глобальные вычислительные сети, современные многозадачные и многопользовательские операционные системы.

Методы удаленного администрирования автоматизированных систем используют распределенную вычислительную среду, и для их анализа рассмотренные модели безопасности в классическом виде неприменимы.

Одна из моделей, которую можно использовать для анализа безопасности распределенных систем, – модель безопасности информационных потоков.

В данной модели все объекты системы делятся на две непересекающиеся группы: высокоуровневые объекты, имеющие право обрабатывать информацию высокого уровня секретности, и низкоуровневые. Все взаимодействия между данными группами объектов осуществляются через систему защиты.

На множестве объектов системы задается вероятностное распределение, оба множества состояний объектов являются случайными величинами. Для описания и анализа информационных потоков между ними используются понятия независимости и условного распределения. Данная модель рассматривает два подхода к определению безопасности информационных потоков, основанных на понятиях информационной невыводимости и информационного невмешательства.

Модель безопасности информационных потоков служит практическим примером подхода к построению системы защиты, которая разрешает корреляцию значений высокоуровневых и низкоуровневых объектов, но при этом остается безопасной.

С точки зрения методов удаленного администрирования, основанных на технологии «клиент-сервер», множество высокоуровневых объектов находится на серверной части, а низкоуровневых – на удаленных клиентских станциях, которые принимают управляющие команды, обрабатывают их и возвращают результат обработки серверу. Но с другой стороны, если абстрагироваться до уровня клиентской части, то множество высокоуровневых объектов представляет собой набор компонентов программы удаленного администрирования, например, специальной службы, драйвера и динамических модулей, а множество низкоуровневых объектов – пользовательские файлы. Поэтому необходимо также учитывать локальную политику безопасности для каждой клиентской станции.

В результате, можно сделать вывод, что для исследования и анализа безопасности систем, использующих в своей работе методы удаленного доступа и администрирования, не подходит ни одна из классических формальных моделей безопасности. Для получения наиболее точной оценки эффективности защиты таких систем необходимо использовать сочетание моделей, предназначенных для исследования детерминированных систем защиты, и моделей для анализа безопасности информационных потоков в распределенной вычислительной среде. Другой подход – разработка новой специализированной модели, учитывающей факторы удаленного администрирования автоматизированных систем, является темой дальнейших исследований в данной области.

Литература: 1. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. - Киев, 1999. 2. Проскурин В. Г. и др. Защита в операционных системах. – М., 2000. 3. Девянин П. Н. и др. Теоретические основы компьютерной безопасности. – М., 2000. 4. Michael A. Harrison. Theoretical Issues Concerning Protection in Operating Systems. 5. Ross J. Anderson. Lectures on Computer Science – Security. University of Cambridge, 1999.

УДК 638.235.231

ПРО ОДИН ПІДХІД ДО ВИЗНАЧЕННЯ ПОТРЕБ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ

Антон Михайлюк, Сергій Гончарук, Сергій Колотило
Національний Технічний Університет України «КПІ"

Анотація: **Розроблено механізм визначення потреб у захисті багаторівневих неоднорідних інформаційно-обчислювальних систем і побудови на основі отриманих даних комплексного засобу захисту, що відповідає державним стандартам технічного захисту інформації від несанкціонованого доступу.**

Summary: **In this methodological approach was developed mechanism of determining requirements in protecting of multilevel heterogeneous information-calculating systems and building complex protective medium on the bases of findings, which fully corresponds national standards of technical information protecting from unauthorized access.**

Ключові слова: **Методологічний підхід, захист від несанкціонованого доступу, оцінки потреб у захисті.**

I Вступ

Після винайдення першої ЕОМ інформаційне життя людства зазнало суттєвих змін. Сьогодні практично неможливо знайти галузь, в якій би не використовували комп'ютерну технологію. Застосування комп'ютера в різноманітних сферах людської діяльності стало стандартом de facto.

