УДК 681.3.06

В.О. Хорошко
Державний університет інформаційно-комунікаційних технологій
Інститут захисту інформації

Н.Ф. Казакова
Міжнародний гуманітарний університет
Кафедра Інформаційної безпеки

НАУКОВІ ЗАДАЧІ СИНТЕЗУ ОРГАНІЗАЦІЙНО-ТЕХНОЛОГІЧНОЇ СХЕМИ СТВОРЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ КОМП'ЮТЕРНИХ МЕРЕЖ З ОБМЕЖЕНИМ ДОСТУПОМ

Пропонується технологічна схема, яка з єдиних позицій відображає комплекс наукових досліджень з проблеми створення і управління інформаційною безпекою в комп'ютерних мережах з обмеженим доступом на основі застосування програмних засобів захисту інформації.

Постановка проблеми в загальному вигляді та її зв'язок з науковими та практичними задачами. Ефективне застосування створюваних перспективних програмних систем захисту інформації (ПСЗІ) в комп'ютерних мережах з обмеженим доступом (КМОД) для захисту інформації (ЗІ) від несанкціонованого доступу (НСД) припускає організацію управління інформаційною безпекою (ІБ) в КМОД на основі застосування програмних засобів захисту інформації (ПЗЗІ).

Аналіз наукової і технічної літератури (наприклад, [1...7]) показує відсутність в даний час єдиного підходу до комплексного рішення проблеми створення ПСЗІ і управління ІБ в КМОД на основі застосування ПЗЗІ. Зазначена проблема є ще ***не вирішеною частиною*** загальної проблеми забезпечення ІБ в КМОД. Для її вирішення, згідно мал. 1, пропонується організаційно-технологічна схема процесу створення ПСЗІ для КМОД [8...10]. Таким чином, згідно зазначеного рисунку, ***метою статті*** є вирішення наукової задачі синтезу організаційно-технологічної схеми створення програмного забезпечення для КМОД. Відповідно до сказаного, досконало розглянемо та піддамо аналізу пропоновану організаційно-технологічну схему, призначення та функції її відповідних блоків та їх сукупностей.

Верхня група блоків на мал. 1 представляють завдання створення ПСЗІ і управління ІБ в КМОД на основі застосування ПЗЗІ. Таким чином, завдання створення ПСЗІ і управління ІБ в КМОД на основі застосування ПЗЗІ (блок 1 – *тут і далі: на мал. 1*) підрозділяються на:

– *завдання розробки ПСЗІ в КМОД* (блок 2)*;*
– *завдання організаційно-технологічного управління процесами ЗІ в КМОД на основі застосування ПЗЗІ* (блок 3).

Можна виділити чотири завдання розробки ПСЗІ в КМОД (блоки 4-7). Перш за все, на основі існуючого нормативно-методичного забезпечення, при обґрунтуванні вимог до ПСЗІ при створенні КМОД, необхідно сформувати вимоги для вибору або розробки ПЗЗІ (блок 4). Далі, відповідно до сформованих вимог, необхідно провести вибір або розробку ПЗЗІ (блок 5). В результаті створюється первинний варіант ПСЗІ, який надалі може допрацьовуватися. Можливість подальшого доопрацювання ПСЗІ пов'язана з тим, що, не дивлячись на задоволення окремих вимог, що пред'являється до ПЗЗІ, якість ПСЗІ в цілому може бути незадовільною. Тому необхідна комплексна оцінка якості ПСЗІ (блок 6).

Якість ПСЗІ взагалі характеризує її придатність задовольняти вимогам, які до неї пред'являються при застосуванні в даній комп'ютерній мережі (КМ) або в даному класі КМ [8]. Якість ПСЗІ при організації управління ІБ в КМОД на основі застосування ПЗЗІ (блок 6) характеризує придатність ПСЗІ задовольняти вимогам, що пред'являються до неї, при застосуванні в даній конкретній КМОД.

