3. Аутентификационное предупреждение. Прежде чем аутентифицированный пользователь получит доступ к ресурсам приложения, он должен быть ознакомлен с такой информацией:

- к какой системе пользователь получает доступ;
- степень защиты приложением личной информации пользователя (privacy right);
- максимальный уровень конфиденциальности, с которым может работать пользователь;
- предупреждение о том, что действия пользователя регистрируются;
- мера ответственности пользователя за обрабатываемые данные.

Дополнительно может сообщаться:

- дата, время домен или адрес последнего подключения данного пользователя;
- количество неудачных попыток доступа после последнего удачного.

4. Выбор аутентифицирующих сущностей. Следует отдавать предпочтение аутентифицирующим сущностям, которые нельзя забыть и невозможно подделать, например, аппаратные токены, биометрию, одноразовые пароли, PKI или single side one (SSO - технология Микрософт).

5. Цепочки доверия. Цепочки доверия определяют отношения доверия между объектами инфраструктуры приложения (например, с помощью сертификатов). Для каждой пользовательской сессии или транзакции приложение должно убедиться, что установлена и поддерживается цепочка доверия между клиентом, сервером приложения и другими серверами.

6. Доверенный путь. Механизм аутентификации должен использовать доверенный путь, например криптографию. Этот путь должен инициироваться пользователем, а не приложением. Пароли и другая информация, используемая в процессе аутентификации должны шифроваться перед передачей их по сети. Надежность шифрования должна соответствовать степени конфиденциальности защищаемых данных.

7. Аутентификация групп/ролей. Если в приложении используется аутентификация на уровне групп или ролей, то прежде чем пользователь будет авторизован как член группы или роли, он должен пройти индивидуальную процедуру аутентификации.

8. База безопасности. Пароли и другая информация, используемая в процессе аутентификации, должны быть надежно зашифрованы перед сохранением. База сохраненной информации должна быть защищена от удаления или модификации.

9. Аутентификация лиц с административными полномочиями. Требования к аутентификации лиц с административными полномочиями должны быть более строгими (например, требования к длине и сложности пароля).

10. Аутентификация каждой сессии пользователя. Каждый раз, при инициализации новой сессии пользователь должен вводить пароль. Приложение не должно хранить пароль в файлах cookies, либо в программах (скриптах) на стороне клиента или сервера, позволяющим пользователю не вводить пароль при инициализации новой сессии.

*Литература: **1.** Ховард М., Лебланк Д. Защищенный код: Пер. с англ, - 2-е изд., испр. М.: Издательско-торговый дом "Русская Редакция", 2004. - 704 стр.: ил. **2.** ISO/IEC 9798-1:1997 Information technology -- Security techniques -- Entity authentication. **3.** Application security and development. Security technical implementation guide. V. 2, r.1, DISA 2008 **4.** G. McGraw, Software Security: Building Security In, Addison-Wesley Professional, 2006*

УДК 681.3

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД НСД. ВАРІАНТ РЕАЛІЗАЦІЇ АЛГОРИТМУ МНОЖИННОЇ АВТЕНТИФІКАЦІЇ

Вячеслав Василенко

Національний авіаційний університет

Анотація: ***Для систем захисту ієрархічних автоматизованих систем 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 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 Вступ

Одним із різновидів організації взаємодії користувачів є наразі побудова сучасних автоматизованих систем як ієрархічних, розподілених. Це дозволяє забезпечити ефективний обмін різнорідною інформацією як в межах окремих робочих станцій, так і в межах локальних та розподілених мереж. Однак зручність використання таких мереж призводить і до можливостей несанкціонованого доступу до відповідних ресурсів

із відповідним порушенням їх конфіденційності, цілісності чи доступності. Отже виникає проблема захисту інформаційних ресурсів від несанкціонованого доступу (НСД). Ця проблема вирішується шляхом застосування тих чи інших систем чи комплексів засобів захисту від НСД, одним із механізмів яких є автентифікація, а з врахуванням необхідності забезпечення доступу до ресурсів АС користувачів із різних ієрархічних рівнів – множинна автентифікація. Деякі аспекти побудови такої системи захисту і розглядаються в цій статті.

