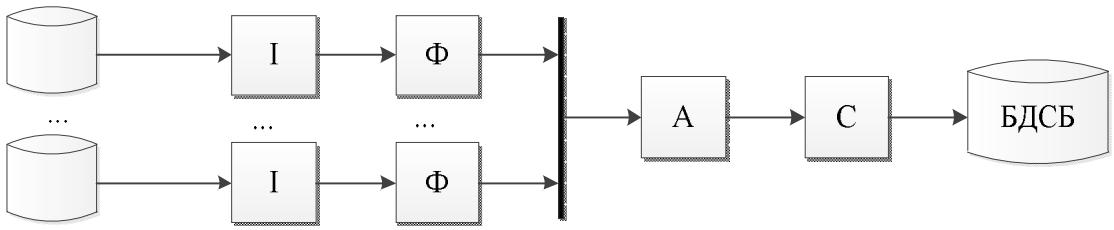

Рис. 4. Схема „*A*” організації обробки подій безпеки в системі

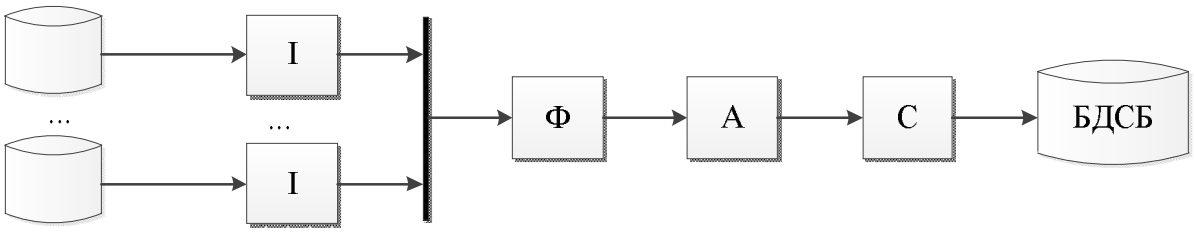

Рис. 5. Схема „*B*” організації обробки подій безпеки в системі

У схемі „B” паралельно виконуються отримання даних із журналів аудиту та їх формалізація, а наступні етапи обробки виконуються послідовно.

На рисунку 6 показана схема „*C*” організації обробки подій безпеки. У схемі „*C*” паралельно виконуються отримання даних із журналів аудиту, формалізація даних і аналіз подій безпеки, а наступні етапи обробки виконуються послідовно.

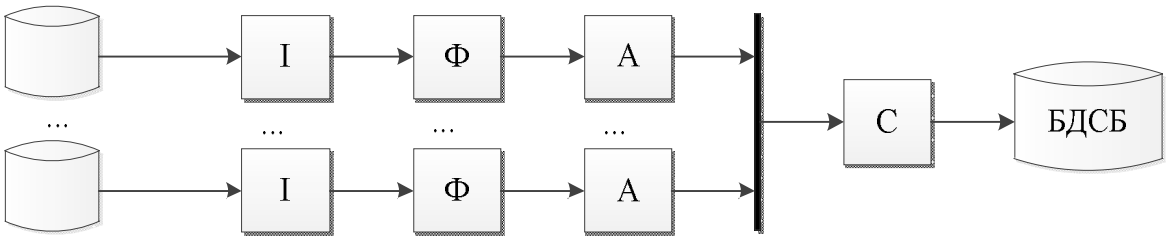

Рис. 6. Схема „*C*” організації обробки подій безпеки в системі

На рисунку 7 показана схема „*D*” організації обробки подій безпеки. Особливістю схеми „*D*” є те, що всі етапи обробки подій безпеки виконуються паралельно. Це приводить або до необхідності використання безлічі з’єднань з базою даних, або до синхронізованого використання мінімальної кількості з’єднань.

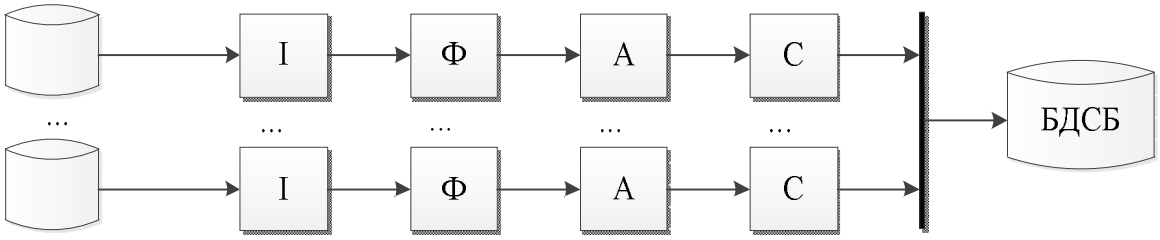

Рис. 7. Схема „D” організації обробки подій безпеки в системі

Розглянуті схеми організації обробки подій безпеки не відображають розподілу функцій обробки між модулями системи-безліччю агентів і єдиним монітором подій безпеки. Однак вони дозволяють розглянути можливі варіанти такого розподілу.

При розгляді можливих варіантів вирішення задачі розподілу функцій обробки подій безпеки між модулями системи доцільно також виводити вирази для обчислення показників ефективності організації процесу обробки подій безпеки для розглянутих варіантів.

Література:

1.Курило А. П. Аудит информационной безопасности. / А. П. Курило. – М. : БДЦ-пресс, 2006. – 304 с.

2.Макаревич О.Б. Регистрация и анализ событий безопасности в информационных системах. / Макаревич О.Б., Шелудько И.А. Известия ТРТУ. Тематический выпуск. Материалы V Международной научно-практической конференции „Информационная безопасность", Таганрог: ТРТУ, 2003, с. 211-216.

3.Норткат С. Анализ типовых нарушений безопасности в сетях. Киев: Лорри, 2001. – 192с.

4.Глушаков С.В. Базы данных. / Глушаков С.В., Ломотько Д.В. – М: 000 „Издательство АСТ". Харьков: Фолио, 2002. – 504 с.

5.Безкоровайный М.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем. / Безкоровайный М.М., Костогрызов А.И., Львов В. М. – М.: Вооружение. Политика. Конверсия. 2001. – 313 с.