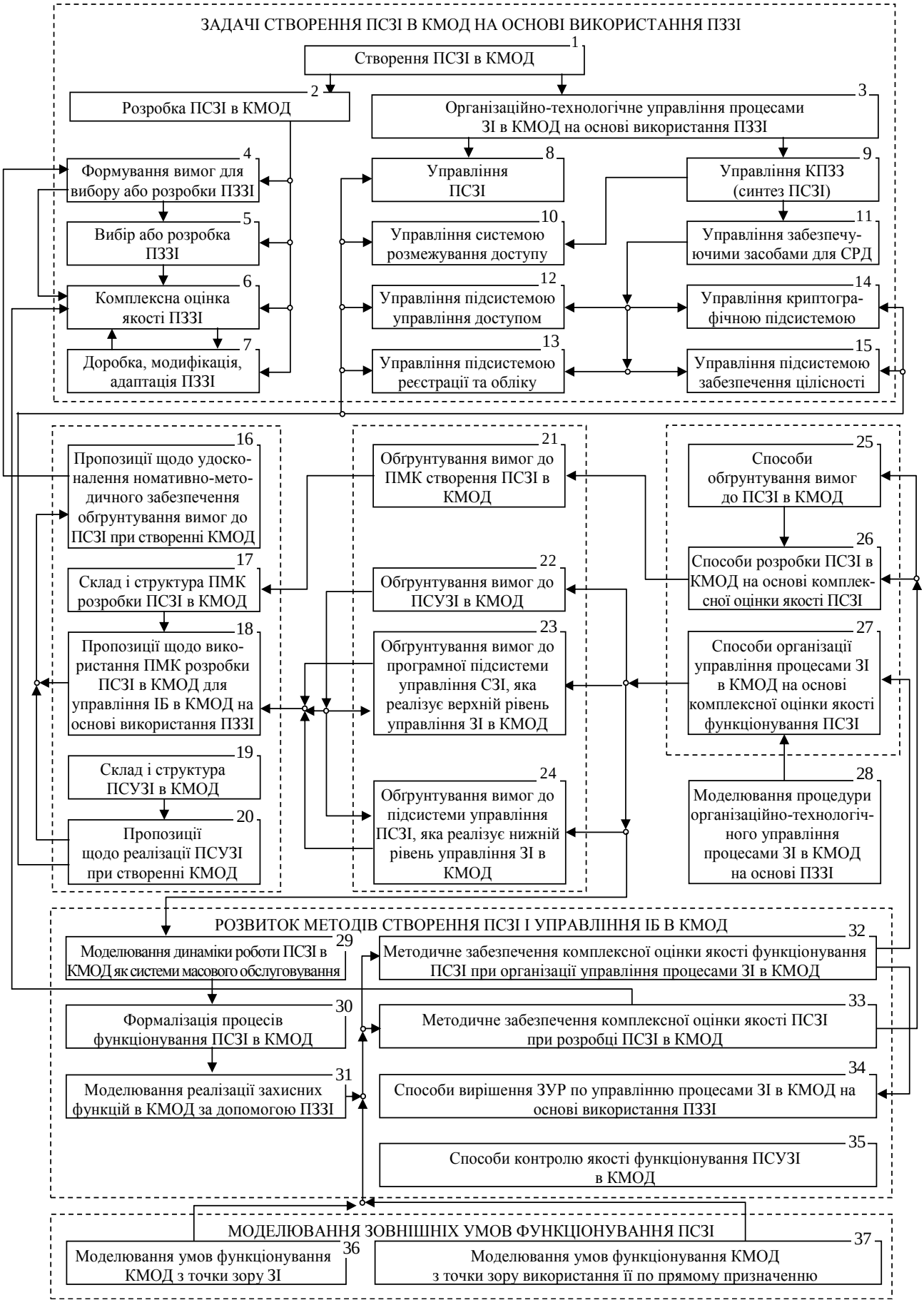

Рис. 1 – Організаційно-технологічна схема процесу створення ПСЗІ для КМОД

Оскільки ПСЗІ є програмною системою, то для комплексної оцінки її якості можна використовувати прийнятий підхід до комплексної оцінки якості програмних засобів [8...11]. Якщо відповідно до проведеної комплексної оцінки якості ПСЗІ в цілому не задовольняє вимогам, що пред'являються до неї, то необхідно провести доопрацювання (модифікація, адаптація) ПСЗІ (блок 7). Допрацьована ПСЗІ знову піддається комплексній оцінці якості і т.д. Таким чином, контур управління процесами ЗІ в КМОД на основі застосування ПЗЗІ може включати два основних взаємозв'язаних управляючих контури:

– контур верхнього рівня, який призначений для управління загальною організацією ЗІ – називатимемо його контуром управління ПСЗІ (блок 8)*;*
– контур нижнього рівня, який призначений для управління окремими ПЗЗІ.