II Захист робочих станцій в локальних обчислювальних мережах

Засоби захисту робочих станцій, як елемент комплексу засобів захисту (КЗЗ) локальної обчислювальної мережі (ЛОМ), мають знаходитись під централізованим управлінням монітора безпеки (МБ). До складу засобів захисту входять засоби автентифікації, засоби захисту операційної системи та систем керування базами даних (за їх наявності), засоби контролю цілісності та програмно-технічні засоби управління доступом. Варіант взаємодії засобів з МБ представлено на рис. 1.

Програмно – технічні засоби управління доступом забезпечують запобіганню або суттєвому перешкоджанню несанкціонованому 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 за відсутності повноважень на включення в суб'єкта, який пред'явив ідентифікатор;
- ідентифікація та автентифікація суб'єкта при завантаженні ОС;
- блокування роботи робочої станції за 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.

III Реалізація механізмів множинної ідентифікації і автентифікації

Використання в складі комплексу засобів захисту ЛОМ програмно-технічних засобів управління доступом дозволяє забезпечити ефективну реалізацію в КЗЗ вузлів кожного з рівнів АС механізмів множинної ідентифікації і автентифікації, тобто 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 повинен 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) забезпечує захист даних автентифікації від НСД, модифікації або руйнування;

4) в процесі ідентифікації та автентифікації в КЗЗ 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 в вигляді унікальних символьних чи цифрових кодів.

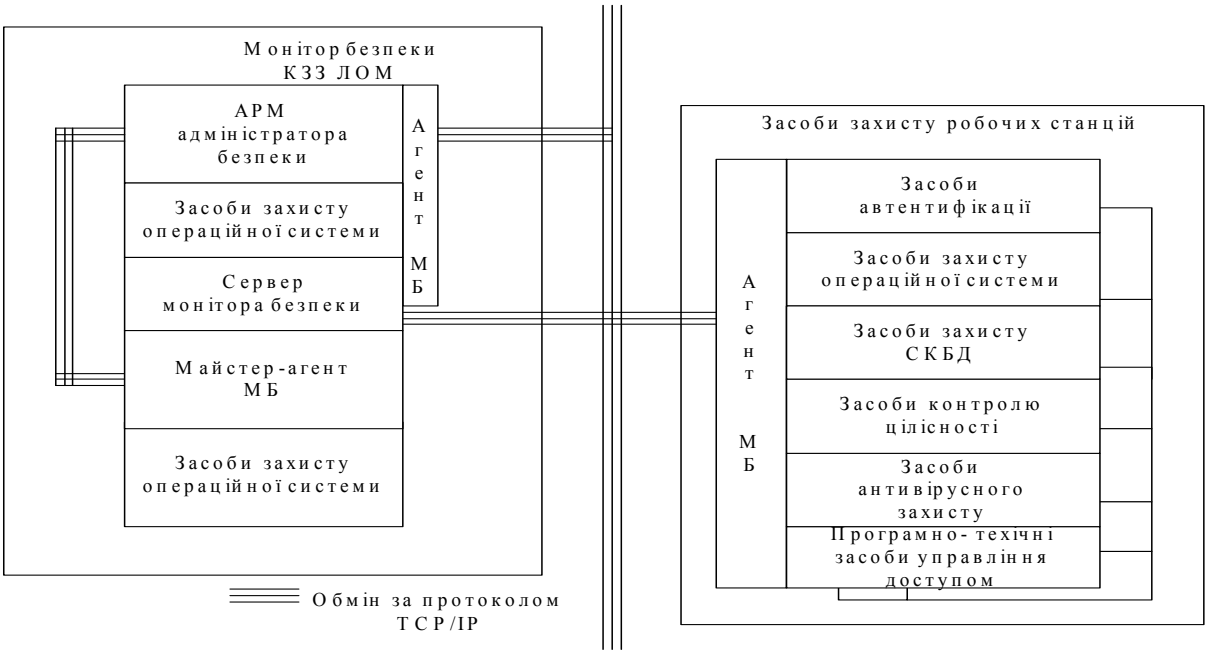

Рисунок 1 – Варіант взаємодії засобів захисту робочих станцій з монітором безпеки комплексу засобів захисту ЛОМ

