УДК 004.056.8

О.О. Скопа, Н.Ф. Казакова

Міжнародний гуманітарний університет, Одеса

АНАЛІЗ РОЗВИТКУ СУЧАСНИХ НАПРЯМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ

Приведено аналіз розвитку концепції інформаційної безпеки автоматизованих систем. Показано, що однією з причин невдач при вирішенні проблем підвищення захищеності автоматизованих систем є той факт, що сучасні моделі загроз мають вербальний характер. Це пояснюється тим, що відсутні реальні формальні моделі оцінок інформаційних втрат від дії загроз. Показується, відсутність формалізованих оцінок для слабо структурованих проблем не дозволяють провести кількісний і якісний аналіз збитків та дати практичні рекомендації по виявленню і скороченню вразливих місць в автоматизованих системах на етапі їх розробки в захищеному виконанні.

Ключові слова: *інформаційна безпека, автоматизована система, несанкціонований доступ, конфіденційність.*

Вступ

Постановка проблеми в загальному вигляді, її зв'язок науковими та практичними завданнями. Інформаційні технології поступово охоплюють всі області людської діяльності – як сферу матеріального виробництва, так і соціальну, військову й культурну сфери. Вони традиційно використовуються для автоматизації виконання великого числа монотонних і рутинних операцій: документообіг, завдання захисту і обліку, контролю і розподілу різних обчислювальних та інформаційних ресурсів, завдання, пов'язані з великими обсягами обчислень (наукові, технічні та економічні розрахунки), пошук необхідної інформації у великих інформаційних масивах та ін. Сучасний період розвитку суспільства характеризується, з одного боку, широким впровадженням інформаційних технологій у всі сфери сучасного суспільства, а з іншого – зростанням злочинів у сфері високих технологій, що вимагає проведення енергійних заходів по захисту інформаційного ресурсу автоматизованих систем (АС) від несанкціонованого доступу (НСД) зловмисників.

Метою роботи є аналіз передумов до розробки та практичної реалізації системного підходу до проектування і організаційно-технологічного управління програмними системами захисту інформації, що включає створення наукової концепції, методологічних основ, моделей і алгоритмів, направлених на підвищення якості функціонування систем інформаційної безпеки, що є **невирішеною раніше частиною** загальної проблеми.

Основний матеріал

Рішення проблеми інформаційної безпеки (ІБ) АС на сьогоднішній день прийняло регулярний характер та здійснюється на промисловій основі з

вкладенням значних матеріальних засобів. Проте з часом проблема ІБ АС не знижується, а має тенденцію тільки до зростання. Це пов'язано безпосередньо зі збільшенням потоків конфіденційної інформації, що обробляється АС [1].

Як показує **аналіз останніх досліджень та публікацій**, [2 – 9], одним з перспективних напрямів подальшого розвитку концепції ІБ АС на сучасному етапі є рішення проблеми на основі комплексної оцінки якості функціонування програмних засобів захисту інформації (ПЗЗІ) на етапах їх проектування і експлуатації, що дозволить проводити кількісну оцінку їх ефективності, якості функціонування, як вимагають як вітчизняні, так і зарубіжні нормативно-технічні документи з даної проблеми, а також забезпечити необхідний рівень захищеності АС на основі оптимізації керованих параметрів ПЗЗІ.

Серед робіт, які опубліковані за останнє десятиліття, та які внесли значний внесок у розвиток концепції ІБ АС на сучасному етапі, можна назвати наукові дослідження В.А. Герасименко [10, 11], В.В. Мельникова [12], Д.П. Зегжди і А.М. Івашко [13 – 15], В.І. Завгороднього [6], А.Ю. Щербакова [16] і О.Ю. Гацєнко [17]. Перша робота, наприклад, орієнтована на територіально-зосереджені автоматизовані системи обробки даних (АСОД) і організацію робіт по ЗІ при їх розробці. У другій роботі запропоновані концепція, принципи побудови захисту і оцінки рівня безпеки інформації в обчислювальних системах, мережах і АСУ. З цих позицій розглядаються інформація та умови її обробки в АС. У розрахунках надійності захисту автор в зазначеній роботі використане час життя інформації в АС. У третій роботі викладені результати досліджень, узагальнюючі вітчизняний і зарубіжний досвід у області розробки нормативних, теоретичних і практичних положень технології побудови спеціальних захищених інформаційних систем. У вказаних роботах описуються основні положення базових стандартів безпеки інформаційних технологій, досліджуються порушення ІБ, розглядаються формальні моделі безпеки та принципи їх використання в системах обробки інформації, аналізується існуюча архітектура захищених систем. У четвертій роботі освітлюються питання ЗІ в комп'ютерних системах. Тут же аналізуються та класифікуються можливі загрози безпеці інформації, розглядаються методи і засоби захисту від незаконного проникнення в обчислювальні мережі, розкриваються підходи до побудови та експлуатації комплексних систем захисту. П'ята робота присвячена розгляду широкого кола проблем по комп'ютерній безпеці, разом з теоретичним, методичний матеріал містить опис практичних підходів до реалізації безпеки систем безпеки. У шостій роботі представлені загальні принципи, моделі і методи рішення задач підвищення ефективності організаційного управління ЗІ в АС, які обробляють критично важливу інформацію. Основу пропонованої методології складає оптимальна організація процесу захисту, що включає ухвалення рішень по вибору адекватних загрозам стратегій захисту, управління технологіями обробки, передачі та зберігання інформації. Окрім загальних методів організаційного управління детально розглянуті питання антивірусного захисту.

