УДК 681.3

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД НСД “РУБІЖ”. ЗАБЕЗПЕЧЕННЯ СТАНДАРТНОГО ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ 3.КЦ.3 В АС НА ПЛАТФОРМІ OS/390

Юрій Дмитрук, Станіслав Могильний, Євгеній Федченко
Відкрите акціонерне товариство “КП ОТІ”

Анотація: **Розглядається підхід до забезпечення стандартного функціонального профілю захищеності автоматизованої системи 3-го класу 3.КЦ.3 на платформі OS/390 шляхом використання власних засобів захисту операційної системи (диспетчера доступу RACF) і їх взаємодії з централізованою системою захисту “Рубіж”.**
Summary: **In clause the approach to maintenance of a standard functional structure of security of the automated system 3 is considered(examined). КЦ.3 on a platform OS/390 by use of own means of protection of operational system (dispatcher of access RACF) and their interaction with the centralized system of protection “Rubig”.**
Ключові слова: **Автоматизована система, платформа OS/390, профіль захищеності, диспетчер доступу, достовірне обчислювальне середовище.**

I Вступ

Автоматизована система (АС) являє собою організаційно-технічну систему, що об’єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію. Захист інформації, що обробляється в АС, полягає в створенні і підтримці в дієздатному стані системи заходів як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Система зазначених заходів, що забезпечує захист інформації в АС, називається комплексною системою захисту інформації.

Множина всіх механізмів автоматизованої системи, які безпосередньо призначені для реалізації політики безпеки або впливають на безпеку опосередковано, складає КЗЗ (КЗЗ). КЗЗ розглядає ресурси АС як об’єкти і керує взаємодією цих об’єктів відповідно до політики безпеки інформації, що реалізується. Вимоги до функціонального складу КЗЗ та обчислювального середовища залежать від характеристик оброблюваної інформації, самого обчислювального середовища, фізичного середовища, персоналу і організаційної підсистеми та визначаються політикою безпеки, яка формується через функціональний профіль захищеності згідно з вимогами НД ТЗІ.

КЗЗ АС на платформі операційної системи OS/390 базується на концепції диспетчера доступу (RACF). Диспетчер доступу забезпечує безперервний і повний захист об’єктів АС і достовірне обчислювальне середовище.

II Інтеграція засобів захисту OS/390 в систему “Рубіж”

Головною метою функціонування системи захисту “Рубіж” є реалізація основних механізмів захисту інформації АС від несанкціонованого доступу.

Система захисту „Рубіж” структурно складається з монітору безпеки (МБ) і агентів монітору безпеки, які розміщуються на серверах та робочих станціях, що захищаються. МБ, в свою чергу, складається з АРМ адміністратора безпеки і серверу МБ.

АРМ адміністратора безпеки призначений для виконання функцій адміністрування засобів захисту інформаційних ресурсів АС (власне МБ та механізмів захисту операційних систем та СКБД) за допомогою зручного та інтуїтивно зрозумілого інтерфейсу користувача.

Сервер МБ забезпечує виконання команд адміністратора безпеки конфігурування КЗЗ, і/або адміністрування механізмів захисту інших засобів КЗЗ – програмно-технічних та проблемно-орієнтованих засобів захисту (функціональних АРМ, контролеру домену, комунікаційної мережі зв’язку (КМЗ), підсистеми управління фізичним доступом, операційних систем, СКБД, засобів антивірусного захисту) та надання інформації на АРМ про результати виконання команд. Крім того, сервер забезпечує ведення бази даних МБ (конфігурація КЗЗ, дані автентифікації, репозитарій команд, журнали подій, архіви журналів), реалізацію бізнес-логіки роботи монітору, реагування на критичні події та ін.

Агенти МБ забезпечують взаємодію серверу МБ з проблемно-орієнтованими засобами захисту (ПОЗЗ) серверів та робочих станцій локальних обчислювальних мереж (ЛОМ), відслідковування подій захищеної системи та видачу інформації на сервер МБ. Агент МБ приймає команди адміністрування ПОЗЗ від серверу

МБ, виконує команди і відправляє серверу інформацію про результати виконання. Крім того, агент МБ відслідковує події на ПОЗЗ, видає інформацію про події серверу МБ і забезпечує реагування на критичні події.