Сукупність всіх ПЗЗІ, що входять до складу ПСЗІ, можна називати *комплексом програмних засобів захисту* (КПЗЗ) – по аналогії зі стандартизованим терміном «*комплекс засобів захисту*» – КЗЗ [15]. У зв'язку з цим контур управління нижнього рівня можна назвати *контуром управління КПЗЗ* (блок 9). Не дивлячись на те, що в діючих як вітчизняних, так і зарубіжних стандартах, в їх проектах і нормативних документах, які регламентують питання інформаційної безпеки, безпосередньо не відбиті питання управління ІБ, проте, на основі їх можна виявити структуру завдань управління КПЗЗ. Так, наприклад, згідно керівному документу РФ «Концепція захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації» [8, 12, 15], забезпечення захисту КМОД здійснюється системою розмежування доступу (СРД) суб'єктів до об'єктів доступу, яка виконується засобами для СРД. Тому управління КПЗЗ (синтез ПСЗІ) може підрозділятися на:

– управління СРД (блок 10)*;*
– управління забезпечуючими засобами для СРД (блок 11)*;*
– управління чотирма підсистемами (блоки 12-15)*.*

Рішення розглянутих задач управління ІБ в КМОД на основі застосування ПЗЗІ вимагає проведення комплексу різноманітних наукових досліджень. Для вирішення завдання формування вимог для вибору або розробки ПЗЗІ при створенні ПСЗІ в КМОД (блок 4) необхідно виробити пропозиції по вдосконаленню нормативно-методичного забезпечення обґрунтування вимог до ПСЗІ при створенні КМОД (блок 16).

Вказане вдосконалення нормативно-методичного забезпечення повинне здійснюватися у напрямі можливості максимального урахування специфіки конкретної КМОД, оскільки, не дивлячись на очевидну необхідність такого обліку при управлінні ІБ в КМОД, існуюче нормативно-методичне забезпечення не дозволяє це робити достатньою мірою.

Для вирішення завдання комплексної оцінки якості ПСЗІ при розробці ПСЗІ в КМОД (блок 6) необхідно розробити відповідне методичне забезпечення (блок 33).

Для вирішення завдань організаційно-технологічного управління процесами ЗІ в КМОД на основі застосування ПЗЗІ (блоки 8, 10, 12-15) необхідно виробити пропозиції по реалізації програмних систем управління захистом інформації (ПСУЗІ) при створенні КМОД (блок 20). Реалізація ПСУЗІ при створенні КМОД повинна здійснюватися так, щоб, з одного боку, забезпечувалося рішення задач організаційно-технологічного управління процесами ЗІ в КМОД, а з іншого боку, процес функціонування ПСУЗІ повинен бути інтегрований в процеси обробки інформації в КМОД так, щоб виключалася суперечність з прийнятою технологією. Для цього необхідно, щоб ПСУЗІ мала визначені склад і структуру (блок 19), а також коректно сполучалася з іншими підкласами систем захисту інформації (СЗІ) від несанкціонованого доступу (СЗІ НСД).

Одним з напрямів наукових досліджень на користь рішення задач управління ІБ в КМОД на основі застосування ПЗЗІ є створення програмно-методичного комплексу (ПМК) розробки ПСЗІ в КМОД. Перш за все, повинні бути визначені склад і структура цього ПМК (блок 17), і далі повинні бути розроблені пропозиції по використанню ПМК на користь

управління ІБ в КМОД на основі застосування ПЗЗІ (блок 18). Доцільність використання даного ПМК полягає в тому, що він дозволяє підвищити ефективність управління ІБ в КМОД за рахунок автоматизації розробки ПСЗІ в КМОД.