Виходячи з результату аналізу вищезгаданих досліджень можна зробити висновок про те, що ці роботи, поза сумнівом, внесли значний внесок у розвиток концепції ІБ АС на сучасному етапі. В той же час загальним недоліком багатьох робіт, що розглядають завдання створення ПЗЗІ у формальній постановці, є слабке застосування в цільових функцій і обмеження основного комплексного показника якості (ефективності) їх функціонування, пов'язаного з імовірнісно-часовими характеристиками ПЗЗІ і комплексів засобів захисту в цілому, які достатньо детально розглянуті в [1].

У останні 20-25 років в розвинених промислових країнах робляться величезні зусилля у області забезпечення ІБ АС. Так, наприклад, в США створена федерація по боротьбі розкраданнями програмного забезпечення МО FAST [12].

Перший етап розвитку концепції ІБ АС знаменує собою 60-і роки минулого сторіччя [12]. Основу першого етапу складали ПЗЗІ як основні механізми ЗІ АС. ПЗЗІ включалися до складу існуючих АС, але практика показала їх високу уразливість з погляду ІБ при застосуванні такого роду захисту [12]. У результаті фахівці з ІБ АС дійшли висновку, що концепція ІБ, заснована на конструкції ПЗЗІ в АС не відповідає вимогам, що пред'являються до захищеності АС, особливо до АС конфіденційного напряму (АСК), де інформація, як правило, має гриф секретності [12].

Для подолання вказаних недоліків ухвалювалися наступні рішення:

1) створення в механізмах захисту спеціального організуючого елементу – ядра безпеки;

2) децентралізація механізмів захисту, аж до створення елементів, що знаходяться під управлінням користувачів АС;

3) розширення арсеналу використовуваних засобів, тобто комплексне рішення проблеми ІБ АС.

Вдосконалення цих рішень та впровадження їх в життя сучасного індустріального суспільства склало зміст 2 етапу розвитку концепції ІБ АС (70-і роки минулого сторіччя) [18]. Але, не дивлячись на всі вжиті заходи, проблема ІБ АС все більш загострювалася, про що знаменують факти зростання НСД до інформації в АС [1].

В цей же час була доведена теорема Харрісона про неможливість вирішення для загального випадку завдання про безпеку похідної ПЗЗІ при загаль-

ному завданні на доступ [12]. Рішення вищезгаданих суперечностей складає основний зміст 3 етапу (80-і роки минулого сторіччя і по наш час) розвитку концепції ІБ АС. При цьому генеральний напрям пошуків рішення проблеми ІБ АС ґрунтується на застосуванні основних принципів системного підходу в теорії ЗІ. Під системністю розумілося не тільки створення механізмів захисту, але й ЗІ на всіх технологічних етапах обробки, зберігання і передачі інформації в АС при комплексному використанні всіх ПЗЗІ [12]. При цьому всі ПЗЗІ, використовувані для ЗІ в АС, об'єднуються в умовний єдиний механізм захисту – ПЗЗІ АС.

За повідомленнями зарубіжної преси, наприклад [12], прикладом реалізації системного підходу до проблеми ІБ АС може служити ПЗЗІ, розроблена фірмою *Honeywell Inc.* за контрактом з Міністерством оборони США. Як основоположні принципи розробки ПЗЗІ розглядаються наступні положення [12]:

1) ПЗЗІ повинна розроблятися паралельно з розробкою АС;

2) реалізація функцій захисту на всіх етапах життєвого циклу інформації АС;

3) високі вимоги до захищеності АС.