Схема взаємодії компонентів системи „Рубіж” може бути представлена наступним чином: АРМ адміністратора безпеки ↔ сервер МБ ↔ агент МБ ↔ ПОЗЗ. Крім того, такий підхід до інтегрування КЗЗ дозволяє здійснювати взаємодію моніторів безпеки різних ЛОМ і створювати систему захисту ресурсів гетерогенних розподілених ієрархічних АС з централізованим управлінням різними механізмами захисту з єдиних позицій та єдиної точки.

Система “Рубіж” інтегрує в себе засоби захисту OS/390 як диспетчер доступу платформи OS/390. Тобто “Рубіж” залишає під своїм керуванням функції керування засобами захисту, а безпосереднє санкціонування доступу відбувається використанням механізмів захисту RACF. Схема інтеграції засобів захисту OS/390 в систему „Рубіж” зображена на рис. 1.

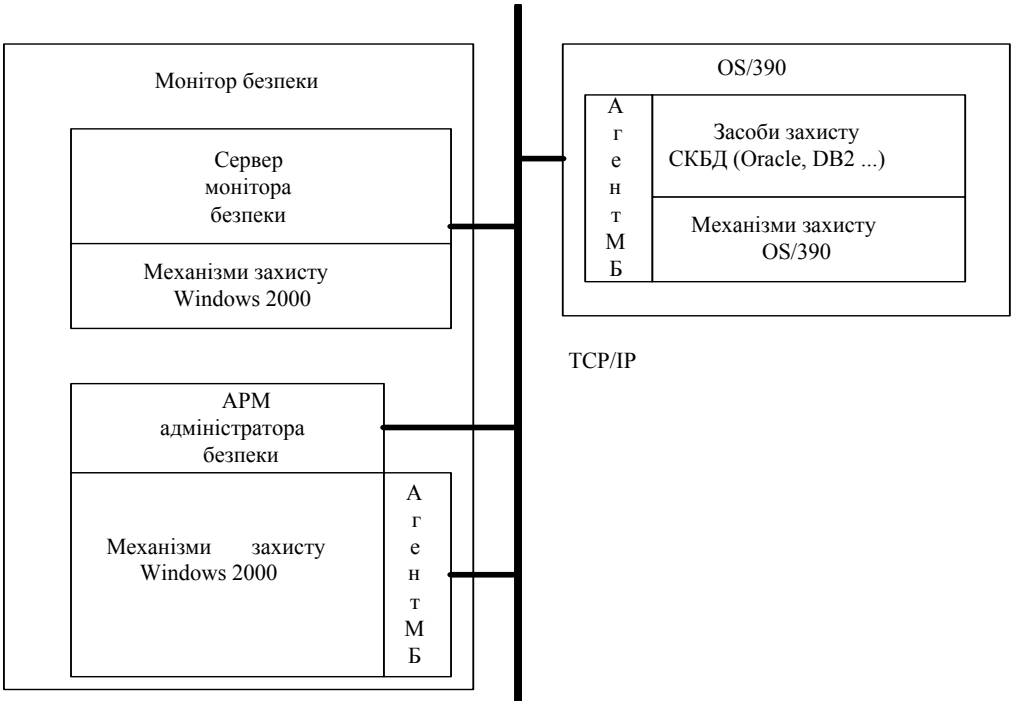

Рисунок 1 – Схема інтеграції засобів захисту OS/390 в систему “Рубіж”

Інтеграція механізмів розмежування доступу операційної системи OS/390 з системою “Рубіж” потребує розробки додаткових програмних засобів – драйверів адміністрування RACF і динамічного відслідковування подій у складі МБ і відповідних модулів на платформі OS/390: модуля адміністрування, модуля обробки подій, модуля обробки невідісланих подій. Схему взаємодії агента МБ з механізмами розмежування доступом OS/390 наведено на рис. 2.