Наш час – епоха всеохоплюючої глобалізації та інформатизації суспільства. Інформація є одним із найважливіших факторів масового впливу в теперішньому житті. Як наслідок цих процесів виникає стрімке збільшення інформаційних потоків, що обробляються. Тенденції росту кількості інформації та подальший розвиток обчислювальної техніки, а особливо поява персональних комп'ютерів, призвели до появи нового типу інформаційно-обчислювальних систем – комп'ютерних мереж, які дозволяють набагато ефективніше використовувати сумарні ресурси для обробки значно більших об'ємів даних. Причому процеси глобалізації спостерігаються і в області побудови комп'ютерних мереж. Сучасні розвинуті комп'ютерні мережі є складними інформаційно-обчислювальними системами з багаторівневими й неоднорідними архітектурами, а також, як правило, взаємодіють з іншими подібними системами. При їх використанні для вирішення задач обробки (в тому числі збирання, зберігання, передачі і т. д.) критичних даних (інформації, що вимагає захисту) виникає потреба у використанні спеціальних додаткових засобів, що виконують функції забезпечення постійного та адекватного технічного захисту інформації. Для забезпечення найбільшої ефективності захисту, а також для відповідності державним нормам з захисту інформації дані засоби мають бути передбачені і реалізовані в самій архітектурі подібної комп'ютерної інформаційно-обчислювальної системи.

На жаль, на сьогоднішньому етапі розвитку технологій не існує універсального і єдиного ні технічного, ні програмного чи апаратно-програмного засобу захисту критичних даних у довільній мережі, а особливо у корпоративній мережі з розвинутою багаторівневою і неоднорідною архітектурою. Більше того, у зв'язку із значною комерціалізацією даної сфери діяльності, часто пропонуються лише односторонні рішення конкретного розробника, який прагне отримати максимальний прибуток від використання саме його технічного рішення, відкидаючи при цьому елементарні поняття доцільності використання тих чи інших засобів захисту, а також їх корисність та ефективність з практичної точки зору. Для ліквідації такої ситуації в області технічного захисту інформації був розроблений описаний нижче методологічний підхід до визначення потреб корпоративних комп'ютерних мереж щодо захисту інформації.

II Постановка завдання

Основною задачею даної роботи є побудова методологічного підходу до визначення потреб у технічному захисті від несанкціонованого доступу (НСД) до інформації, що обробляється у довільній корпоративній комп'ютерній мережі, на етапі проектування мережі, та побудова на основі цих потреб інформаційної моделі комплексу засобів захисту, який необхідно реалізувати. Даний методологічний підхід призначений для адміністраторів мереж подібного типу.

III Опис методологічного підходу

Об'єктом дослідження даного методологічного підходу є корпоративна мережа з неоднорідною архітектурою. Кінцевою метою є отримання інформаційної моделі комплексу засобів захисту інформації від несанкціонованого доступу, який має бути реалізований в рамках архітектури проаналізованої мережі.

Для того щоб позбутися неоднорідності архітектури і розгляду параметрів в єдиному логічно-структурному контексті пропонується вхідну багаторівневу мережу з неоднорідною архітектурою розбити на n однорідних за логічним контекстом і/або архітектурою рівнів, які називатимемо надалі сегментами. З урахуванням такого розбиття вхідна мережа матиме схематичний вигляд, який зображено на рисунку 1.

Далі в рамках одного сегмента відбувається побудова інформаційної моделі, зображеної на рисунку 2.

В ній сегмент розглядається з інформаційної точки зору, тобто виділяються об'єкти захисту, які становлять ресурси вхідної мережі та інформаційні потоки між ними. Ресурси мережі, що є об'єктами захисту, розділяють на 3 наступні категорії: засоби спеціально призначені для реалізації політики безпеки або керування потоками інформації; ті, які опосередковано впливають на безпеку (наприклад забезпечують

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

функціонування компонентів першого типу); не задіяні під час вирішення завдань забезпечення безпеки.