Вищезгаданий аналіз дозволяє виділити наступні основні напрями забезпечення ЗІ, що вирішуються ПЗЗІ на сучасному етапі розвитку концепції ІБ АС [1]:

1) ПО грає основну роль в якісній обробці інформації;

2) наявність «грифа секретності» у програм АСК;

3) програмні засоби є одним з найуразливіших компонентів АСК.

Досвід експлуатації АСК показує, що на сучасному етапі від захисту потрібні абсолютно нові функції, а саме: механізми, що забезпечують безпеку цих систем. Ця проблема може бути вирішена засобами розмежування доступу, шляхом введення додаткових сервісних функцій по ЗІ до складу тих ПЗЗІ, що вже існують.

При забезпеченні безпеки нових типів інформаційних ресурсів ПЗЗІ повинні враховувати сучасні форми представлення інформації (гіпертекст, мультимедіа і т.д.). Це означає, що ПЗЗІ повинні забезпечувати безпеку на рівні інформаційних ресурсів, а не окремих документів, файлів або повідомлень.

Організація довіреної взаємодії сторін (взаємної ідентифікації/аутентифікації) в інформаційному просторі. Розвиток локальних мереж і Internet диктує необхідність здійснення ефективного захисту при видаленому доступі до інформації, а також взаємодії користувачів через загальнодоступні мережі. Сторони, що при цьому беруть участь, можуть функціонувати на різних апаратних платформах і в різних операційних системах (ОС).

Що стосується захисту від автоматичних засобів нападу – комп'ютерних вірусів, автоматизованих засобів злому, агресивних агентів, то можна відзначити наступне:

1) інтеграція захисту інформації в процес автоматизації її обробки є обов'язковим елементом;

2) ПЗЗІ не повинні вступати в конфлікт з існуючими додатками і технологіями обробки інформації, що склалися, а навпроти, повинні стати невід'ємною частиною цих коштів і технологій.

Будь-яка успішна реалізація загрози ІБ (атака) неодмінно використовує певні особливості побудови і функціонування АС або недоліки засобів захисту. Ці особливості досліджуються вже достатньо давно і отримали назву «Вади захисту» або «Вразливості». Всі механізми здійснення атак базуються на вадах захисту, які як би провокують появу засобів нападу. Таким чином, протистояння загроз та ПЗЗІ нагадує систему зі зворотним зв'язком – новий вигляд атак приводить до появи нових ПЗЗІ, а недоліки в ПЗЗІ приводять до появи нових засобів нападу і т.д. [13...15]. Розірвати це порочне коло нескінченного протистояння можна двома способами:

1) створити ефективні та бездоганно надійні ПЗЗІ від кожного типу атак;

2) усунути уразливості АС, які служать джерелом успішної реалізації загроз безпеки.

Відповідно, забезпечувати ІБ АС можна двома шляхами:

1) застосовувати достатньо універсальні ПЗЗІ від конкретних видів загроз;

2) з самого початку розробляти конкретну АС як захищену, усуваючи в її архітектурі уразливості, що є причинами успішної реалізації загроз.

ПЗЗІ від конкретних видів загроз безпосередньо не залежать від призначення АС і не вимагають модифікації у міру її розвитку.

Недоліки використання вказаних ПЗЗІ очевидні: для створення ефективної системи ІБ необхідно проаналізувати всі типи загроз і виробити ефективні механізми протидії для кожного типу. Крім того, практика показує, що забезпечення гарантованої ІБ АС на даному шляху є важко здійсненою внаслідок наступних чинників [13 – 15]:

– множина загроз постійно розширюється і має тенденцію експоненціального зростання. Це означає, що весь час з'являтимуться нові загрози, що вимагають нових заходів захисту, оскільки старі проти них безсилі. Поява нових ПЗЗІ приводитиме до появи нових класів загроз і т.д.;

– множина загроз росте не тільки кількісно, але й якісно, оскільки для того, щоб загроза відбулася, вона повинна принципово відрізнятися від тих, на які розраховані системи захисту. Це означає, що неможливо створити вичерпну класифікацію загроз безпеці і передбачати появу нових типів загроз.

