УДК 681.3

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД НСД “РУБІЖ”. ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ БЕЗПЕКОЮ КОРПОРАТИВНОЇ СИСТЕМИ

Микола Будько, Вячеслав Василенко, Михайло Короленко, Олександр Буточнов
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонується використання в розподілених корпоративних мережах розробленого в ВАТ “КП ОТІ” комплексу засобів захисту з ієрархічною структурою та централізованим управлінням.**
Summary: **Use in the distributed(allocated) corporate networks developed in OJC “KP VTI” of a complex of means of protection with hierarchical structure and centralized management is offered.**
Ключові слова: **Інформація, інформаційна безпека, засоби захисту.**

І Вступ

Широке впровадження інформаційно-телекомунікаційних технологій в усі сфери життя суспільства висуває на перший план питання інформаційної безпеки. Збільшення обсягу оброблюваної інформації та інформації, що накопичується, зростання важливості інформації для прийняття рішень на корпоративному і державному рівні, територіальна розподіленість інформаційних систем, можливість віддаленого доступу до ресурсів корпоративної мережі, з одного боку, роблять інформаційні системи досить привабливим об'єктом для атак, а з іншої, надають технічні можливості для реалізації таких атак.

Одним з основних напрямків створення систем захисту інформації є побудова систем захисту інформації від несанкціонованого доступу. Такі системи встановлюються на автономні чи мережні комп'ютери і відповідають за розмежування доступу користувачів до інформації, що зберігається на цих комп'ютерах. Стирання чіткої межі між відкритою і закритою мережами приводить до необхідності розробки комплексних систем захисту, включаючи системи захисту від несанкціонованого доступу, міжмережні екрани і системи виявлення атак**.**

В даний час у світі зареєстровано більш як 1000 фірм, що переймаються питаннями інформаційної безпеки, при цьому, майже половина цих фірм знаходиться в США. До їхнього числа в першу чергу варто віднести компанії ISS (Internet Security Systems), Symantec Enterprise Security, Cisco Systems, Novell, Check Point Software Technologies, Raptor Systems, Secure computing, Lucent, Axent Technologies, Memco Software, Security Dynamics, ON Technologies, Network Associates, IBM, Oracle і ін.

Інтерес до розробки систем захисту інформації в Україні значно виріс за останні роки. До числа фірм, що розробляють комплексні системи захисту інформації, варто віднести, у першу чергу, Geos Inform, ТОВ “Інститут комп'ютерних технологій”, АТ “Інститут інформаційних технологій”, Цебит, Інком та ін.

Відкрите акціонерне товариство “КП ОТІ”, яке є головним розробником складних гетерогенних корпоративних та державних автоматизованих систем (“Експрес-УЗ”, ЄДАПС), не могло залишити поза своєю увагою проблему захисту інформації в АС. З цією метою в 1996 році у ВАТ “КП ОТІ” було створено Центр технічного захисту інформації.

Центр технічного захисту інформації ВАТ “КП ОТІ” здійснює свою діяльність на підставі ліцензії Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Видами діяльності центру є: розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу, надання консультативних послуг з наданням права технічного захисту інформації усіх видів, у тому числі інформації, що містить відомості, які становлять державну таємницю.

У рамках ліцензійної діяльності в 1996-2002 р.р. центром ТЗІ ВАТ “КП ОТІ” розроблено та частково впроваджено “АРМ адміністратора підсистеми захисту інформації АСК “Експрес-УЗ” та Підсистему контролю доступу та захисту інформації ЄДАПС. Досвід розробки таких систем показав, що замовник чи власник автоматизованої системи не завжди готовий до формулювання конкретних вимог захисту інформації в АС. Нажаль, необхідний для формалізації вимог до системи захисту інформації в АС час – незмірно малий порівняно з часом, необхідним для їх реалізації. Тому, в основу розробок ЦТЗІ ВАТ “КП ОТІ” було покладено концепцію інтеграції комплексних засобів захисту платформи функціонування АС в єдину систему захисту інформації, що керується з одного центру.

У даній статті розглядається запропонований та реалізований авторами в системі захисту інформації від НСД (СЗІ) “Рубіж” підхід до побудови комплексної системи захисту інформації в АС.

ІІ Загальна характеристика СЗІ “Рубіж”

СЗІ “Рубіж” призначено для забезпечення основних функціональних властивостей захищеності ресурсів АС, передбачених вимогами нормативних документів Системи технічного захисту інформації, таких як: конфіденційність, цілісність, доступність, спостереженість.

Структура СЗІ “Рубіж” відповідає структурі ієрархічної розподіленої автоматизованої системи класу 3, захист інформації якої вона забезпечує. Тому надалі СЗІ “Рубіж” може розглядатися як централізована багаторівнева ієрархічна система захисту інформації від НСД, яка складається з КЗЗ рівнів та засобів забезпечення їх взаємодії. Загальна структура СЗІ як сукупності КЗЗ певних рівнів АС, наведена на рис. 1. Кількість рівнів може бути різною для різних АС.