III Реалізація механізмів множинної ідентифікації і автентифікації

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

1) засобами підсистеми управління фізичним доступом (ПУФД) під час входу (виходу) в приміщення з розташуванням ідентифікаційної інформації на зовнішньому (відносно 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 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 монітора безпеки 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.

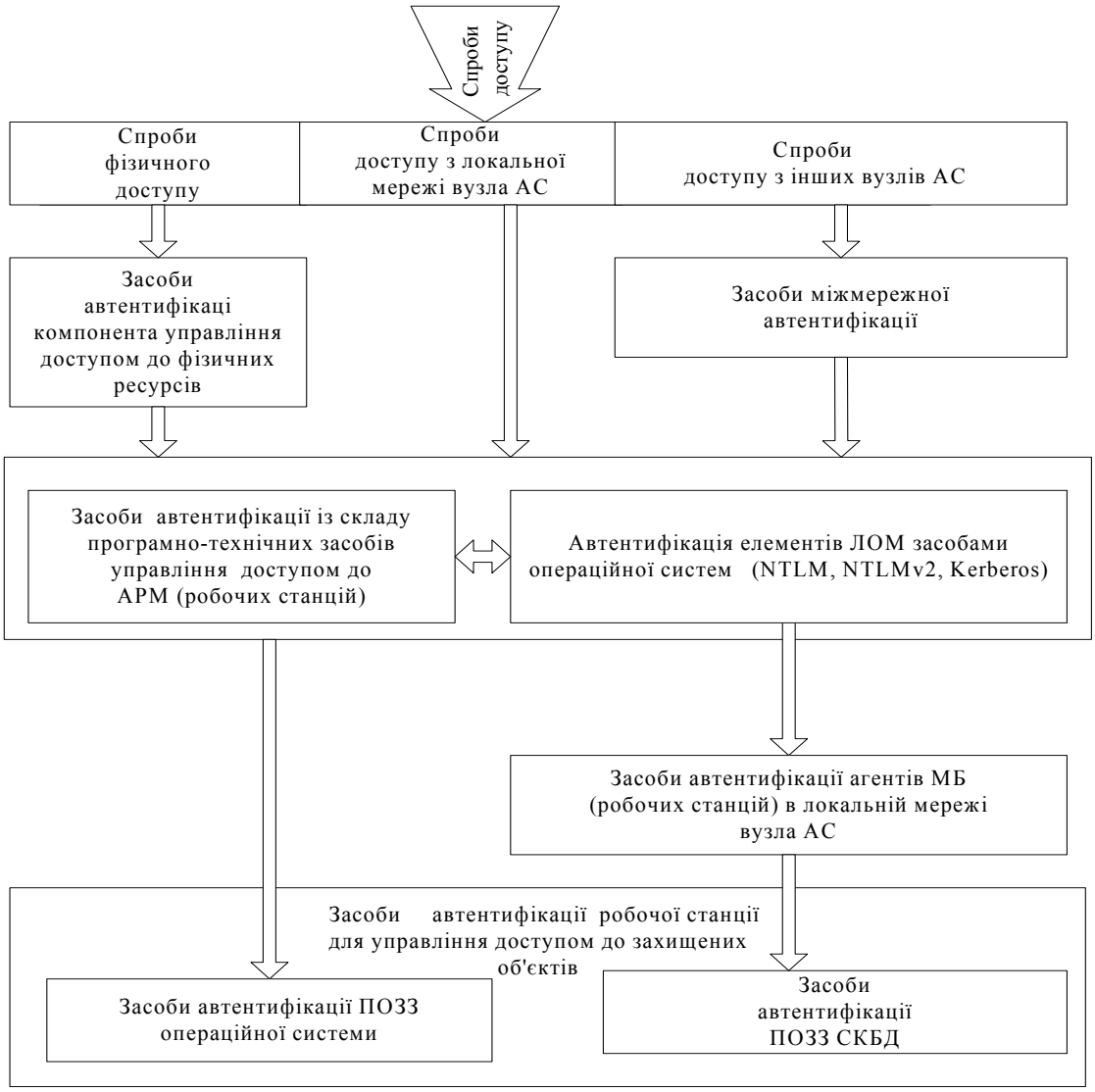

Рисунок 2 – Схема множинної автентифікації в КЗЗ ЛОМ

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

8) 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);

9) 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:

5) 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.
6) збереження даних автентифікації в перетвореному вигляді в базі даних серверу МБ, коли ключ перетворення, в свою чергу, зберігається на зовнішньому носії.
7) збереження їх як на зовнішніх носіях (Touch Memory, Smart Cart, ГМД, пам'яті користувача тощо), наприклад, у вигляді Pin-коду.
8) 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.

IV Порядок автентифікації засобів вузла АС

Автентифікація засобів вузла АС здійснюється:

1) при старті (включенні) робочих станцій засобами МБ та його агентів;
2) таймерно згідно з установками адміністратора безпеки;
3) 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 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 монітора безпеки та агентів монітора безпеки (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) повинен 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 (за наявності такого носія) та перевірка наявності Pin-коду в базі даних КУД. За 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. За 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. За 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. За 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.

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 ПЕОМ, IP – адреса, номер мережної картки, номер плат та т. ін.)), та запуск генератора випадкового числа.

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 монітора безпеки. Окрім того менеджером автентифікації МБ для кожного зі своїх агентів формується код відповіді автентифікації Sres 1_i (Rand, K_i) шляхом перетворення випадкового числа запиту автентифікації ключем перетворення K_i, яким є код, що отримано шляхом конкатенації індивідуальних ознак даного агента МБ (K_i = Є (номер системного блоку ПЕОМ, IP – адреса, номер мережної картки, номер плат, Pin-код користувача та т. ін.)). Код відповіді автентифікації Sres 1_i (Rand, K_i) запам'ятовується в каталозі (журналі) автентифікації МБ.