На відміну від використання ПЗЗІ від конкрет-

них видів загроз, метод забезпечення ІБ АС шляхом початкової її розробки з архітектурою, позбавленою уразливостей, обумовлюючих успішну реалізацію загроз, має очевидні переваги: він не залежить від розвитку загроз, оскільки ліквідовує причину, а не слідство. Тому він ефективніший, ніж створення ПЗЗІ від кожного виду загроз. Проте даний метод відносно важко реалізувати. Він вимагає застосування технологій проектування та розробки АС, направлених на усунення причин успішної реалізації загроз. Замість використання достатньо універсальних ПЗЗІ в спочатку незахищених системах необхідно створювати захищені з самого початку АС з застосуванням вказаних технологій їх проектування і розробки.

На сучасному етапі розвитку концепції при створенні АСК доцільно використовувати обидва розглянуті шляхи забезпечення ІБ [13 – 15]. Якщо важливість завдання забезпечення ІБ особливо велика для даної АСК, то дану АСК необхідно спочатку розробляти як захищену. Якщо для захисту інформації в якій-небудь АСК використовувати шлях застосування достатньо універсальних ПЗЗІ від конкретних видів загроз, то можна або використовувати сертифіковані засоби, або розробляти нові, модернізувати існуючі функції даного класу, що краще враховують конкретні аспекти АСК в плані ІБ.

Велика увага в даний час приділяється проблемі ІБ ОС. Це обумовлено наступною обставиною [1]: особливу тривогу, на думку зарубіжних і вітчизняних засобів масової інформації, викликають шкідливі програмні дії. Посилює цю проблему поява і неухильне зростання та розвиток розподілених обчислювальних мереж (типу «Internet») і виникаюча у зв'язку з цим проблема захисту інформаційного ресурсу в цих мережах.

Але не дивлячись на те, що 3 етап в розвитку концепції ІБ АС знаменує використання принципів системного підходу в теорії ЗІ, у пресі знову стали з'являтися заяви про неможливість рішення проблеми ІБ АС [12]. Це пов'язано з тим, що питання ЗІ АС розглядалися без обмежень зв'язків з проектуванням і технологією функціонування конкретних АС.

Однією з причин невдач щодо рішення зазначеної проблеми можна назвати і те, що сучасні моделі порушників АС мають, як правило, вербальний характер, тобто складаються з наукових текстів, що супроводжуються блок-схемами, таблицями, графіками і т.д.). Призначення цих моделей – служити узагальненим і в той же час достатньо повно вираженим обсягом знань у області ІБ АС в рамках певної наукової концепції [1]. Як видно, відсутні реальні формальні (математичні) моделі оцінок інформаційних втрат від дії загроз, а також формалізовані (логіко-лінгвістичні) у разі слабо структурованих проблем, які б дозволили провести кількісний і якісний аналіз збитків і дати практичні рекомендації по виявленню і скороченню вразливих місць в АС на етапі їх розробки і експлуатації. Перші спроби рішення цієї проблеми були зроблені в роботах [2, 8, 9, 19], які присвячені розробці методології проектування ПЗЗІ в АСК. В той же час ці роботи мають і ряд істотних недоліків. В них, зокрема, запропоновані показники ефективності ПЗЗІ характеризують її тільки як об'єкт проектування. Це пов'язано з тим, що, як і будь-яка складна система, ПЗЗІ може ефективно функціонувати тільки при якісній реалізації відповідних функцій управління. Відповідно, організація ЗІ від НСД в АСК припускає наявність безперервного управління процесами ЗІ [1].

Головною причиною складного характеру вказаної проблеми є необхідність обліку множин як кількісних, так і якісних аспектів різнорідних властивостей і показників ПЗЗІ АСК. Оскільки при проектуванні ПЗЗІ багато вимог та показників носять якісний характер (наприклад, [20, 21]) унаслідок особливостей завдань і предметної області, то часто використовуються неформальні методи, особливістю яких є участь людини не тільки в постановці завдання, але і в процесі її рішення. Тут широко використовуються методи експертних оцінок та різні евристичні методи. При цьому отримувані рішення можуть бути достатньо далекі від дійсно оптимальних, але повинні забезпечувати виконання вимог ТЗ за прийнятний час. В даний час такий підхід найбільш поширений, але вимагає залучення кваліфікованих фахівців-експертів, а також широкого використання експериментально-статистичного матеріалу [1].

