Перед тим як дозволити будь-кому виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ має автентифікувати цього користувача з використанням захищеного механізму. Сервер безпеки RACF виконує автентифікацію суб'єкта на основі паролю або спеціальної карти (operation ID card).

КЗЗ має забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування. В базі даних RACF пароль зберігається в зашифрованому вигляді.

НО-2. Розподіл повноважень адміністраторів. Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування.

Механізми захисту OS/390 дозволяють призначати суб'єкту повноваження адміністратора на рівні групи, що дозволяє уникнути авторитарності керування та зменшити можливі збитки.

НЦ-2. КЗЗ з гарантованою цілісністю. Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Диспетчер доступу RACF насамперед захищає свою базу даних та власні механізми захисту. Заборона видачі команд RACF за допомогою відповідних опцій дозволяє гарантувати доступ лише через засоби системи захисту "Рубіж".

НТ-2. Самотестування при старті. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій комп'ютерної системи. Гарантується прикладним програмним забезпеченням КС та засобами самотестування OS/390.

Таким чином, програмне забезпечення системи „Рубіж" дозволяє інтегрувати в своєму складі механізми розмежування доступу операційної системи OS/390, централізовано адмініструвати RACF і відслідковувати події в захищеній системі, забезпечувати довірче обчислювальне середовище для програмних засобів, що розташовані на платформі OS/390 (СКБД Oracle, DB2) та забезпечувати необхідний профіль захищеності ресурсів.

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).

УДК 681.3

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД НСД "РУБІЖ". ВАРІАНТ РЕАЛІЗАЦІЇ АЛГОРИТМУ МНОЖИННОЇ АВТЕНТИФІКАЦІЇ

Микола Будько, Олександр Буточнов, Вячеслав Василенко, Василь Сергієнко, Володимир Стрюченко*, Станіслав Могильний, Олександр Терлецький

Відкрите акціонерне товариство "КП ОТІ",

**Науково-виробниче об'єднання "Електронмаш"*

Анотація: **Для систем захисту ієрархічних автоматизованих систем "Рубіж" пропонується алгоритм множинної автентифікації з використанням можливостей програмно-технічних засобів управління доступом до ресурсів автоматизованих систем.**

Summary: **For systems of protection the hierarchical automated systems "Rubyg" is offered algorithm of multiple authentication with use of opportunities program-technical means of management of access to resources of the automated systems.**

Ключові слова: **Технічний захист інформації, ідентифікація, автентифікація.**

І Засоби захисту робочих станцій "Рубіж-РС"

Засоби захисту робочих станцій "Рубіж-РС" є елементом комплексу засобів захисту (КЗЗ) "Рубіж" і знаходяться під централізованим управлінням його монітора безпеки (МБ). До складу засобів захисту "Рубіж-РС" входять засоби автентифікації, засоби захисту операційної системи та систем керування базами даних (при їх наявності), засоби контролю цілісності та програмно-технічні засоби управління доступом. Схема взаємодії засобів "Рубіж-РС" з МБ представлена на рис. 1.