Весь набір функцій керування засобами захисту OS/390 можна розділити наступним чином:

1) функції, призначені для адміністрування суб’єктів та груп суб’єктів;
2) функції, призначені для адміністрування об’єктів;
3) функції, призначені для керування доступом за дискретним принципом;
4) функції, призначені для керування доступом за мандатним принципом;
5) функції динамічного відслідковування подій.

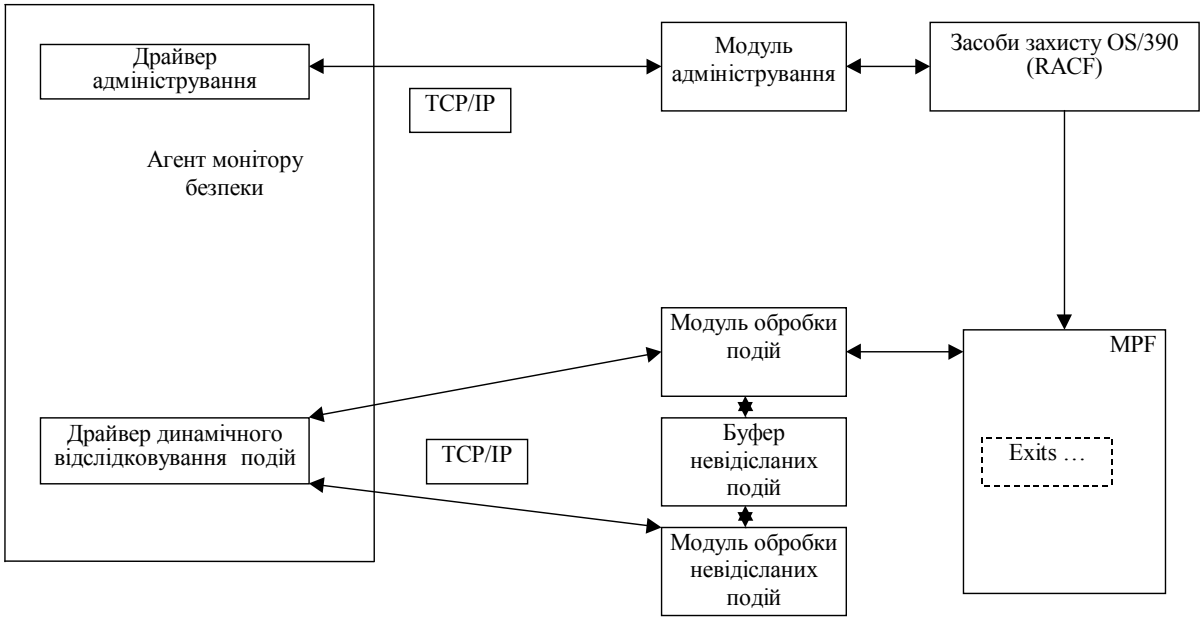

Рисунок 2 – Схема взаємодії МБ з механізмами розмежування доступом OS/390

III Достовірне обчислювальне середовище (The Trusted Computing Base) OS/390

Для того, щоб говорити про захищеність комп'ютерної системи (КС) необхідно бути впевненим у надійності всіх компонент (програмних, апаратних), з яких вона складається. Частина системи, яка стосується захисту, або так зване "достовірне обчислювальне середовище", складається з окремих компонентів, що забезпечують виконання вимог захисту в системі.

Достовірне обчислювальне середовище OS/390 складається з апаратних засобів, підключених до процесора(рів), мікропрограм апаратних засобів та всього достовірного програмного забезпечення OS/390, яке є частиною продукту. Всі програми, що не належать до достовірного обчислювального середовища, вважаються ненадійними. Програмне забезпечення, яке є частиною достовірного обчислювального середовища OS/390, має гарантувати, що прикладні програми не порушать систему захисту.

IV Функціонування засобів захисту на платформі OS/390

Всі програмні компоненти достовірного обчислювального середовища звертаються до диспетчера доступу RACF (Resource Access Control Facility) з запитами на перевірку авторизації суб'єктів чи процесів. Оскільки тільки ці програмні продукти входять до достовірного обчислювального середовища (тобто мають доступ до ядра системи), а всі інші програми працюють через них, то гарантія надійності програмних продуктів є гарантією надійності системи. В даному випадку виключенням є APF-авторизовані програми (програми, які містяться в APF-авторизованих бібліотеках і мають доступ до функцій ядра системи). Але всі ці бібліотеки мають бути наперед визначеними і контролюватися системою захисту. Схема функціонування засобів захисту операційної системи OS/390 при виконанні запиту користувача або процесу до ресурсу АС зображена на рис. 3.