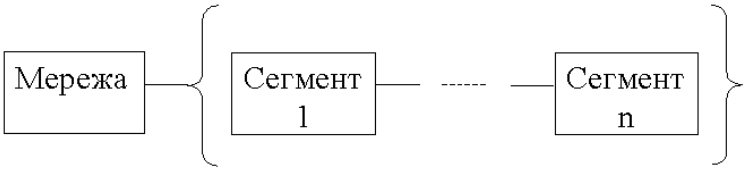

Рисунок 1 – Схема вхідної мережі після розбиття на сегменти

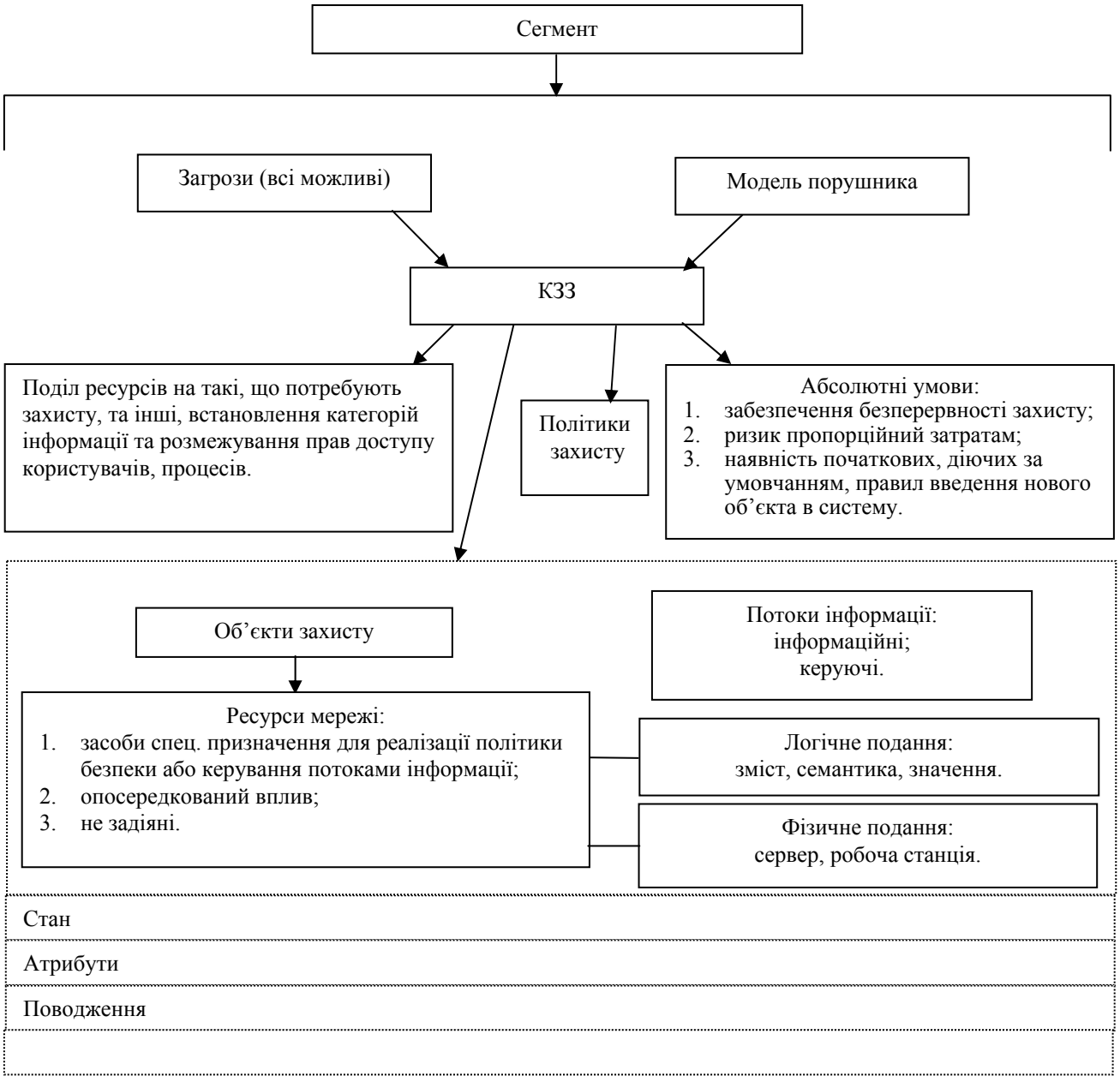

Рисунок 2 – Інформаційна модель сегмента

Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне (форма, синтаксис). Об'єкт характеризується своїм станом, що в свою чергу характеризується атрибутами і поводженням, яке визначає способи зміни стану. Для різних комп’ютерних систем (КС) об'єкти

можуть бути різні.

При розгляді взаємодії двох об'єктів КС, що виступають як приймальники або джерела інформації, слід виділити пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію. Далі розглядаються такі типи об'єктів КС: об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти. Прийнятий у деяких зарубіжних документах термін "суб'єкт" є суперпозицією об'єкта-користувача і об'єкта-процеса. Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного сегмента – ізольованої логічної області, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини. В інших сегментах об'єкти залишаються в пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим об'єктом-процесом або навіть об'єктом-користувачем, оскільки останній залишається "пасивним" з точки зору керуючого об'єкта. Іншими словами, об'єкти можуть знаходитись в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт. Перехід між станами означає, що об'єкт просто розглядається в іншому контексті. Пасивний об'єкт переходить в стан об'єкта-користувача, коли індивід (фізична особа-користувач) «входить» в систему. Цей об'єкт-користувач виступає для комплексу засобів захисту (КЗЗ) як образ фізичного користувача. Звичайно, за цим процесом іде активізація об'єкта-процесу за ініціативою користувача. Цей об'єкт-процес є керуючим для пасивних об'єктів всередині сегмента користувача. Об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти далі позначаються просто