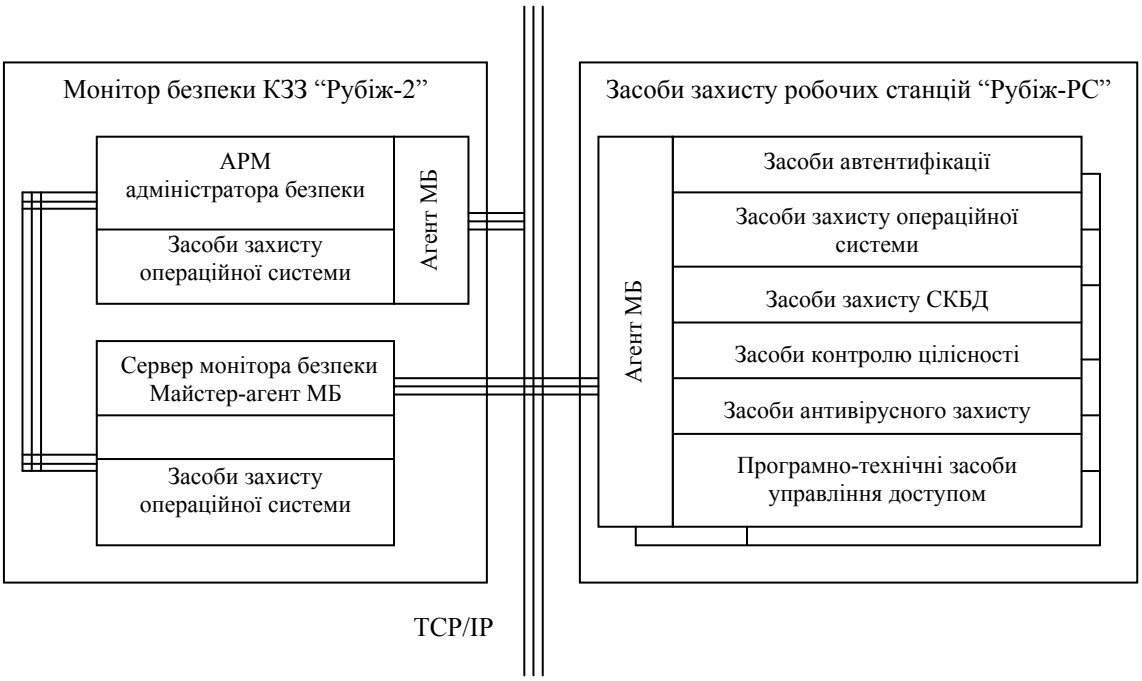

Рисунок 1 – Схема взаємодії засобів захисту робочих станцій “Рубіж-РС” з монітором безпеки КЗЗ “Рубіж-2”

Програмно-технічні засоби управління доступом забезпечують запобігання або суттєве перешкоджання несанкціонованого доступу до ресурсів робочих станцій АС. Основними задачами цих засобів є:

- інтеграція в єдину систему захисту з централізованим управлінням від МБ вузла АС;
- ідентифікація та автентифікація суб’єктів при включенні живлення робочої станції;
- блокування завантаження операційної системи при відсутності повноважень на включення у суб’єкта, який пред’явив ідентифікатор;
- ідентифікація та автентифікація суб’єкта при завантаженні ОС;
- блокування роботи робочої станції при відсутності відповідних повноважень суб’єкта, що пред’явив ідентифікатор;
- контроль наявності ідентифікатора суб’єкта в зчитувачі в процесі роботи, блокування роботи станції в разі його тимчасової відсутності;
- зв’язок з монітором безпеки через його агента на робочій станції;
- однозначна ідентифікація робочої станції при її реєстрації в домені, контроль цілісності конфігурації технічних засобів робочої станції;
- однозначна прив’язка агента МБ до робочої станції;
- контроль цілісності програмного забезпечення агента МБ;
- контроль несанкціонованого відкривання корпусу робочої станції в т. ч. і при виключеному живленні;
- оповіщення АРМ адміністратора керування фізичним доступом про несанкціоноване механічне втручання;
- автономне живлення і реєстрація подій при виключеному живленні станції.

II Реалізація механізмів множинної ідентифікації і автентифікації

Використання в складі КЗЗ “Рубіж-2” програмно-технічних засобів управління доступом дозволяє забезпечити ефективну реалізацію в КЗЗ вузлів кожного з рівнів АС механізмів множинної ідентифікації і автентифікації, тобто забезпечення відповідної функціональної послуги рівня НИ-3. Ця послуга передбачає, що в КЗЗ:

1) політика ідентифікації та автентифікації визначає атрибути користувача і послуги, для використання яких необхідні ці атрибути; кожен користувач має однозначно ідентифікуватися механізмами ідентифікації і автентифікації КЗЗ;

2) перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, здійснюється автентифікація цього користувача з використанням захищених механізмів двох або більше типів;

3) забезпечується захист даних автентифікації від НСД, модифікації або руйнування;

4) в процесі ідентифікації та автентифікації забезпечується використання, як мінімум, однонаправленого достовірного каналу, який використовується для початкової ідентифікації та автентифікації, причому зв'язок з використанням цього каналу ініціюється виключно користувачем.

Як атрибути користувача для його однозначної ідентифікації в КЗЗ використовуються ідентифікатори та пароль користувача, які формуються у вигляді унікальних символьних чи цифрових кодів.

Множинна автентифікація користувача за його ідентифікатором та унікальним цифровим кодом здійснюється (рис. 2):