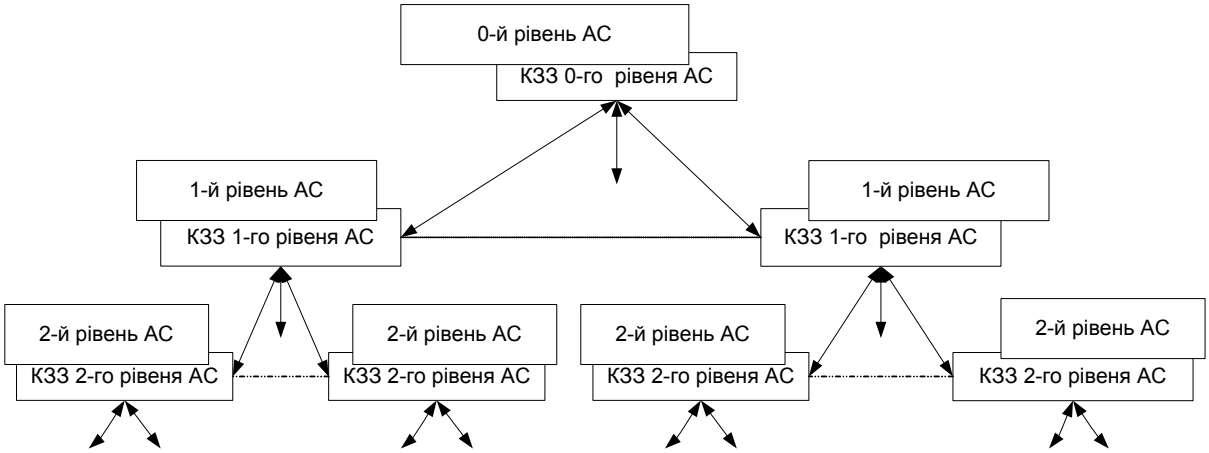

Рисунок 1 – Загальна структура СЗІ “Рубіж”

У свою чергу, комплекси засобів захисту кожного з рівнів АС інтегрують у своєму складі визначені платформою та умовами функціонування АС механізми захисту інформації.

Комплекси засобів захисту кожного рівня АС мають уніфіковану структуру і можуть різнитися складом проблемно-орієнтованих засобів захисту та визначеною політикою захисту функціональністю.

До складу КЗЗ кожного рівня входять монітор безпеки (МБ) у складі автоматизованого робочого місця адміністратора безпеки та серверу МБ. Монітор безпеки інтегрує через своїх агентів в єдину систему керування захистом:

1) засоби захисту домену;
2) засоби захисту функціональних робочих місць у складі засобів автентифікації, засобів захисту операційної системи та засобів управління фізичним доступом до робочих станцій – “Рубіж – РС”;
3) засоби підсистеми управління фізичним доступом до території та приміщень вузла АС – “Рубіж – Ф”;
4) засоби захисту баз даних (БД) рівня АС;
5) засоби захисту комунікаційної мережі зв'язку;
6) засоби криптографічного захисту інформації;
7) засоби антивірусного захисту;
8) засоби резервного копіювання та відновлення інформації КЗЗ, операційного середовища та БД.

Крім монітора безпеки в СЗІ входять агенти монітора безпеки, які здійснюють взаємодію з програмно-технічними та проблемно-орієнтованими засобами захисту (функціональних АРМ, контролеру домену та мережних серверів, операційних систем та СКБД).

Монітор безпеки СЗІ “ Рубіж” у складі АРМ адміністратора безпеки та сервера монітора безпеки (майстер-агента) є програмно-технічним ядром системи захисту, яке забезпечує централізоване управління КЗЗ та взаємодію його елементів. Програмні засоби монітора безпеки разом з програмно-технічними та проблемно-орієнтованими засобами захисту інтегруються в єдину систему захисту інформації АС і забезпечують захист його ресурсів згідно з визначеним функціональним профілем захищеності.

Інтегрування здійснюється шляхом використання агентів монітора безпеки (агент МБ), які розташовуються на серверах та робочих станціях АС. Агент є компонентом, який забезпечує взаємодію монітора безпеки з проблемно-орієнтованими засобами захисту (ПОЗЗ) для реалізації основних

функціональних послуг безпеки. Програмні засоби монітора безпеки АС (зокрема АРМ адміністратора безпеки), окрім того, забезпечують зручний та інтуїтивно зрозумілий інтерфейс адміністратора безпеки АС. Структура (склад та взаємозв'язки) КЗЗ АС представлено на рис. 2.