як користувачі, процеси і об'єкти, відповідно. Взаємодія двох об'єктів КС (звернення активного об'єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об'єктами і/або зміни стану системи. Як потік інформації розглядається будь-яка порція інформації, що передається між об'єктами КС.

Основою захисту сегмента є КЗЗ. КЗЗ – це сукупність всіх програмно-апаратних засобів, задіяних під час реалізації політики безпеки (захисту). Будь-який компонент сегмента, який внаслідок якого-небудь впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина КЗЗ.

Вводиться також поняття загрози, що являє собою будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків сегмента.

Загрози оброблюваної в автоматизованих системах інформації залежать від характеристик операційної системи (ОС), фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою. Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

Окремо виділяється модель порушника, яка є одним з джерел аналізу можливих загроз. Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу системи засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей проведення діалогу з системою — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів системи, аж до включення до складу системи власних засобів з новими функціями обробки інформації.

Припускається, що за своїм рівнем порушник — це фахівець вищої кваліфікації, який має повну інформацію про структуру комп'ютерної системи і КЗЗ. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Отримуючи на вході інформацію про структуру сегмента (ресурси захисту, всі можливі загрози, ймовірного порушника, атрибутів доступу об'єктів) даний методологічний підхід дозволяє на основі інтерактивного спілкування з користувачем (адміністратором системи) побудувати необхідну політику захисту реальної системи, виходячи з її потреб. Суттєвим також є дотримання певних початкових