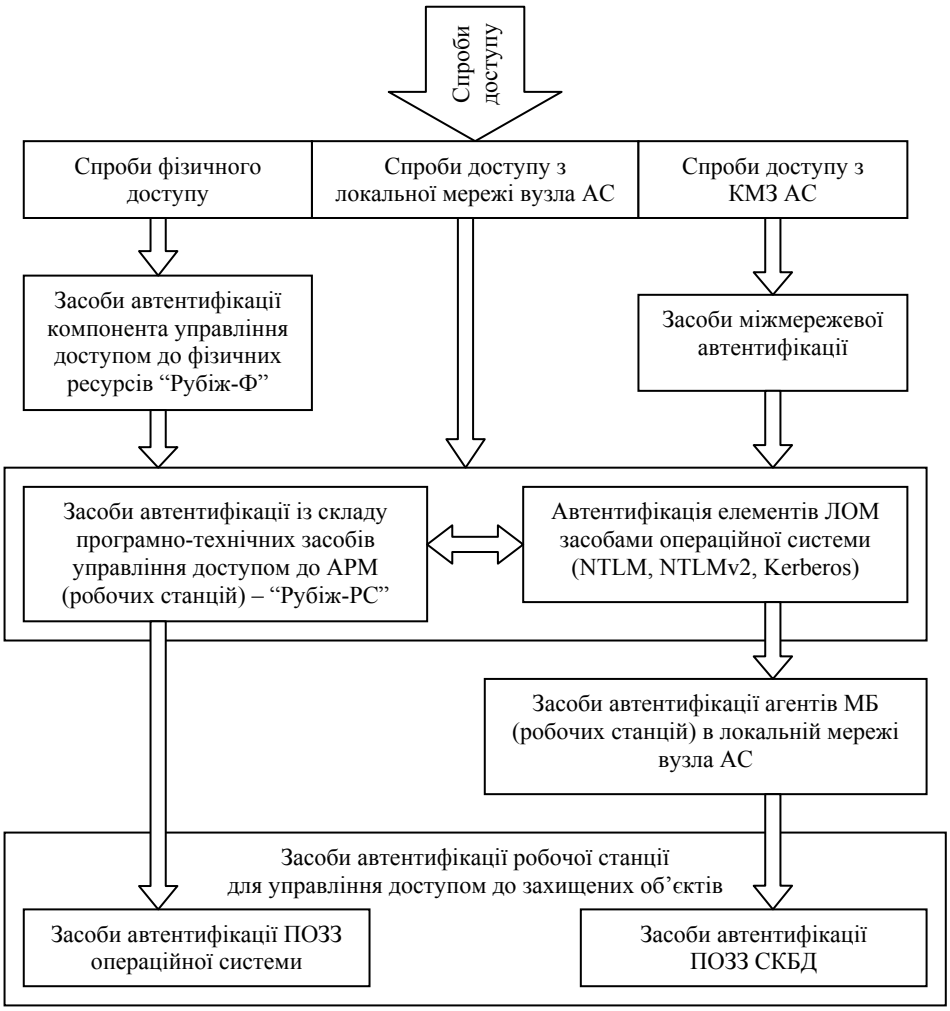

Рисунок 2 – Схема множинної автентифікації в КЗЗ "Рубіж-2"

1) засобами підсистеми управління фізичним доступом (ПУФД) "Рубіж-Ф" під час входу (виходу) в приміщення з розташуванням ідентифікаційної інформації на зовнішньому (по відношенню до засобів КЗЗ) носії типу Touch Memory;

2) засобами підсистеми управління фізичним доступом під час фізичного доступу (включення, використання органів управління) до функціонального АРМ (робочої станції) – аналогічно п. 1;

3) засобами автентифікації елементів локальної обчислювальної системи (ЛОМ, робочих станцій) вузлів АС засобами операційної системи (при спробах доступу до ресурсів даної робочої станції з інших робочих станцій ЛОМ даного вузла АС);

4) засобами автентифікації агентів МБ в локальних мережах відповідних вузлів АС при старті, таймерно чи за запитом адміністратора безпеки;

5) засобами міжмережної автентифікації в глобальній мережі АС (при спробах доступу до ресурсів ЛОМ даного вузла АС чи до даної робочої станції з інших робочих станцій ЛОМ, інших вузлів АС);

6) засобами ОС, СКБД чи контролю цілісності, інтегрованими до складу КЗЗ, під час спроби звернення до об'єктів, захищених засобами КЗЗ.

Захист даних автентифікації ОС та СКБД від НСД, модифікації або руйнування забезпечується шляхом:

1) збереження їх в перетвореному вигляді в захищених базах даних складових операційних систем та СКБД:

– в системах управління безпекою доступу (SAM, Active Directory) – в базі контролера домену операційних систем (Windows 2000/NT) (з копіюванням у всі резервні копії контролера домену);

– локально в базах даних складових систем управління безпекою доступу (SAM) операційних систем кожної з робочих станцій; в таблицях СКБД типу SYS.USERS.

2) збереження даних автентифікації в перетвореному вигляді в базі даних серверу МБ, коли ключ перетворення, в свою чергу, зберігається на зовнішньому носії;

3) збереження їх як на зовнішніх носіях (Touch Memory, Smart Cart, ГМД, пам'яті користувача тощо), наприклад, у вигляді Pin-коду;

4) контролю їх довжини (не менше ніж 8 символів, або 64 біт) під час реєстрації користувача в КЗЗ та перевірки унікальності паролів та ідентифікаторів засобами ОС чи СКБД під час реєстрації користувача в КЗЗ.

III Порядок автентифікації засобів вузла АС

Автентифікація засобів вузла АС здійснюється:

– при старті (включенні) робочих станцій засобами монітора безпеки та його агентів;

– таймерно згідно з установками адміністратора безпеки;

– за запитом адміністратора безпеки.