При виробленні пропозицій по вдосконаленню нормативно-методичного забезпечення обґрунтування вимог до ПСЗІ при створенні КМОД (блок 16) необхідно враховувати раніше розроблені пропозиції по використанню ПМК розробки ПСЗІ в КМОД (блок 18), а також вже розроблені пропозиції по реалізації ПСУЗІ при створенні КМОД (блок 20). ПМК розробки ПСЗІ в КМОД в сукупності з ПСУЗІ покликані забезпечити максимальне урахування специфіки конкретної КМОД при управлінні ІБ в ній, проте динаміка цього обліку різна: довгостроковий облік для ПМК розробки ПСЗІ в КМОД і поточний облік для ПСУЗІ.

Початковою основою для вибору складу і структури ПСУЗІ або ПМК розробки ПСЗІ є відповідні вимоги до даних об’єктів. Тому необхідним етапом при створенні ПМК розробки ПСЗІ в КМОД є обґрунтування вимог до нього (блок 21), а необхідним етапом при розробці ПСУЗІ в КМОД є обґрунтування вимог до неї (блок 22) і до її підсистем (блоки 23-24).

Розбиття ПСУЗІ на підсистеми є наслідком розділення контуру управління процесами ЗІ, що реалізовується ПСУЗІ, на два основних взаємозв’язаних управляючих контури – верхнього і нижнього рівнів. Відповідно до загальних уявлень про управління [8, 13] кожний з цих двох контурів можна представити як два взаємодіючі блоки – об’єкту управління і управляючої системи. Управляюча система передає управляючі дії на об’єкт управління, а інформація про стан об’єкту управління передається в управляючу систему [16].

Для контуру управління ПСЗІ об’єктом управління виступає ПСЗІ, а в якості управляючої система – програмна підсистема управління СЗІ, що є функціональною підсистемою ПСУЗІ.

Для контуру управління КПЗЗ в якості об’єкта управління виступає КПЗЗ, а управляючої система – підсистема управління ПСЗІ, що є функціональною підсистемою як ПСУЗІ, так і ПСЗІ.

Таким чином, обґрунтування вимог до підсистем ПСУЗІ в КМОД включає обґрунтування вимог до програмної підсистеми управління СЗІ, що реалізовує верхній рівень управління процесами ЗІ в КМОД, (блок 23) і обґрунтування вимог до підсистеми управління ПСЗІ, що реалізує нижній рівень управління процесами ЗІ в КМОД (блок 24).

У основі процесу автоматизованої розробки ПСЗІ в КМОД покладена процедура комплексної оцінки її якості, тому обґрунтування вимог до ПМК розробки ПСЗІ в КМОД (блок 21) може проводитися тільки на базі вироблення способів розробки ПСЗІ в КМОД на основі комплексної оцінки якості ПСЗІ (блок 26).

Оскільки якість ПСЗІ при організації управління ІБ в КМОД характеризує придатність ПСЗІ задовольняти вимогам, що пред’являються до неї, в КМОД способи розробки ПСЗІ на основі комплексної оцінки її якості (блок 26) розробляються на основі вище зазначених способів обґрунтування вимог до ПСЗІ в КМОД (блок 25). При цьому методичною базою розробки всіх цих способів є методичне забезпечення комплексної оцінки якості ПСЗІ при розробці ПСЗІ в КМОД (блок 33).

При розробці ПСУЗІ необхідно розробити способи організації управління процесами ЗІ в КМОД. Типове завдання управління процесами ЗІ, як і будь-яке завдання управління взагалі, полягає в забезпеченні досягнення (по можливості якнайкращої) мети управління. По вигляду мети управління і відповідному характеру функціонування управляючої системи розрізняють основні типи управління [8, 13, 16]:

– *програмне управління;*
– *авторегулювання;*
– *стеження;*
– *оптимальне управління.*

Стосовно КМОД, типове завдання управління процесами ЗІ на основі ПЗЗІ є найскладнішим завданням управління – завдання оптимального управління, в якому метою управління є підтримка необхідної залежності екстремального значення деякої функції від двох груп

параметрів – критерію оптимального управління. Параметри першої групи (зовнішні умови) міняються незалежно від управляючої системи. Параметри другої групи є регульованими, тобто їх значення можуть мінятися під впливом управляючих сигналів. Критерій оптимального управління в даному випадку, який можна назвати *якістю функціонування* ПСЗІ, має комплексний характер, що приводить до багатокритеріальності завдання оптимального управління. Це пов'язано з тим, що вимоги ІБ обов'язково суперечать функціональним вимогам до КМОД – зручності роботи, швидкодії [5, 8, 11] і т.д.