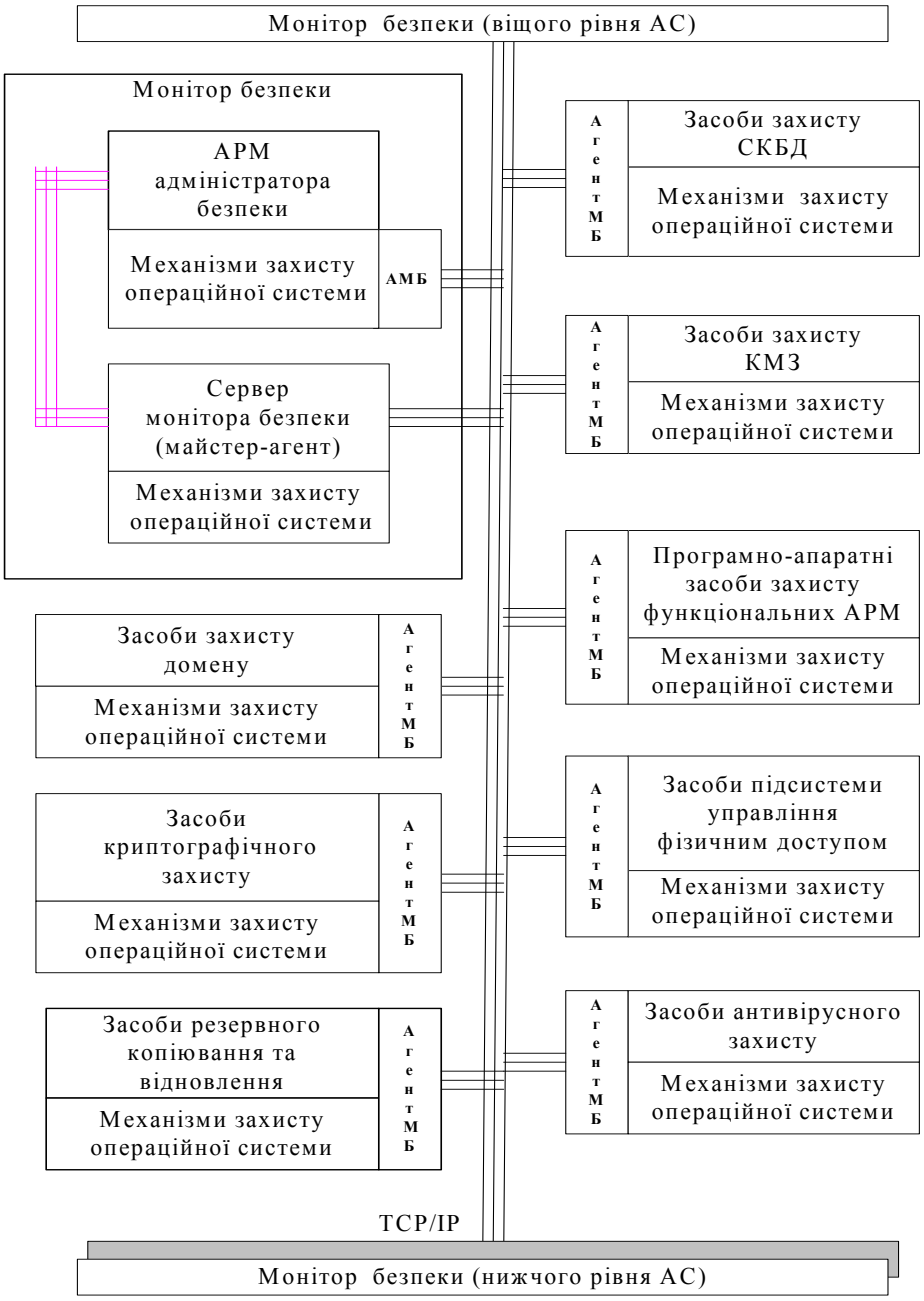

Рисунок 2 – Структурна схема КЗЗ рівня АС

Сервер монітора безпеки СЗІ. Сервер монітора безпеки забезпечує реалізацію бізнес-логіки функціонування системи захисту інформації АС від НСД, зберігання параметрів моделі системи захисту, конфігурації системи, ведення та обробку журналів подій, зберігання параметрів аудиту системи та реагування на критичні події, автентифікацію адміністраторів (агентів), мережну взаємодію з АРМ адміністратора безпеки та агентами МБ, формування команд для взаємодії з ПОЗЗ, відслідковування подій та видачу інформації на АРМ адміністратора безпеки для керування КЗЗ. Структурна схема серверу монітора безпеки представлена на рис. 3.