Ці способи автентифікації засобів вузла АС відрізняються лише порядком запуску модуля автентифікації МБ та модулів автентифікації агентів МБ. При старті процес автентифікації ініціюється кожним з агентів МБ, в той час як при таймерній автентифікації чи автентифікації за запитом адміністратора безпеки ці процеси ініціюються сервером МБ.

Алгоритм автентифікації засобів вузла АС при старті представлено на схемі взаємодії менеджерів автентифікації МБ та агентів МБ в ЛОМ вузла єдиної державної автоматизованої паспортної системи (ЄДАПС) (рис. 3). Автентифікація засобів вузла АС при старті здійснюється наступним чином. Для включення будь-якої з робочих станцій відповідний користувач (адміністратор безпеки чи суб'єкт інформаційної діяльності вузла АС) має вставити свій носій Pin-коду в зчитувач та включити живлення робочої станції. При цьому програмно-технічними засобами управління доступом здійснюється ідентифікація власника носія Pin-коду. Ця ідентифікація здійснюється за схемою, наведеною на рис. 4. З цією метою контролером управління доступом (КУД) в режимі очікування здійснюється блокування ПЕОМ, наприклад шляхом формування сигналу блокування синхронізації ПЕОМ, і здійснюється безперервний контроль наявності носія Pin-коду, читання Pin-коду (при наявності такого носія) та перевірка наявності Pin-коду в базі даних КУД. При відсутності носія Pin-коду засобами КУД здійснюється блокування клавіатури ПЕОМ та перевіряється наявність сигналу завантаження операційної системи (ЗОС). Відсутність такого сигналу свідчить про те, що здійснюється спроба несанкціонованого включення робочої станції, тому відбувається перехід на процес блокування ПЕОМ. При наявності сигналу ЗОС, що свідчить про те, що робоча станція уже була включеною із завантаженням операційної системи, відбувається перехід на процес контролю наявності Pin-коду. При відсутності Pin-коду, наданого користувачем, в базі даних КУД ідентифікація вважається неуспішною і блокування ПЕОМ продовжується. Якщо ж Pin-код, наданий користувачем, в базі даних КУД є, то ідентифікація користувача засобами ПУФД вважається успішною. В цьому випадку здійснюється зняття блокування ПЕОМ, завантаження BIOS та розпочинається завантаження операційної системи. Після цього формується сигнал ЗОС, розблоковується клавіатура та засобами КУД здійснюється ініціалізація контролера управління засобами захисту (КУЗЗ).

При успішній ідентифікації користувача програмно-технічними засобами управління доступом за його Pin-кодом перевіряється цілісність конфігурації технічних засобів робочої станції. При відсутності порушень здійснюється автентифікація робочої станції в домені (в ЛОМ вузла АС) засобами операційної системи. В разі успішності автентифікації здійснюється контроль цілісності засобів монітора безпеки. В разі порушення цілісності формується команда блокування процесів. В разі відсутності порушення цілісності на кожній із робочих станцій вузла АС здійснюється, насамперед, запуск менеджера автентифікації агента МБ даної робочої станції. Модулем автентифікації агента МБ формується повідомлення готовності автентифікації даного (і-го) агента МБ, яке надсилається на сервер МБ. Після цього агент МБ забезпечує очікування отримання від серверу МБ запиту автентифікації.

Сервером МБ забезпечується безперервний процес перевірки наявності повідомлень готовності автентифікації від усіх агентів МБ. Цим самим сервер здійснює блокування усіх інших прикладних процесів до отримання повідомлення готовності автентифікації будь-якого з агентів.