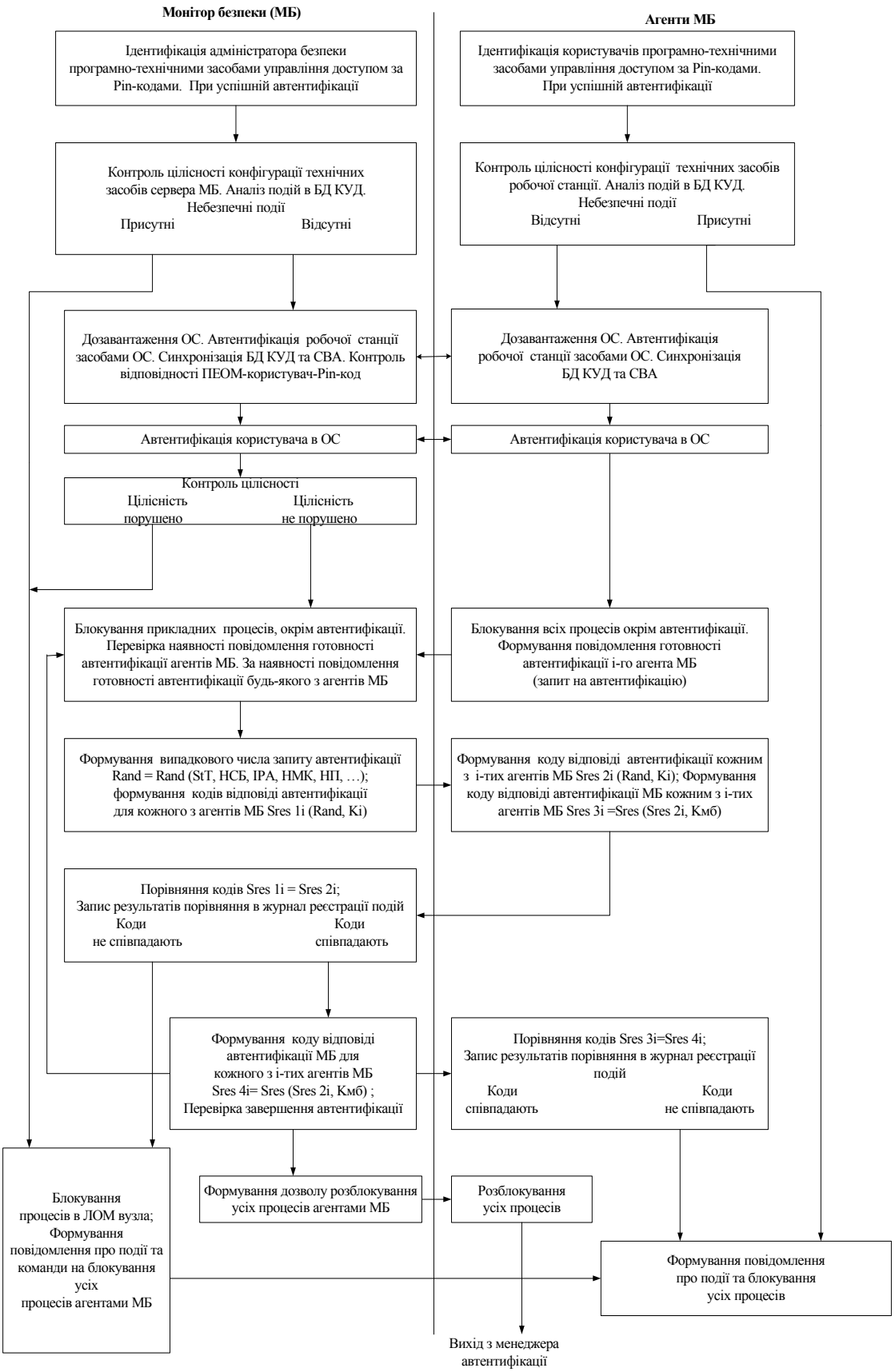

Рисунок 3 – Схема взаємодії менеджерів автентифікації в ЛОМ вузла ЄДАПС

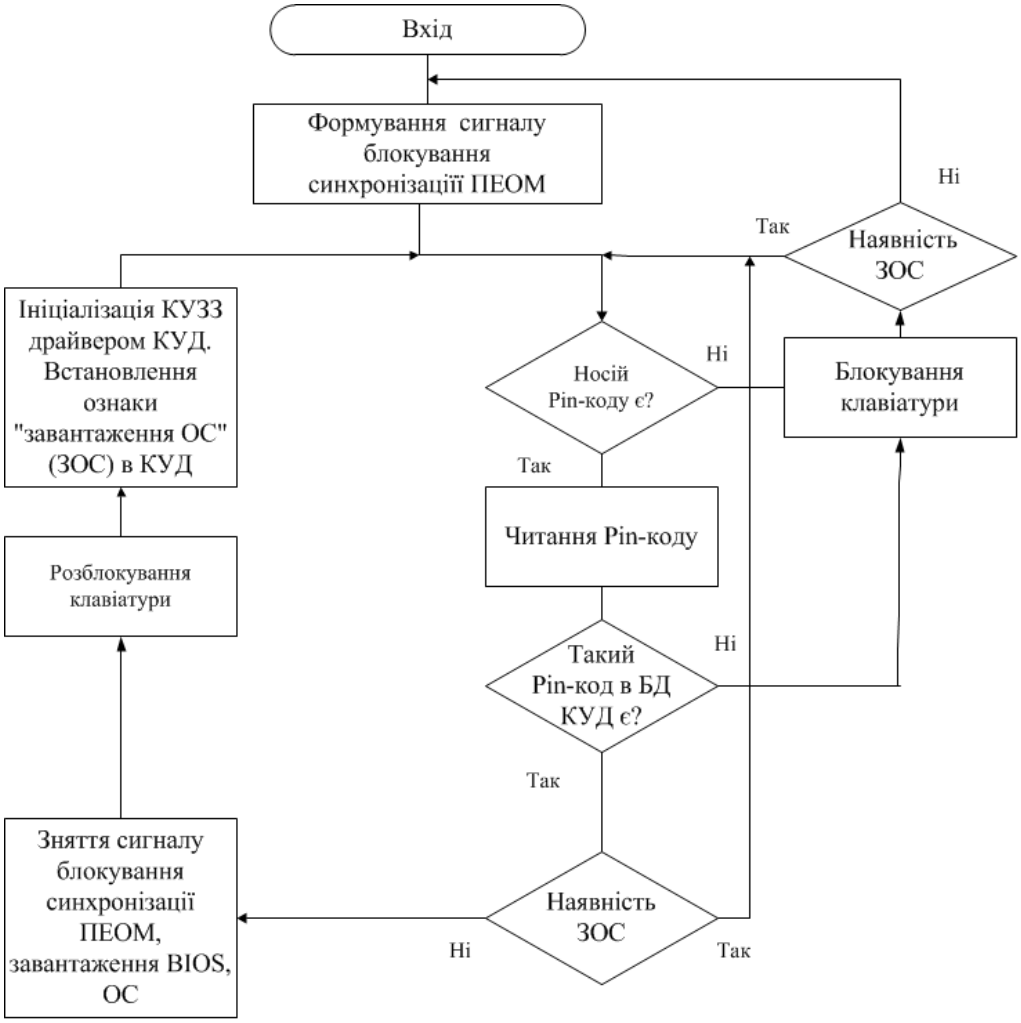

Рисунок 4 – Схема ідентифікації користувачів програмно-технічними засобами управління доступом за Pin-кодами

При отриманні 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 $K_{мб}$. Отримані коди (Sres 3_i) запам'ятовуються в каталогах (журналах) автентифікації агентів МБ. Сформований код відповіді автентифікації даного агента МБ Sres 2i надсилається у 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 збігання цих кодів (Sres 1_i = Sres 2_i) операція автентифікації агента МБ (а значить і відповідної робочої станції) вважається успішною. При незбіганні 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 всіх процесів в ЛОМ вузла АС.

При успішності операцій автентифікації даного агента МБ для кожного зі своїх агентів формується код відповіді автентифікації МБ (Sres 4_i) за тими ж процедурами, що і в менеджері автентифікації агентів МБ. Ці коди надсилаються у 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 всіх робочих станцій робиться відповідний запис в журнал реєстрації подій МБ і формується дозвіл на розблокування процесів агентами МБ. У 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 із агентів МБ здійснюється їх порівняння з кодами (Sres 3_i), які сформовано раніше за кодами відповіді автентифікації агентів МБ. У 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, за умови 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 монітора безпеки та агентів монітора безпеки (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 усіх агентів монітора безпеки.

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 монітора безпеки 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 монітора безпеки (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 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 має ініціюватися 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), повинен ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму, а використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об’єкта незалежною третьою стороною (адміністратором безпеки).