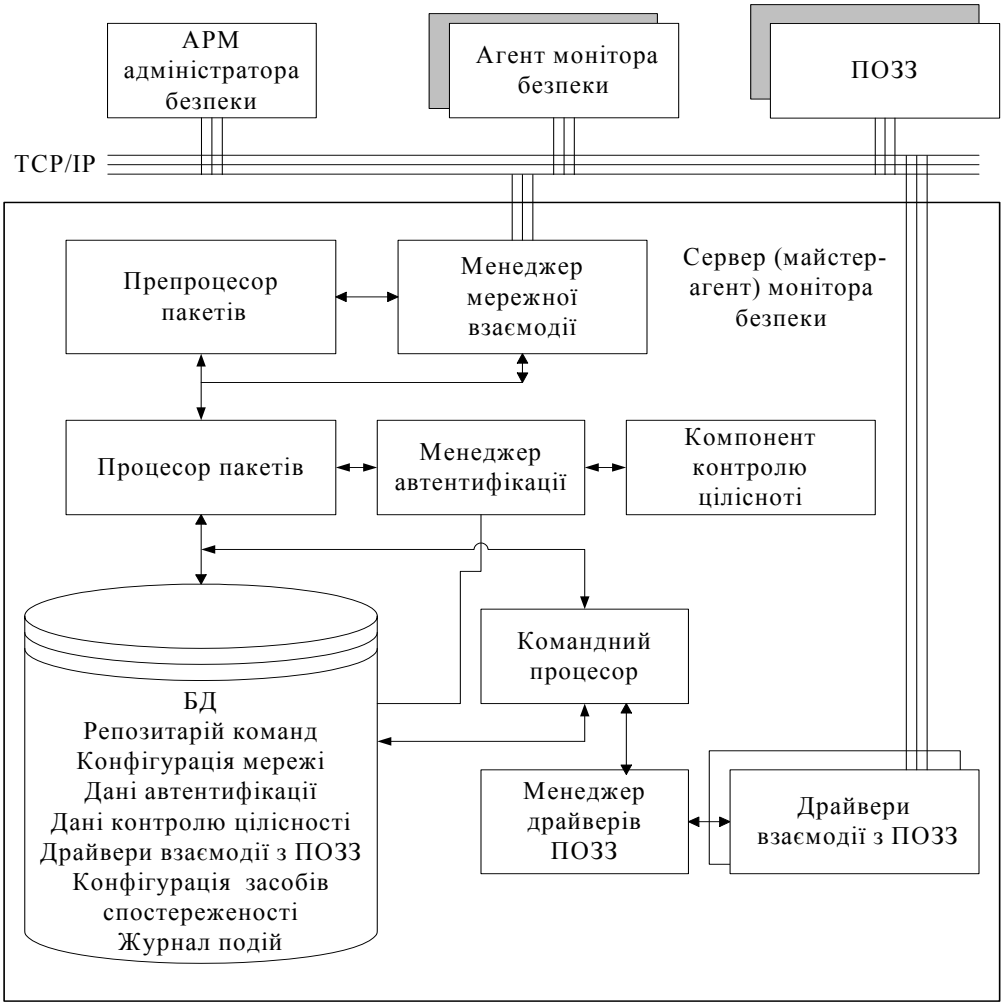

Рисунок 3 – Узагальнена структурна схема серверу монітора безпеки КЗЗ

Взаємодія монітора безпеки з ПОЗЗ. Взаємодія монітора безпеки з проблемно–орієнтованими засобами захисту (функціональних АРМ, контролера домену, операційних систем та СКБД) забезпечується його структурним елементом – сервером монітора безпеки за схемою:

АРМ адміністратора ↔ сервер МБ ↔ агент монітора безпеки↔ПОЗЗ.

Взаємодія з програмно-технічними та проблемно-орієнтованими засобами захисту інформаційних ресурсів кожного з хостів здійснюється через окремі функціональні компоненти – агенти МБ, які інсталюються на окремих серверах та робочих станціях АС (рис. 2). Кожний агент для взаємодії з проблемно-орієнтованими засобами захисту має набір драйверів відповідно до складу ПОЗЗ. Для інтегрування інших ПОЗЗ, не передбачених в складі КЗЗ, необхідно розробити відповідний драйвер та інсталювати його на сервері та агенті МБ. Крім того, це потребує включення функцій взаємодії з ПОЗЗ в інтерфейс користувача (АРМ адміністратора безпеки). Такий підхід дозволяє подальшу модифікацію СЗІ без значних витрат. Слід відмітити, що КЗЗ СЗІ “Рубіж” розроблені з урахуванням такої модифікації програмних засобів. Агенти МБ СЗІ “Рубіж” призначені для виконання команд керування механізмами захисту ПОЗЗ, відслідковування подій та видачі інформації та повідомлень на АРМ адміністратора безпеки. Агент МБ приймає команди на адміністрування ПОЗЗ від АРМ адміністратора, виконує команди і відправляє монітору безпеки інформацію про результати їх виконання. Крім того, агент МБ відслідковує події на ПОЗЗ, видає інформацію про події монітору безпеки і забезпечує реагування на критичні події.