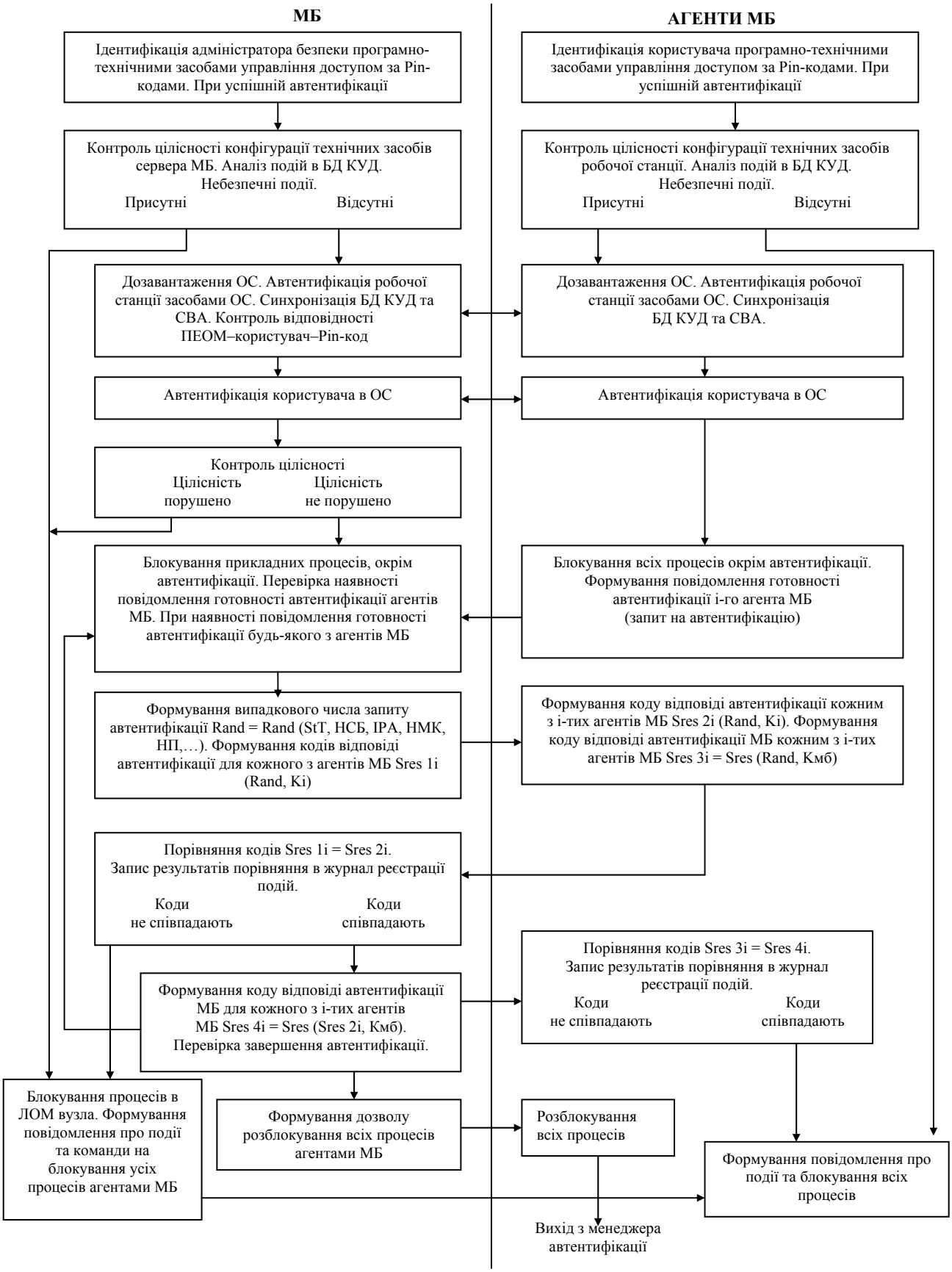

Рисунок 3 – Схема взаємодії менеджерів автентифікації в ЛОМ вузла ЄДАПС

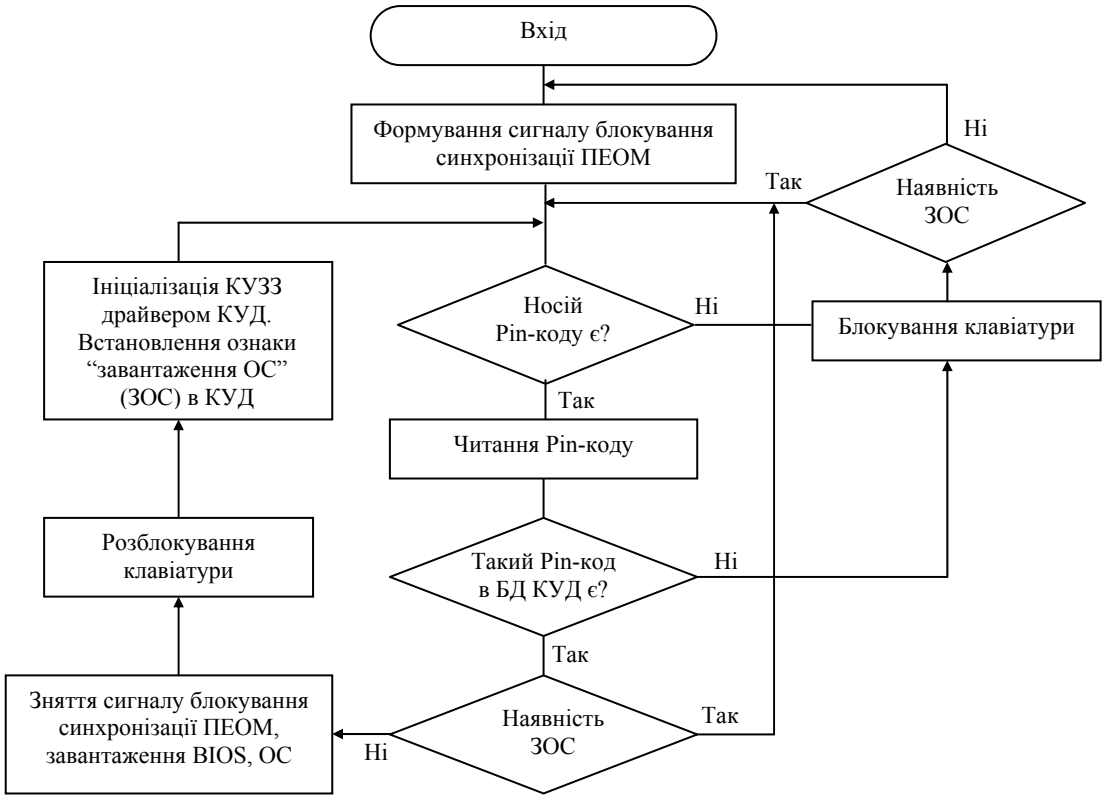

Рисунок 4 – Схема ідентифікації користувачів програмно-технічними засобами управління доступом за Pin-кодами

При отриманні повідомлення готовності автентифікації будь-якого з агентів МБ менеджером автентифікації МБ здійснюється передача на вхід генератора випадкових чисел ініціюючого коду, яким є сума за модулем 2 вихідного коду лічильника часу (StT) з ключем автентифікації $К_{мб}$. При цьому ключем автентифікації $К_{мб}$ є інформація, отримана шляхом конкатенації (ця операція в подальшому позначена як ‖) індивідуальних ознак даного засобу ($К_{мб}$ = ‖(номер системного блоку (НСБ) ПЕОМ, IP-адреса (IPA), номер мережної картки (НМК), номер плат (НП) і т. ін.)) та запуску генератора випадкових чисел.

Генератором випадкових чисел формується випадкове число запиту автентифікації (Rand = Rand (StT, $К_{мб}$)). Це випадкове число запиту автентифікації у складі автентифікаційного пакету надсилається в адреси усіх агентів МБ. Окрім того менеджером автентифікації МБ для кожного із своїх агентів формується код відповіді автентифікації Sres 1_i (Rand, K_i) шляхом перетворення випадкового числа запиту автентифікації з ключем перетворення K_i, яким є код, що отримано шляхом конкатенації індивідуальних ознак даного агента МБ (K_i = Є (номер системного блоку (НСБ) ПЕОМ, IP-адреса (IPA), номер мережної картки (НМК), номер плат (НП), Pin-код користувача та т. ін.)). Код відповіді автентифікації Sres 1_i (Rand, K_i) запам'ятовується в каталозі (журналі) автентифікації МБ.