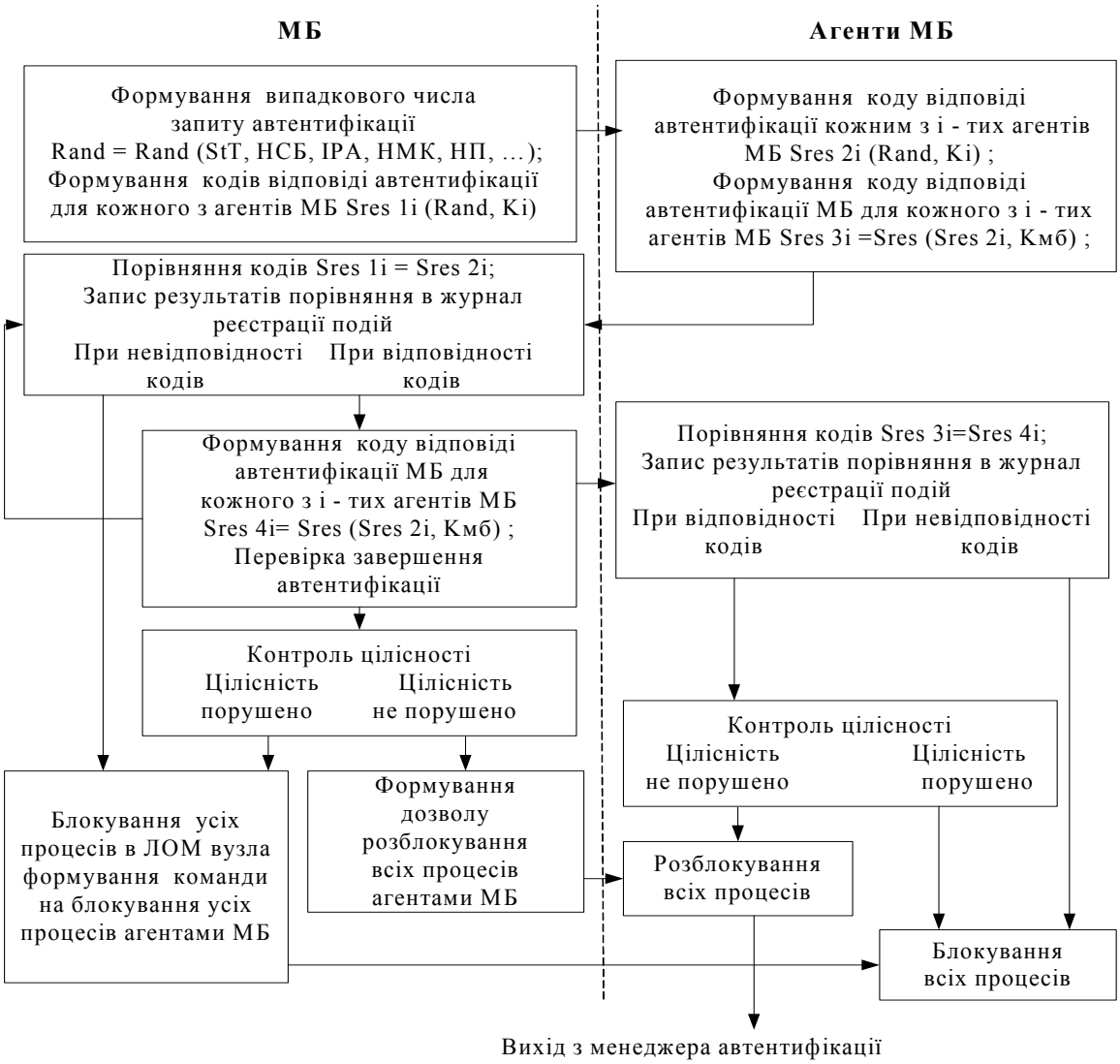

Рисунок 5 – Схема взаємодії менеджерів автентифікації в ЛОМ вузла ЄДАПС

V Висновки

Таким чином, розглянуто можливості використання у складі комплексів засобів захисту локальних обчислювальних мереж програмно-технічних засобів управління доступом, що, на думку автора, може забезпечити ефективну реалізацію в комплексах засобів захисту вузлів кожного з рівнів АС механізмів множинної ідентифікації і автентифікації. Як атрибути користувача для його однозначної ідентифікації запропоновано використання ідентифікаторів та паролів користувачів, які формуються у вигляді унікальних символьних чи цифрових кодів. Множинна автентифікація користувача за його ідентифікатором та унікальним цифровим кодом здійснюється засобами підсистеми управління фізичним доступом (під час входу (виходу) в приміщення) з розташуванням ідентифікаційної інформації на зовнішньому (відносно до засобів КЗЗ) носії; засобами підсистеми управління фізичним доступом під час фізичного доступу (включення, використання органів управління) до функціонального АРМ (робочої станції); засобами автентифікації елементів ЛОМ (робочих станцій) вузлів АС, що входять до складу операційної системи; засобами автентифікації агентів МБ в локальних мережах відповідних вузлів АС при старті, таймерно чи за запитом адміністратора безпеки; 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); та, нарешті, засобами операційних систем, систем керування базами даних чи засобами контролю цілісності, інтегрованими до складу комплексів засобів захисту, під час спроби звернення до об'єктів, захищених засобами КЗЗ.