У випадку відсутності зв'язку з монітором безпеки (або його непрацездатністю) агент МБ автономно виконує функції захисту інформаційних ресурсів хосту, відслідковує події, забезпечує реагування на критичні події. При відновленні зв'язку з монітором безпеки всю необхідну інформацію агент пересилає на монітор безпеки для подальшої обробки і прийняття відповідних рішень.

Структура агента монітора безпеки аналогічна структурі серверу монітора безпеки (рис. 3) і відрізняється тільки функціональністю.

АРМ адміністратора безпеки СЗІ "Рубіж". Програмні засоби АРМ адміністратора безпеки СЗІ забезпечують зручний та інтуїтивно зрозумілий інтерфейс для адміністратора безпеки і є програмними модулями, що функціонують у середовищі Windows NT/2000. Загальна структурна схема АРМ адміністратора безпеки відображена на рис. 4.

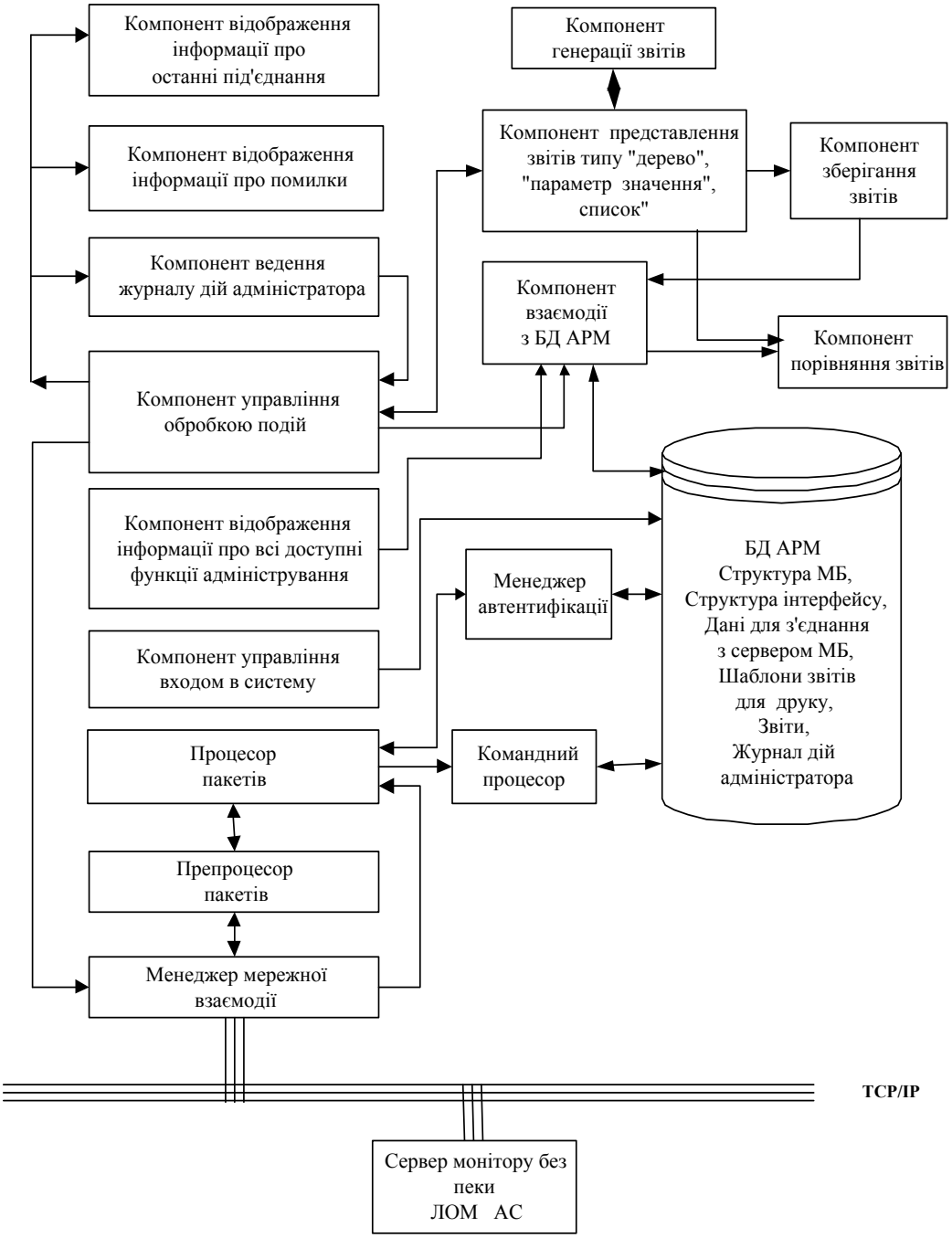

Рисунок 4 – Загальна структурна схема АРМ адміністратора безпеки

Інтерфейс забезпечує введення та відображення інформації, необхідної для налагодження та керування механізмами захисту АРМ адміністратора безпеки, а також відслідкування подій, що впливають на стан захищеності АС.