При отриманні коду запиту автентифікації менеджером автентифікації кожного агента МБ-отримувача формується код відповіді автентифікації даного агента МБ Sres 2_i (Rand, K_i) за тими ж правилами, що і в МБ. Код відповіді автентифікації кожного із агентів МБ Sres 2_i розглядається, окрім того, як код запиту автентифікації даного агента МБ-відправника до МБ. Тому ці коди відповіді автентифікації кожного із агентів МБ в менеджері автентифікації агентів МБ перетворюються за ключем перетворення МБ $К_{мб}$. Отримані коди (Sres 3_i) запам'ятовуються в каталогах (журналах) автентифікації агентів МБ. Сформований код відповіді автентифікації даного агента МБ Sres 2i надсилається в складі автентифікаційного пакету на менеджер автентифікації серверу МБ, де здійснюється його порівняння із відповідним кодом з каталогу (журналу) автентифікації МБ Sres 1_i. В разі співпаданні цих кодів (Sres 1_i = Sres 2_i) операція автентифікації агента МБ (а значить і відповідної робочої станції) вважається успішною. При неспівпаданні кодів агента МБ, автентифікація якого здійснюється на поточний час, ця подія фіксується в журналі реєстрації подій МБ як порушення конфігурації ЛОМ даного вузла і здійснюється блокування усіх процесів в ЛОМ вузла АС.

При успішності операцій автентифікації даного агента МБ для кожного із своїх агентів формується код відповіді автентифікації МБ (Sres 4_i) за тими ж процедурами, що і в менеджері автентифікації агентів МБ. Ці коди надсилаються в складі автентифікаційних пакетів на відповідні робочі станції та здійснюється перевірка

завершення автентифікації в ЛОМ. Умовою завершення автентифікації в ЛОМ є формування кодів відповіді автентифікації МБ (Sres 4_i) для усіх агентів МБ. При успішності операцій автентифікації усіх робочих станцій робиться відповідний запис в журнал реєстрації подій МБ і формується дозвіл розблокування процесів агентами МБ. В разі невиконання умови завершення автентифікації в ЛОМ здійснюється повернення до процесу перевірки наявності повідомлень готовності автентифікації від усіх агентів МБ. Цим самим забезпечується блокування сервером МБ усіх інших процесів, окрім процесу автентифікації.