При оцінці якості функціонування ПСЗІ ефективність ЗІ в КМОД не можна розглядати у відриві від ефективності КМОД при роботі по прямому призначенню [5, 8, 14]. Тому можна говорити про якість функціонування ПСЗІ лише для конкретної КМОД і притому як для конкретних умов функціонування КМОД з погляду ЗІ (рівень конфіденційності оброблюваної інформації), які визначають характер і ступінь погроз захищеності інформації, так і для конкретних умов функціонування КМОД з погляду вимог до неї в плані функціонування по прямому призначенню.

Якість функціонування ПСЗІ при організації управління процесами ЗІ в КМОД необхідно відрізняти від просто якості ПСЗІ, яка характеризує придатність ПСЗІ задовольняти вимогам, що пред'являються до неї, при застосуванні в даній КМОД або в даному класі КМОД безвідносно до конкретних умов функціонування КМОД, що складаються. Завдання оптимізації характеристик якості ПСЗІ виникає при створенні ПСЗІ, а завдання оптимізації якості функціонування ПСЗІ виникає при управлінні процесами ЗІ в КМОД при реалізованій в ній ПСЗІ.

Таким чином, в основі організаційно-технологічного управління процесами ЗІ в КМОД на основі застосування ПЗЗІ лежить процедура комплексної оцінки якості функціонування ПСЗІ, тому обґрунтування вимог до ПСУЗІ в цілому і до її підсистемам (блоки 22-24) може проводитися тільки на базі вироблення способів організації управління процесами ЗІ в КМОД на основі комплексної оцінки якості функціонування ПСЗІ (блок 27). При цьому методичною базою вироблення цих способів є моделювання організації організаційно-технологічного управління процесами ЗІ в КМОД на основі ПЗЗІ (блок 28), а також застосування методичного забезпечення комплексної оцінки якості функціонування ПСЗІ при організації управління процесами ЗІ в КМОД (блок 32).

Методичне забезпечення комплексної оцінки якості функціонування ПСЗІ при організації управління процесами ЗІ в КМОД (блок 32) і методичне забезпечення комплексної оцінки якості ПСЗІ при розробці ПСЗІ в КМОД (блок 33) є складовими частинами результатів наукових досліджень по розвитку методів управління ІБ в КМОД на основі застосування ПЗЗІ (блоки 29-35). Ключовою складовою організаційно-технологічного управління процесами ЗІ в КМОД на основі ПЗЗІ є ухвалення рішень, що реалізуються відповідними підсистемами ухвалення рішень.

Складність завдань оптимального управління процесами ЗІ в КМОД на основі ПЗЗІ обумовлена складністю формалізованої постановки і рішення відповідних задач ухвалення рішень (ЗУР). Тому основоположними результатами наукових досліджень по розвитку методів управління процесами ЗІ в КМОД на основі ПЗЗІ є способи рішення ЗУР по управлінню процесами ЗІ в КМОД на основі застосування ПЗЗІ (блок 34).

Процеси контролю якості функціонування механізмів захисту, здійснювані відповідними підсистемами, реалізують функцію зворотного зв'язку управління процесами ЗІ в КМОД на основі ПЗЗІ. У зв'язку з цим необхідна розробка способів контролю якості функціонування ПСУЗІ в КМОД (блок 35).

Ухвалення рішень по управлінню процесами ЗІ в КМОД на основі ПЗЗІ проводиться на основі наступних даних [3, 8, 11]:

– аналізу умов функціонування КМОД як з погляду ЗІ, так і з погляду вимог до КМОД в плані функціонування по прямому призначенню;

– результатів контролю якості функціонування механізмів захисту.