обов’язкових умов: забезпечення безперервності захисту, ризик має зіставлятися з витратами на створення КЗЗ, повинні існувати початкові, діючі за умовчуванням, правила введення нового об’єкта в систему. КЗЗ в даному випадку можна розглядати як сукупність функціональних послуг, які відповідно підібрані для забезпечення технічного захисту інформації від НСД в рамках певного сегмента. Причому ця сукупність послуг повністю відповідає нормативним документам України про технічний захист інформації від НСД. На рисунку 2 вона зображена блоком з назвою “Політики захисту”. Політика безпеки поділяється на 4 основні підмножини: політику цілісності, політику доступності, політику конфіденційності, політику спостереженості. Кожна з 4-ьох підмножин є також в свою чергу сукупністю певної множини послуг, що відповідно забезпечують однойменні основні принципи інформаційної безпеки інформації. В рамках даного методологічного підходу введений такий термін як ”умови ранжирування”. Умови ранжирування дозволяють кінцевому розробнику КЗЗ розмежувати рівні кожної послуги відповідної політики, оцінити їх пріоритетність та визначити необхідну повноту їх реалізації в конкретній кінцевій інформаційно-обчислювальній системі. Умови існування дозволяють оцінити потрібність реалізації тієї чи іншої послуги в рамках реального сегмента. Методологічний підхід побудований за принципом логічної блок схеми, на виході якої отримуємо перелік необхідних послуг для повного забезпечення технічного захисту інформації від НСД, які повністю приведені у відповідність держстандартам України захисту інформації в комп’ютерних системах від несанкціонованого доступу. Фрагмент алгоритму визначення потрібного переліку наведений на рис. 3.

На рис. 3 позначено:

ОУДК – обов’язкові умови довірчої конфіденційності:

- запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі об'єкта і атрибутів доступу користувача, що ініціює запит;
- права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації;
- як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту;

УР М_Б_ДК:

- умови ранжирування мінімальної та базової довірчих конфіденційностей;

УР1 М_Б_ДК:

- необхідність розмежування конкретних процесів і захищених об’єктів за можливим доступом шляхом введення атрибутів доступу;

УР2 М_Б_ДК:

- необхідність розмежування конкретних користувачів і захищених об’єктів за можливим доступом шляхом введення атрибутів доступу;

ОУ Б_ДК – обов’язкові умови базової довірчої конфіденційності:

- КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його сегменту, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

IV Висновки

Запропонований методологічний підхід є спробою заповнити нішу в області комплексної оцінки потреб у технічному захисті від несанкціонованого доступу інформаційних систем. Вона суттєво спрощує та прискорює процес вибору необхідних для реалізації послуг в рамках конкретної архітектури довільної комп’ютерної мережі корпоративного масштабу.

Завдяки отриманим на виході результатам, що являють собою інформаційну модель комплексу засобів захисту, адміністратор отримує повний перелік послуг, які повинні бути реалізовані у його сегменті згідно з державними стандартами технічного захисту інформації від несанкціонованого доступу. Це сприяє отриманню на етапі проектування архітектури, яка повністю відповідає вимогам існуючих держстандартів.

Література: 1. Абалмазов Э. И. Методы и инженерно-технические средства противодействия информационным угрозам М.: Гротек, 1997. 2. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. 3. Барсуков В. С. Обеспечение информационной безопасности М.: Эко-Трендз, 1996. 4. Безопасность информационных технологий, Выпуск 4, Московский государственный инженерно-физический институт (технический университет), 1995. 5. Безопасность информационных технологий. Выпуск 1. М.: Госкомитет РФ по высшему образованию, МИФИ. 1994. 6. Безопасность информационных технологий. Выпуск 3, Московский

государственный инженерно-физический институт (технический университет), 1995. 7. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств

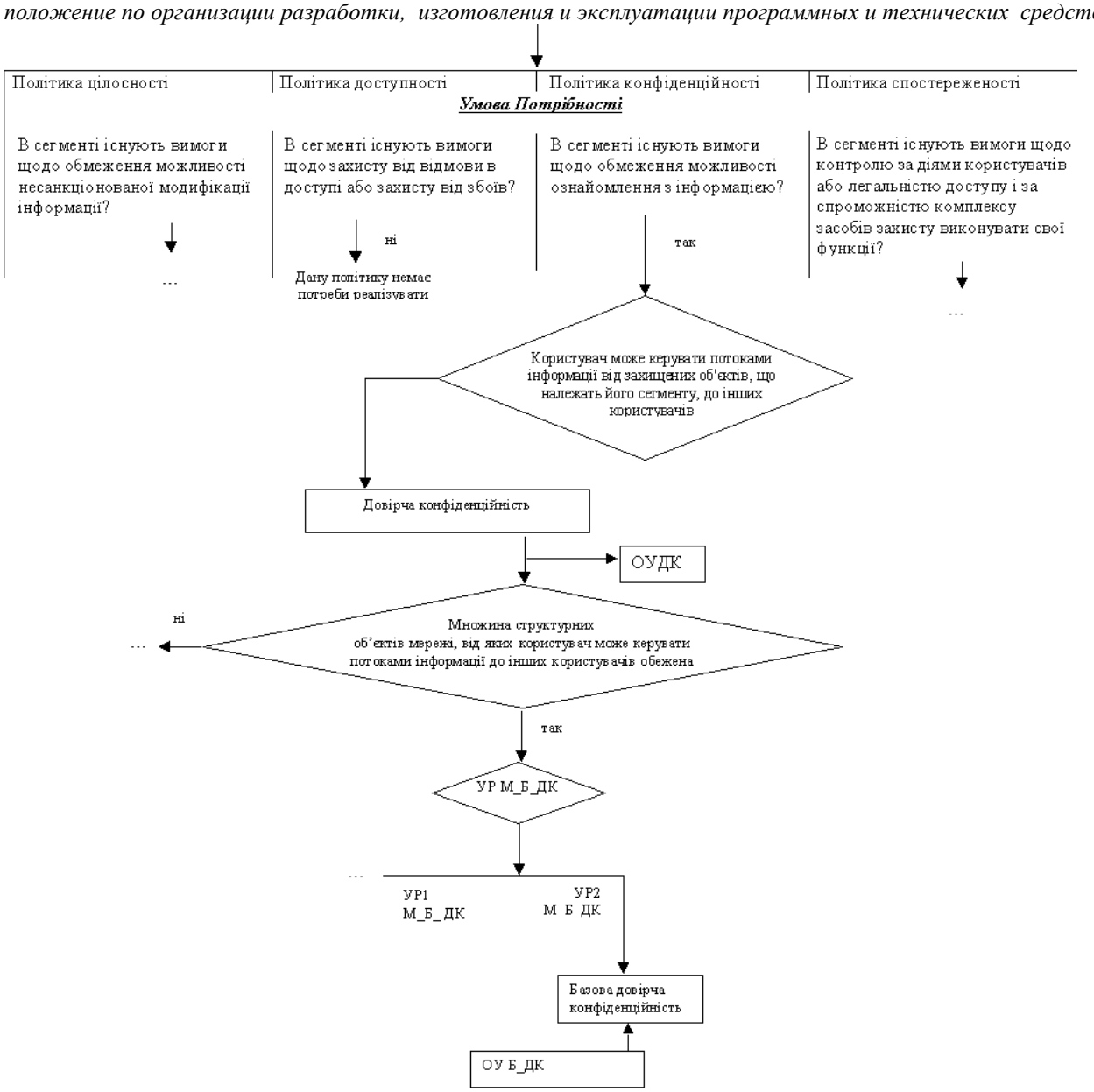

Рисунок 3 – Приклад аналізу потреб у захисті за запропонованою методикою

защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России,- М.: ГТК РФ, 1992. 29 с. 8. Герасименко В., Размахнин М. Защита информации в вычислительных, информационных и управляющих системах и сетях. — Зарубежная радиоэлектроника, 1985, № 8, с. 41—60. 9. Герасименко В. А. Защита информации в автоматизированных системах обработки данных М.: Энергоатомиздат, 1994. 10. Герасименко В. А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы. — Зарубежная радиоэлектроника, № 3, 1993. 11. Герасименко В. А. Комплексная защита информации в современных системах обработки данных. — Зарубежная радиоэлектроника, № 2, 1993. 12. Герасименко В. А., Малюк А. А., Погожин Н. С. Системно-концептуальный подход к защите информации в системах её обработки. — Безопасность информационных технологий. Выпуск № 3, 1995 г. Московский государственный инженерно-