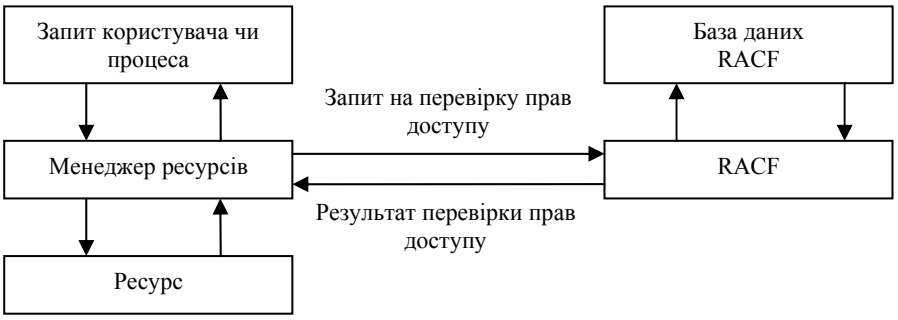

Рисунок 3 – Схема функціонування засобів захисту OS/390

Диспетчер доступу RACF забезпечує наступні можливості захисту ресурсів АС на платформі OS/390:

- гнучкий контроль доступу до захищених ресурсів;
- захист ресурсів, що додаються до системи;
- можливість захищати інформацію інших програмних продуктів;
- вибір централізованого або децентралізованого контролю за профілями;
- прозорість для користувачів;
- можливість встановлення програм-виходів (exit routines).

V Забезпечення стандартного функціонального профілю захищеності 3.КЦ.3

Автоматизована система, інстальована на сконфігурованій з вимогами достовірного обчислювального середовища платформі OS/390, може бути приведена до стандартного функціонального профілю захищеності "3.КЦ.3":

3.КЦ.3 = {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}.

Розглянемо послуги.

КД-2. Базова довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів.

КА-2. Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

ЦД-1. Мінімальна довірча цілісність. Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Множина об'єктів комп'ютерної системи (КС), які потребують захисту та перевірки цілісності, визначається спеціальним документом "Політика безпеки". Зокрема, потребують захисту системні набори даних, стандартні утиліти, набори даних з прикладним програмним забезпеченням КС, термінали, ресурси баз даних. Захист ресурсів забезпечується реєстрацією профілів відповідних класів.

Рішення про санкціонування доступу приймається RACF за алгоритмами дискретного та адміністративного принципу доступу. Для забезпечення послуг необхідно сформувати списки доступу до ресурсів, та встановити категорії і рівні безпеки для користувачів і ресурсів за адміністративним принципом доступу.

Сервер безпеки RACF дозволяє зміну прав доступу до об'єкту тільки суб'єктам з відповідними атрибутами та суб'єктам, які присутні в стандартному списку доступу об'єкта з правом ALTER.

Механізми захисту RACF передбачають можливість розмежування повноважень адміністраторів у межах певної множини груп (доменів) шляхом встановлення відповідних атрибутів на рівні групи.

З усіх класів об'єктів, що захищаються КС, фізично створюються лише набори даних. Профілі всіх інших об'єктів уже закладені в механізмах захисту. При реєстрації суб'єкта функціями для адміністрування суб'єктів та груп суб'єктів має бути створений профіль, який буде захищати всі створені суб'єктом набори даних (профіль "USERID.**", де USERID – ідентифікатор користувача). При експорті та імпорті разом з набором даних копіюється відповідний запис VTOC (Volume Table Of Contents), де міститься інформація про захищеність набору даних.

КО-1. Повторне використання об'єктів. Ця послуга дозволяє забезпечити коректність повторного використання об'єктів, гарантуючи, що в разі, якщо об'єкт, призначений для загального користування, виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Всі вимоги, що висуваються до цієї послуги, забезпечуються операційною системою, а саме механізмами керування пам'яттю (оперативною, віртуальною, на магнітних носіях), механізмами захисту оперативної пам'яті.