Сукупність цих даних характеризує ситуацію при управлінні процесами ЗІ в КМОД на основі ПЗЗІ. Умови функціонування КМОД впливають на якість функціонування ПСЗІ при організації управління процесами ЗІ в КМОД, що обумовлює необхідність їх врахування у відповідних ЗУР. Крім того, умови функціонування КМОД впливають на якість ПСЗІ при розробці ПСЗІ в КМОД. Тому для створення як методичного забезпечення комплексної оцінки якості функціонування ПСЗІ при організації управління процесами ЗІ в КМОД (блок 32), так і методичного забезпечення комплексної оцінки якості ПСЗІ при розробці ПСЗІ в КМОД (блок 33), необхідне моделювання умов функціонування КМОД як з погляду ЗІ (блок 36), так і з погляду вимог до неї при функціонуванні по прямому призначенню (блок 37).

Окрім моделювання зовнішніх умов функціонування ПСЗІ (блоки 36-37), для створення вказаного методичного забезпечення необхідне моделювання внутрішніх процесів, що протікають в ПСЗІ (блоки 29-31). З погляду користувачів КМОД ПСЗІ фактично є системою масового обслуговування. При цьому порушник правил розмежування доступу повинен отримувати відмову в обслуговуванні, а будь-який суб'єкт доступу, що здійснює санкціонований доступ до інформації, повинен обслуговуватися. Обслуговування суб'єкта доступу ПСЗІ як системою масового обслуговування, є наданням йому доступу до інформації. Таким чином, початковим пунктом моделювання внутрішніх процесів, що протікають в ПСЗІ, є моделювання динаміки функціонування ПСЗІ в КМОД як системи масового обслуговування (блок 29).

Одним з основних етапів при моделюванні складних технічних та логічних систем, який істотним чином визначає якість моделі, є формалізація модельованих процесів. Як показав аналіз наукової і технічної літератури, для формалізації саме динаміки функціонування складних систем в рамках теоретико-графового підходу розроблені різні математичні об'єкти щодо розвитку ідеї про формалізацію орієнтованим графом складних систем (кінцеві автомати, мережі Петрі, Е-мережі та ін.). З метою формалізації процесів функціонування ПСЗІ в КМОД (блок 30) необхідно провести їх ієрархічну структуризацію. Для цього процес функціонування ПСЗІ представляється у вигляді послідовності реалізацій певних сервісних завдань по організації ЗІ в КМОД. У свою чергу, процес реалізації сервісних завдань представляється сукупністю функцій, що реалізують конкретний алгоритм ЗІ в конкретному сервісному завданні. Це дозволяє представити процес ЗІ в КМОД у вигляді послідовної зміни станів функціонування ПСЗІ. При цьому стани функціонування ПСЗІ відповідають виконанню конкретних функцій сервісного завдання з ЗІ. Перехід від одного стану до іншого означає виконання наступної, згідно алгоритму, функції забезпечення ЗІ. При такому розгляді формалізація процесів функціонування ПСЗІ в КМОД означає формалізацію станів функціонування ПСЗІ і переходів між ними. А оскільки стани функціонування ПСЗІ відповідають виконанню конкретних захисних функцій, то для моделювання внутрішніх процесів, що протікають в ПСЗІ, необхідне моделювання реалізації захисних функцій в КМОД за допомогою ПЗЗІ (блок31).

Висновок

Запропонована технологічна схема розробки програмного забезпечення для комп'ютерних мереж з обмеженим доступом з єдиних позицій достатньо повно відображає весь комплекс наукових досліджень з проблеми створення ПСЗІ і управління ІБ на основі застосування ПЗЗІ.

Список літератури

1. Гайкович В.Ю., Першин А.Н. Безопасность электронных банковских систем. – М.: Единая Европа, 1994. – 264 с. // [Электронный ресурс]: http://www.cplire.ru/rus/os/3_12/1/4.htm (Режим доступа ограниченный).

2. Торокин А.А. Инженерно-техническая защита информации: Учебн. пособие. – М.: «Гелиос АРВ» // [Электронный ресурс]: http://protected-house.ru/lib/book/index.php (Режим доступа свободный).