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 004.43(031):681.3.01(02)

ВИЗНАЧЕННЯ УРАЗЛИВОСТІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЯК СКЛАДОВА ПОРЯДКУ РОЗРОБКИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Луценко, Валерій Худяков
НТУУ «КПІ»

Анотація: **Розглядається проблема аналізу властивостей методів та засобів підтримки прийняття рішень для створення проектів систем захисту інформації. Визначено основні властивості таких проектів. Запропоновано підхід до створення нової методики проектування системи захисту інформації від несанкціонованого доступу.**

Summary: **The paper considers problem of analyzing of property of means of support of acceptance of decisions for information security systems projects. The basic properties of such projects are given.The technique of complex system designing for non-authorized access protection is developed on the basis of means of support of acceptance of decisions.**

Ключові слова: **Захист інформації; комплексна система захисту; асоціативна пам'ять; нейроподібна сітка.**

I Вступ

Складні системи найчастіше тому складні, що передбачають необхідність прийняття рішень при протирічних або неповних даних і загалом є напрямком, котрий має тенденцію до розвитку. Це стосується і технічного захисту інформації (ТЗІ), а особливо комплексних систем захисту інформації (КСЗІ) для інформаційно-комунікаційних систем (ІКС) та об'єктів інформаційної діяльності (ОІД) [1, 2], у тому числі таких, котрі не мають у своєму складі засобів інформаційних комунікацій, або мають, але без виходу за межі контрольованої зони (КЗ).

Реальні проекти захисту за якісними показниками мають об'єктивно відтворювати умови життєдіяльності об'єктів, але реально мають тенденцію до відставання від життєвих вимог. Для подолання такого відставання мають відтворюватися вимоги щодо життєдіяльності системи проектування окремо для кожного об'єкту в повному обсязі. Такі вимоги передбачають необхідність використання системи захисту, що базується на базі принципово об'єктивного проектування, тобто такого, котре не залежить від якісних показників проектанта. Крім того, створювана система захисту має бути динамічною в часі, тобто відкритою щодо можливості змін у часі складових методів та засобів захисту або умов існування об'єкту, а такий чинник залежить від методологічних властивостей системи проектування, котра створювала систему захисту. І, насамкінець, майже завжди є відкритим питання необхідної та достатньої завершеності проекту системи захисту. Складність визначення завершеності проекту полягає у відсутності критерію завершеності. Таким реальним критерієм може стати правило, згідно з яким система захисту є достатньо завершеною, якщо за визначений термін часу повторне незалежне проектування дає однаковий результат. Наразі ні один з зазначених чинників не приймається до уваги, а найголовнішою умовою завершеності проектів є формальна за нормативними документами дієздатність системи захисту на даний час та відповідність реалізації спроектованої системи захисту фінансовим можливостям користувача.

Початком більш об'єктивного проектування має бути напрацювання методів та засобів отримання максимально повної та об'єктивної інформації про об'єкт на етапі дослідження об'єкту, а також інженерний аналіз для виявлення місць уразливості об'єкту, тобто визначення ступеня стійкості об'єкта до загроз. Найбільш суб'єктивним фрагментом зазначеного етапу є експертна оцінка при визначенні ризиків і характеристик можливих каналів витоку інформації. Причому, математична або логіко-статистична обробка отриманих від експертів даних є більш досконалою, ніж сама процедура експертизи обмеженою кількістю