III Забезпечення захисту інформації від НСД в АС засобами СЗІ “Рубіж”

Захист інформації в АС з використанням засобів СЗІ “Рубіж” здійснюється шляхом автоматизованого забезпечення функціональних послуг захищеності, які реалізуються у відповідності до визначеної політики безпеки. Вимоги політики безпеки формалізуються у вигляді відповідних моделей захищених систем (АС у цілому, її підсистем – рівнів АС та їх елементів). Моделі відповідають архітектурі захищених систем, а їх параметри визначаються адміністратором безпеки через засоби АРМ моніторів безпеки КЗЗ вузлів кожного з рівнів

Модель захищеної системи. Модель захищеної системи СЗІ “Рубіж” включає:

- структуру системи, що захищається;
- структуру власне СЗІ;
- структуру суб'єктів інформаційної діяльності;
- структуру об'єктів захисту;
- правила розмежування доступу;
- правила забезпечення спостереженості за станом систем;
- правила реагування на критичні події.

Суб'єктами інформаційної діяльності КЗЗ “Рубіж” є:

- адміністратор безпеки;
- системні та мережні адміністратори АС;
- адміністратори функціональних підсистем АС;
- користувачі ресурсів АС.

Об’єктами захисту СЗІ “Рубіж” є:

- системні ресурси АС – ресурси операційних систем, системних та мережевих служб, власне СЗІ;
- інформаційні ресурси АС (об'єкти СКБД, файли);
- інформаційні ресурси власне КЗЗ АС (об'єкти БД КЗЗ: параметри моделі і конфігурація системи захисту, параметри автентифікації користувачів, журнали подій, журнали дії адміністраторів, архіви журналів, звіти про стан захищеності системи, параметри аудиту подій, параметри реагування на події та ін.);
- прикладні ресурси (програмне забезпечення АС).

Правила розмежування доступу визначаються встановленою власником АС політикою безпеки і полягають у наданні повноважень суб'єктам АС на доступ до ресурсів, які захищаються, а також у встановленні типів доступу суб'єктам до об'єктів захищеної системи. На основі такої інформації за внутрішніми алгоритмами перевірки повноважень диспетчери доступу ПОЗЗ реалізують санкціонування доступу суб'єкта до об'єкта. Таким чином забезпечується довірчий та адміністративний принципи керування доступом.

Моделі захисту вузлів кожного з рівнів АС складаються з моделі монітора безпеки, як захищеної системи, і моделей об’єктів захисту вузла. Узагальнена модель захисту рівня АС представлена на рис. 5.