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

физический институт (технический университет) 13. Домарев В. В. Защита информации и безопасность компьютерных систем К.: «Диасофт», 1999. 14. Еременко В. Т. Методологические подходы к оценке систем защиты информации по критерию "эффективность – стоимость". – Безопасность информационных технологий. Выпуск № 4, 1995 г. Московский государственный инженерно-физический институт (технический университет). 15. Закон Украины "О защите информации в информационных системах". 16. Закон Украины "Об информации". 17. Зарубежная радиоэлектроника (тематический выпуск по защите информации), 1989, № 12. 18. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. 19. Магауенов Р. Г. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации М.: Мир безопасности, 1997. 20. Першин А. Организация защиты вычислительных систем "КомпьютерПресс", № 10, 1992. 21. Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России, М.: ГТК РФ, 1992. 22. Ярочкин В. И. Безопасность информационных систем М.: Ось-89, 1996. 23. Eugene H Spafford. Security Seminar, Department of Computer Sciences, Purdue University, Jan 1996. 24. T D Garvey and Teresa F Lunt. Model based intrusion detection. In Proceedings of the 14th National Computer Security Conference, pages 372-385, October 1991.

УДК 621.396.6

ПОМИЛКИ ДІАГНОСТУВАННЯ ЗАСОБІВ ТЗІ ЗАГАЛЬНОГО ПРИЗНАЧЕННЯ ПРИ АГРЕГАТНОМУ МЕТОДІ РЕМОНТУ

Лев Сакович, Олексій Мервінський*, Олег Курченко

Київський військовий інститут телекомунікацій та інформатики,

**Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ*

Анотація: **Отримані аналітичні вирази з оцінки діагностичних похибок при використанні неоднорідних умовних алгоритмів діагностування в процесі ремонту засобів ТЗІ загального призначення агрегатним методом з використанням цифрових засобів вимірювання. Отримані результати доцільно використовувати при розробці діагностичного забезпечення перспективних зразків засобів ТЗІ загального призначення.**

Summary: **In paper the analytical expressions are obtained according to diagnostic errors at use of inhomogeneous conventional algorithms of diagnosing during repair of tools of an engineering guard of the information of common assignment by a modular method with use of digital tools of measurement. The obtained outcomes are expedient for using at development of diagnostic security of perspective samples of tools of an engineering guard of the information of common assignment.**

Ключові слова: **Засоби ТЗІ загального призначення, агрегатний метод ремонту, дерево логічних можливостей.**

Одним з перспективних напрямків підвищення ефективності ремонту засобів ТЗІ загального призначення є впровадження агрегатного методу ремонту (АМР).

Під ремонтом технічних виробів розуміється комплекс операцій по відновленню їхнього працездатного стану і відновленню ресурсів виробів або їх складових частин [1]. Стан виробу називається працездатним, якщо він здатний виконувати всі необхідні функції [2]. Розрізняють плановий, проведення якого регламентується нормативною документацією, і неплановий види ремонтів. Ці види ремонтів можуть виконуватися знеособленим методом, коли не зберігається приналежність відновлених складових частин до визначеного екземпляра технічного виробу. Знеособлений метод ремонту технічних виробів, при якому несправні агрегати заміняються новими або заздалегідь відремонтованими, називається агрегатним. Під агрегатом розуміється складальна одиниця технічного виробу, що володіє властивостями повної взаємозамінності, незалежного збирання і самостійного виконання визначеної функції у виробах різного призначення [1].

Впровадження АМР забезпечує поліпшення комплексного показника надійності, тобто коефіцієнта готовності технічних виробів, що характеризує імовірність справного стану і чисельно дорівнює [2]

$$A = T/(T + T_в),$$

де T – середній наробіток на відмовлення, $T_в$ – середній час відновлення.

Агрегатний метод ремонту дозволяє скоротити значення $T_в$ і збільшити T, якщо у виріб встановлюється новий агрегат або з більшим ресурсом, ніж той, що заміняється і відправляється в ремонт [3 – 5].