3. Модестов А.А., Ермилов Е.В. Структурный синтез как способ построения алгоритмов обнаружения угроз безопасности сегментов информационной сферы / Вестник Воронежского института МВД России. – №1,

2008. – С.175-181. // [Электронный ресурс]: http://www.imvd.vrn.ru/scientificwork/bulletin/1_2008/1_2008(2).pdf (Режим доступа свободный).

4. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебн. пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. – 264 с. // [Электронный ресурс]: http://oldteam.ru/content/view/231/2/ (Режим доступа свободный).

5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000. – 452 с. // [Электронный ресурс]: http://www.kti.ru/elib/elib.aspx?CID=66 (Режим доступа свободный).

6. Конявский В.А. Управление защитой информации на базе СЗИ НСД «Аккорд». – М.: Радио и связь, 1999. – 325 с., ил. // [Электронный ресурс]: http://www.okbsapr.ru/Docs/UZINBA/upravlenie_zashitoi_inf_na_baze_accord.pdf (Режим доступа свободный).

7. Антонюк А.А., Жора В.В., Мостовой В.Н. Угрозы информации и услуги безопасности / Проблемы программирования. – 2003, №4. – С.65-71 // [Электронный ресурс]: http://eprints.isofts.kiev.ua/188/1/06_Antonyuk.pdf (Режим доступа свободный).

8. Рогозин Е.А. Моделирование и алгоритмизация процесса проектирования программных систем защиты информации: дис. ... д-ра техн. наук: 05.13.12 Воронеж, 2006. – 327 с. // [Электронный ресурс]: РГБ ОД, 71:07-5/179 (Режим доступа ограниченный).

9. Задачи организационно-технологического управления процессами защиты информации в автоматизированных системах управления критических применений на основе использования программных средств защиты / Львович Я.Е., Заряев А.В., Дубровин А.С., Зюзина Н.Н., Макаров О.Ю., Рогозин Е.А., Сумин В.И. / Телекоммуникации. – 2002. – №12. – С. 41-45. – Библиогр.: 15 назв. // [Электронный ресурс]: http://ellib.gpntb.ru/index.php/elibgpntb.html?journal=ap&year=2003&num=2&art=7 (Режим доступа ограниченный).

10. Методологический подход к решению задач организационно-технологического управления процессами защиты информации в автоматизированных системах управления критических применений на основе использования программных средств защиты / Львович Я.Е., Дубровин А.С., Зюзина Н.Н., Макаров О.Ю., Рогозин Е.А., Сумин В.И. // Телекоммуникации. – 2003. – №1. – С. 37-41. – Библиогр.: 2 назв. // [Электронный ресурс]: http://ellib.gpntb.ru/index.php/ntb_5_15_2004.htm?journal=ap&year=2003&num=3&art=10 (Режим доступа ограниченный).

11. Багаев М.А., Дубровин А.С., Застрожнов И.И., Макаров О.Ю., Е.А. Рогозин, Сумин В.И. Методы и средства автоматизированной оценки и анализа качества функционирования программных систем защиты информации: Монография. – Воронеж: Воронеж. гос. техн. ун-т, 2004. – 181 с.

12. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. – М.: Воениздат, 1992 // [Электронный ресурс]: http://www.readbox.ru/390.html (Режим доступа свободный).

13. Глушков В.М. Введение в АСУ. – М.: Техника, Киев, 1972. – 310 с.

14. Муратов А.В., Рогозин Е.А., Застрожнов И.И. Управление разграничением доступа к информационным ресурсам автоматизированных систем при проектировании радиоэлектронных средств // Проектирование и технологии электронных средств. – Владимир: ВГУ, 2004. – №1. – С.9-12.

15. Моделирование и исследование динамики функционирования программный систем защиты информации для оценки и анализа качества их функционирования при проектировании и управлении// [Электронный ресурс]: http://www.mirrabot.com/work/work_69501.html (Режим доступа условно свободный).

16. Материалы сайта http://www.cultinfo.ru/fulltext/1/001/008/060/914.htm (Режим доступа условно свободный).