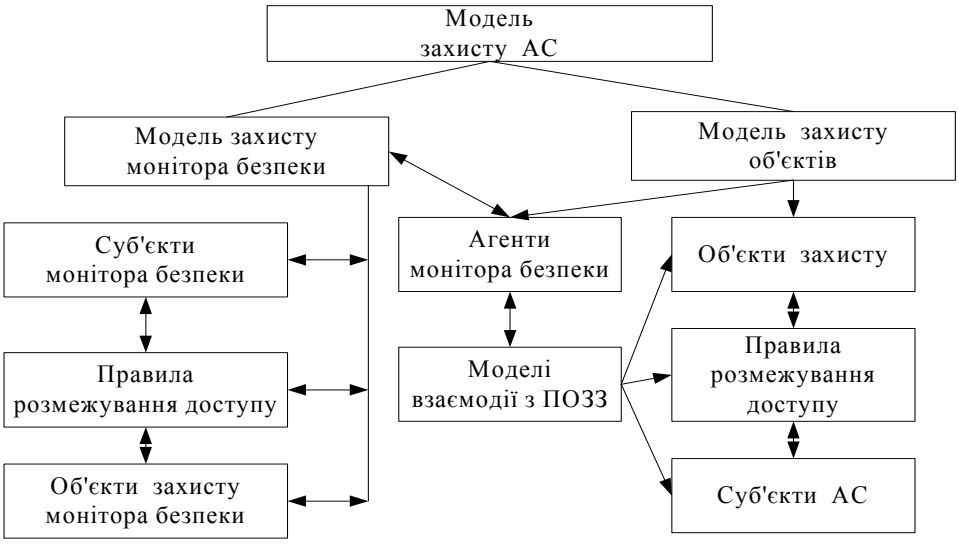

Рисунок 5 – Узагальнена модель захисту АС

Реалізація функцій побудови моделі захищеної системи. Формування кожної складової моделі захищеної системи здійснюється при інсталяції монітора безпеки АС і ПОЗЗ. При інсталяції виконуються необхідні дії для формування конфігураційних файлів монітора безпеки, файлів ініціалізації ПОЗЗ, зміни паролів користувачів, створення облікових записів адміністраторів з певними повноваженнями, створення профілів користувачів, формування необхідних ролей, системних, об'єктних привілеїв та ін. Внаслідок виконання процедури ініціалізації має бути створена конфігурація захищеної системи відповідно до вимог політики безпеки. Адміністратор безпеки через функції інтерфейсу фіксує створену модель захищеної системи в базі даних, на власному паролі формує ознаку цілісності і включає модель захищеної системи, як об'єкт захисту, до складу об'єктів контролю компонента контролю цілісності. Модель захищеної системи використовується для спостереження за всіма спробами зміни її параметрів (еталонна модель).

При необхідності проведення зміни параметрів моделі захищеної системи, у разі зміни політики безпеки, адміністратор безпеки з використанням функцій адміністрування монітора безпеки виконує необхідні налагодження відповідних ПОЗЗ, формує звіт про внесені зміни, на власному паролі формує нову ознаку цілісності і зберігає нову версію моделі захищеної системи в базі даних АРМ адміністратора безпеки.

Всі дії адміністраторів, пов’язані зі спробами зміни параметрів моделі захищеної системи, фіксуються в базі даних монітора безпеки (відповідно до правил реалізації механізмів захисту). Монітор безпеки реагує на події і надає інформацію для відображення. Адміністратор перевіряє спроби зміни параметрів моделі захищеної системи шляхом порівняння звітів про події з еталонної моделлю.

Реалізація функцій реєстрації подій та реагування на критичні події. Монітор безпеки АС забезпечує постійне збирання інформації про події, що відбулися в захищеній системі, або за допомогою таймерного опитування ПОЗЗ, або відслідковуючи сигнали, що генеруються ПОЗЗ. Функції збору інформації про події виконуються компонентом керування динамічним відслідковуванням подій. Також монітор безпеки реагує на певні події відповідно до правил, що зберігаються в БД. Функції реагування на події виконуються компонентом сповіщення про події та реагування.

Користувач АРМ (адміністратор безпеки) має можливість переглядати інформацію про події, що відслідковуються сервером у режимі реального часу, а також виконувати функції аудиту журналу подій за допомогою складних запитів, побудова яких виконується за допомогою зручного інтерфейсу користувача. При виконанні функцій аудиту та перегляду подій відбувається перевірка повноважень механізмами розмежування доступу монітору безпеки.

Взаємодія моніторів безпеки (для розподілених та ієрархічних АС). Взаємодія моніторів безпеки здійснюється відповідно до політики безпеки АС вцілому.

Адміністратор безпеки вищого рівня АС має право на виконання певних функцій на моніторі безпеки нижчого рівня, які стосуються контролю за діями адміністраторів і припиненню їх повноважень у разі деяких порушень, контролю за станом захищеності системи і отриманню журналів подій. Модель захищеної системи (суб’єкти, об’єкти захисту, повноваження суб’єктів на доступ до об’єктів захисту) має формуватися на підставі даних моделі захищеної системи АС з урахуванням особливості функцій роботи з базою даних. Монітор безпеки відправляє повідомлення про порушення політики безпеки на нижчому рівні до адміністратора безпеки вищого рівня АС, а також передбачені політикою безпеки звіти.

Стан робіт зі створення СЗІ “Рубіж”, напрямки подальшого розвитку системи. СЗІ АС від НСД “Рубіж” пройшла попередні випробування і готується для дослідної експлуатації. Попередні випробування підтвердили робоспроможність системи, спроможність системи формувати модель захищеної системи, конфігурувавти монітори безпеки різних рівнів, забезпечити захист ресурсів АС від передбачених загроз та реагування на спроби порушення правил розмежування доступу.

СЗІ “Рубіж” за проектною оцінкою відповідає функціональному профілю захищеності 3.КЦД.2, який є близьким до стандартного функціонального профілю захищеності 3.КЦД. Функціональний профіль захищеності визначається характеристиками інформації, що зберігається, архітектурою побудови АС як автоматизованої системи класу 3 (згідно з нормативним документом системи технічного захисту інформації НД ТЗІ 2.5–005–99 “Класифікація автоматизованих систем та стандартні функціональні профілі захищеності інформації, що обробляється, від несанкціонованого доступу”) та функціональними критеріями захищеності інформації (згідно з нормативним документом системи технічного захисту інформації НД ТЗІ 2.5–004–99 “Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу”). Семантика проектного функціонального профілю захищеності СЗІ “Рубіж”:

3.КЦД = {КД–2, КА–2, ДО–1, ЦД–2, ЦА–2, ЦВ–1, ЦО–2, ДВ-1; ДР–1, ДС–1, ДЗ–2, НР–5, НІ–3, НК–1, НО–3, НЦ–2, НТ–3},

де - КД–2 – базова довірча конфіденційність; КА–2 – базова адміністративна конфіденційність; ДО–1 – повторне використання об’єктів; ЦД–2 – базова довірча цілісність; ЦА–2 – базова адміністративна цілісність; ЦВ–1 – базова цілісність інформації при обміні; ЦО–2 – повний відкат; ДВ-1 - ручне відновлення;

ДР–1 – квоти на використання ресурсів; ДС–1 – стійкість при обмежених відмовах; ДЗ–2 – обмежена гаряча заміна; НК–1 – однонаправлений достовірний канал; НР–5 – аналіз у реальному часі; НІ–3 – множинна ідентифікація і автентифікація; НО–3 – розподіл обов'язків на підставі привілеїв; НЦ–2 – комплекс засобів захисту (КЗЗ) з гарантованою цілісністю; НТ–3 – самотестування в реальному часі.

В даний час розроблено драйвери для інтеграції в СЗІ власних (вбудованих) механізмів захисту СКБД Oracle, DB2 і операційних систем OS/390, AIX, MS Windows NT/2000. У стадії розробки знаходяться драйвери для інтеграції операційної системи Linux.

Література: 1. Нормативний документ Системи технічного захисту інформації "Загальні положення про захист інформації в комп'ютерних системах від несанкціонованого доступу" (НД ТЗІ 1.1 – 002 – 99). 2. Нормативний документ Системи технічного захисту інформації "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД" (НД ТЗІ 2.5 – 004 – 99). 3. Нормативний документ Системи технічного захисту інформації "Класифікація автоматизованих систем та стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [НД ТЗІ 2.5.–005 –99]. 4. Нормативний документ Системи технічного захисту інформації "Типове положення про службу захисту інформації в автоматизованій системі" (НД ТЗІ 1.4–001–2000). 5. Будько М. М., Василенко В. С., Короленко М. П. Архитектура системы защиты информации // К. Комиздат //Корпоративные системы // № 4, 1999. 6. Будько М. М., Василенко В. С., Короленко М. П., Федченко Є. Л. Архитектура системы технической защиты информации // К. НТУ "КПІ" //Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні// 2000, с.62-68. 7. Будько М. М., Василенко В. С., Короленко М. П. та ін. Архитектура системы защиты информации // К. В науковому виданні Безопасность информационных технологий. Методология создания систем защиты/ В. В. Домарев. К.: ООО "ТИД "ДС"", 2001. – 681 с. Частина V. Решения и средства защиты информации.

УДК 681.06

ИЗМЕРИТЕЛЬ НИЗКОЧАСТОТНЫХ МАГНИТНЫХ ПОЛЕЙ

Владислав Галанский, Александр Лаврентьев, Михаил Прокофьев
Научно-исследовательский центр «ТЕЗИС» НТТУ «КПИ»

Анотація: **Розроблено вимірювач низькочастотних магнітних полів, призначений для виявлення і визначення інтенсивності джерел випромінювання. Прилад дозволяє контролювати рівень низькочастотних магнітних полів у приміщеннях з метою оцінки захищеності об'єктів інформаційної діяльності. Розглянуто області практичного застосування вимірювача.**
Summary: **The meter of low frequency magnetic fields intended for the detection and position determination of stimulus sources Is designed. The device allows to control ecological safety of sources of low frequency magnetic fields in habitation and workrooms and to make estimation of hardening of means of electronic - computer facilities from intercepting the confidential information on channels of spurious electromagnetic radiations and aimings. Fields of practical application are reviewed.**
Ключові слова: **Низькочастотне магнітне поле, магнітометр.**

I Введение

Проблемы низкочастотных магнитных полей (НМП) привлекают все более пристальное внимание не только разработчиков и пользователей электронной аппаратуры, но и экологов и медиков, занимающихся изучением изменения экобиосистемы под влиянием неионизирующих электромагнитных излучений. Сегодня доказательно определены и конкретизированы наиболее чувствительные и критичные к воздействию низкочастотных магнитных полей системы организма человека: генетическая, нервная, иммунная, эндокринная и половая. Наибольший интерес представляют исследования НМП в области промышленных частот 50 Гц и их гармоник, а также в области очень низких радиочастот (VLV): 3 – 30 кГц и низких частот (LV): 30–300 кГц. Основной причиной такого интереса к НМП является их высокая проникающая способность и трудность определения местоположения и эффективности экранирования источника излучения, поскольку на сравнительно низких частотах наиболее сложно обеспечить эффективное экранирование магнитной составляющей электромагнитного поля. К примеру, экраны из бетонных или свинцовых плит, либо водяные резервуары, полностью поглощающие жесткое радиоактивное излучение, не являются преградой при распространении слабых НМП [1].