Після отримання кодів відповіді автентифікації Мб (Sres 4_i) кожним з агентів МБ здійснюється їх порівняння з кодами (Sres 3_i), які сформовано раніше за кодами відповіді автентифікації агентів МБ. В разі їх однаковості (Sres 3_i = Sres 4_i) операція автентифікації МБ вважається успішною. Наслідки порівняння фіксуються в журналах реєстрації подій агентів МБ. При неуспішності операцій автентифікації МБ на робочих станціях подальші процеси блокуються.

В разі успішності операцій автентифікації МБ на робочих станціях, при умові наявності дозволу розблокування процесів від МБ, здійснюється розблокування усіх процесів на даній робочій станції.

При блокуванні процесів на робочих станціях, чи в ЛОМ взагалі, формуються відповідні повідомлення для адміністратора безпеки та користувача робочої станції та здійснюється фіксація даної події в журналі реєстрації подій.

Таймерна автентифікація чи автентифікація за запитом відрізняється від автентифікації при старті, по–перше, тим, що вони здійснюються на вже працюючих сервері МБ та робочих станціях вузла АС і тому не потребують проведення процедур автентифікації засобами автентифікації підсистеми управління фізичним доступом. Алгоритм автентифікації засобів вузла АС при таймерній автентифікації чи автентифікації за запитом представлено на схемі взаємодії менеджерів автентифікації МБ та агентів МБ (рис. 5).

По-друге, процес автентифікації засобів вузла АС при цьому ініціюється сервером МБ, і тому повернення після перевірки завершення автентифікації здійснюється не до перевірки наявності повідомлень готовності автентифікації агентів МБ, як це зроблено у попередньому алгоритмі, а до процедури порівняння кодів. При цьому процес автентифікації починається з того, що менеджером автентифікації МБ здійснюється передача на вхід генератора випадкових чисел ініціюючого коду, яким є сума за модулем 2 вихідного коду лічильника часу (StT) з ключем автентифікації $К_{мб}$. Менеджером автентифікації МБ здійснюється передача на вхід генератора випадкових чисел ініціюючого коду, яким є сума за модулем 2 вихідного коду лічильника часу (StT) з ключем автентифікації $К_{мб}$. Генератором випадкових чисел формується випадкове число запиту автентифікації (Rand = Rand (StT, $К_{мб}$)). Це випадкове число запиту автентифікації у складі автентифікаційного пакету надсилається в адреси всіх агентів МБ.

По-третє, контроль цілісності об’єктів захисту здійснюється на передостанніх етапах виконання алгоритмів як на сервері, так і на агенті МБ.

***Примітка* 1.** В обох алгоритмах під час автентифікації шляхом обміну повідомленнями, що містять перетворену на ключах обох абонентів інформацію, забезпечується встановлення достовірного зв’язку між користувачем і КЗЗ, а також між елементами ЛОМ вузла АС. Цей достовірний канал використовується для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв’язок користувач/КЗЗ або КЗЗ/користувач. Зв’язок з використанням даного каналу ініціюється КЗЗ. Окрім того, забезпечується обмін з використанням достовірного каналу, що ініціює КЗЗ, з однозначною ідентифікацією як такого і відбувається тільки після позитивного підтвердження готовності до обміну з боку користувача. Оскільки за цими процедурами здійснюється перевірка конфігурації та контроль цілісності засобів вузла, то це, окрім функціональної послуги НИ-3 (множинна автентифікація в частині автентифікації засобів ЛОМ відповідних вузлів АС), забезпечує реалізацію функціональних послуг НТ-3 (тестування в реальному часі) та НЦ-2 (КЗЗ з гарантованою цілісністю).

***Примітка* 2.** Звернемо увагу на те, що при реалізації даних процедур здійснюється взаємний обмін між МБ та його агентами автентифікаційною інформацією, яка є перетвореною на ключах автентифікації МБ та агентів МБ $К_{мб}$ та $К_i$, тобто обмін відкритою інформацією автентифікації є відсутнім, що відповідає сучасним вимогам щодо двонаправленого достовірного каналу, якщо розглядати функціональні АРМ АС (робочі станції) як користувачів МБ (функціональна послуга з рівнем НК-2) та щодо ідентифікації і автентифікації при обміні – автентифікація з підтвердженням (функціональна послуга з рівнем НВ-3). Це підтверджується тим, що:

1) для функціональної послуги з рівнем НК-2 потрібно, щоб політика достовірного зв’язку, що реалізується комплексом засобів захисту (КЗЗ), визначала механізми встановлення достовірного зв’язку між користувачем і КЗЗ (в даному випадку між елементами ЛОМ вузла АС); достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв’язок користувач/КЗЗ або КЗЗ/користувач; зв’язок з використанням даного каналу повинен ініціюватися

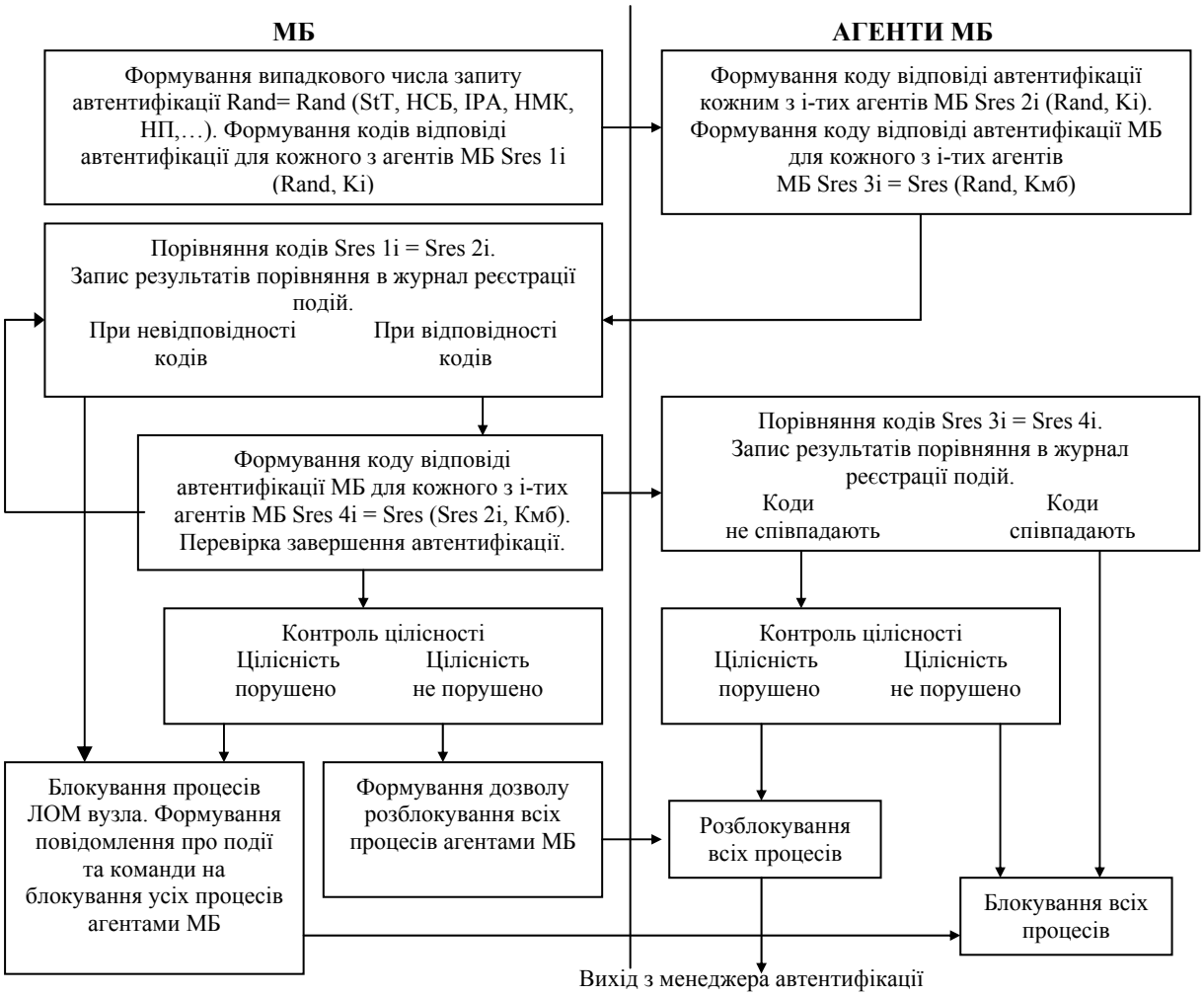

Рисунок 5 – Схема взаємодії менеджерів автентифікації в ЛОМ вузла ЄСДАПС

користувачем або КЗЗ; обмін з використанням достовірного каналу, що ініціює КЗЗ, має бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача;

2) для функціональної послуги з рівнем НВ-3 потрібно, щоб КЗЗ (наприклад, МБ), перш ніж почати обмін даними з іншим КЗЗ (наприклад, агентом МБ), ідентифікував і автентифікував цей КЗЗ з використанням захищеного механізму, а використовуваний протокол автентифікації мав забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною (адміністратором безпеки).

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).