КВ-2. Базова конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

ЦВ-2. Базова цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

НК-1. Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ.

НВ-1. Автентифікація вузла. Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію.

В середовищі OS/390 ця послуга гарантується програмно-апаратним продуктом ICSF. ICSF (Integrated Cryptography Services Facility) – продукт фірми IBM, який підтримує загальну криптографічну архітектуру (Common Cryptographic Architecture), що базується на американському стандарті криптографічного перетворення (DES). З відкритих алгоритмів ICSF підтримує алгоритм RSA (Rivest-Shamir-Adelman).

Окрім шифрування та дешифрування інформації прикладні програми мають можливість використовувати відповідний інтерфейс для:

- генерування та розподілення криптографічних ключів для відкритих і закритих алгоритмів;
- генерування, перевірки та транслювання особистих ідентифікаційних кодів (PINs);
- гарантування цілісності даних за допомогою MAC-кодів, алгоритмів хешування та цифрових підписів.

Основна проблема використання ICSF – відсутність сертифікатів відповідності НДТЗІ. Тому він не придатний для захисту інформації, яка має категорію конфіденційності, але може бути використаний для захисту власних даних.

При неможливості його використання в зв'язку з відсутністю сертифікатів відповідності, послуга забезпечується засобами забезпечення конфіденційності системи "Рубіж".

ЦА-2. Базова адміністративна цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів.

КЗЗ має надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Процеси можуть запускатися або при старті системи, або командою оператора, або командою SUBMIT підсистеми TSO. В першому випадку запуск процесу регламентується доступом до набору даних "SYS1.PARMLIB". В другому випадку запуск процесу регламентується правом на виконання команди оператора START, яка належить класу OPERCMDS та відповідним профілем процесу в класі STARTED. В останньому випадку – наявністю права не нижче READ в профілі "JCL" класу TSOAUTH. В складі програмного інтерфейсу RACF є функції керування доступом за довірчим та мандатним принципами, за допомогою яких адміністратор може дозволяти та забороняти суб'єктам ініціацію процесів.

ЦО-1. Обмежений відкат. Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану.

Множина об'єктів КС, що підлягають відкату, описується документом "Політика безпеки". Відкат об'єктів баз даних відбувається засобами СКБД, а об'єктів операційної системи – шляхом відновлення з резервних копій.

НР-2. Захищений журнал. Реєстрація дозволяє контролювати небезпечні для комп'ютерної системи дії. Політика реєстрації, що реалізується КЗЗ, має визначати перелік подій, що реєструються. В документі "Політика безпеки" мають бути перераховані всі події, необхідні для реєстрації.

КЗЗ має бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Ця вимога реалізується засобами динамічного відстежування подій системи "Рубіж", зокрема всі події, що мають безпосереднє відношення до безпеки, реєструються в системному журналі.

Журнал реєстрації має містити інформацію про дату, час, місце, тип і успішність чи безуспішність кожної зареєстрованої події. Журнал реєстрації має містити інформацію, достатню для встановлення користувача, процесу і/або об'єкту, що має відношення до кожної зареєстрованої події. Журнал реєстрації подій, який входить до складу засобів динамічного відстежування системи "Рубіж", містить інформацію про дату та час виникнення події, суб'єкт, який спричинив виникнення події, об'єкт (клас та профіль) події, успішність події та причину неуспішності (в разі неуспішності).

КЗЗ має забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації. Система "Рубіж", в частині адміністрування засобів захисту OS/390, містить функції, за допомогою яких адміністратор може заборонити доступ до журналу подій, а також провести повний аудит журналу подій.

НИ-2. Одиночна ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до комп'ютерної системи.

Політика ідентифікації і автентифікації, що реалізується КЗЗ, має визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожен користувач має однозначно ідентифікуватися КЗЗ. При реєстрації суб'єкту призначається унікальний ідентифікатор, який однозначно ідентифікує користувача. Всі атрибути визначаються політикою безпеки і зберігаються в базі даних RACF.

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.