Також можливий експериментальний підхід, що реалізовує стратегію «реалізація загрози – протидія – оцінка – зміна ПЗЗІ», що дозволяє створити систему, перевірену на практиці, але вимагає великих часових і матеріальних затрат [2, 22]. Визначення значень таких показників можливе з застосуванням методів теорії ймовірностей, моделювання випадкових процесів (зокрема, напівмарківських [23]), теорії надійності складних систем, математичної логіки та експертних оцінок. Частково зняти цю суперечність дозволила робота [5], де автором розроблені критерії якості функціонування ПЗЗІ як об'єкту управління в АСК, що дозволяє визначити такий набір керованих параметрів (елементарні критерії якості функціонування ПЗЗІ), який у нинішній момент часу може забезпечити максимальний рівень захищеності при мінімізації негативного впливу ПЗЗІ на ефективність функціонування АСК в цілому по прямому призначенню. Але ця робота також повністю не зняла вищезгаданих суперечностей [5], оскільки в ній розглянуто рішення тільки одного конкретного управлінського завдання – контролю цілісності програмного забезпечення (робочого середовища) в АСК, і запропоновані методи рішення

даної задачі не можуть бути поширені на рішення в цілому проблеми проектування та оптимального управління ПЗЗІ в АСК, що вимагає проведення подальших досліджень у вказаному напрямі.

Таким чином, аналіз недоліків в рішенні проблеми створення концепції ІБ АС на сучасному етапі дає підставу для пошуку їх причин на початку шляху, тобто аналізі умов функціонування, інформаційній структурі, програмному забезпеченні АС і оцінці якості функціонування ПЗЗІ АС і т.д., тобто, додавання до існуючої концепції ІБ АС нової методології, заснованої на процедурах моделювання і комплексної оцінки якості функціонування програмних засобів і систем захисту інформації при їх проектуванні та управлінні.

Висновок

Аналіз розвитку концепції ІБ АС на сучасному етапі показав, що однією з причин невдач при знаходженні рішення проблеми підвищення захищеності АС можна назвати ту, що сучасні моделі загроз порушників АС мають, як правило, вербальний характер, тобто слід констатувати відсутність реальних формальних моделей оцінок інформаційних втрат від дії загроз, а також відсутність формалізації у разі слабо структурованих проблем, які б дозволили провести кількісний та якісний аналіз збитків і дати практичні рекомендації по виявленню та зменшенню вразливих місць в АС на етапі їх розробки в захищеному виконанні, що вимагає розробки математичної моделі оцінки збитків в АСК від реалізації загроз НСД.

Список літератури

1. Рогозин Е.А. Моделирование и алгоритмизация процесса проектирования программных систем защиты информации: дис. ... д-ра техн. наук: 05.13.12 / Е.А. Рогозин. – Воронеж, 2006. – 327 с. – РГБ ОД, 71:07-5/179.

2. Информационная безопасность: учебн. пособие / В.И. Сумин, А.И. Кустов, Е.А. Рогозин, М.В. Коротков. – Воронеж: ВЭПИ, 2003. – 154 с.

3. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М.: ИПК Издательство стандартов, 2002. – 64 с.

4. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. – М.: Воениздат, 1992. – 68 с.

5. Методы и средства автоматизированного управления подсистемой контроля целостности в системах защиты информации / А.С. Дубровин, О.Ю. Макаров, Е.А. Рогозин, В.И. Сумин и др. – Воронеж: ВГТУ, 2003. – 165 с.

6. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебн. пособие / В.И. Завгородний. – М.: Логос, 2001. – 264 с.

7. Использование требований ГОСТ Р ИСО/МЭК 15408-2002 для оценки программных систем защиты информации автоматизированных систем / А.С. Дубровин, М.В. Коротков, О.Ю. Макаров, Е.А. Рогозин // Вестник ВГТУ: Сер. Радиоэлектроника и системы связи. – 2003. – Вып. 4.3. – С. 30-32.

8. Методы и средства анализа эффективности при проектировании программных средств защиты информации / О.Ю. Макаров, А.В. Муратов, Е.А. Рогозин и др. – Воронеж: ВГТУ, 2002. – 125 с.

9. Методические основы проектирования программных систем защиты информации / А.А. Голиусов, А.С. Дубровин, В.В. Лавлинский, Е.А. Рогозин. – Воронеж: ВИРЭ, 2002. – 96 с.

10. Герасименко В.А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко. – В 2 кн.: Кн. 1. – М.: Энергоатомиздат, 1994. – 400 с.

11. Герасименко В.Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений / В.Г. Герасименко // Информация и безопасность: Регион. науч.-техн. вестник. – Воронеж: ВГТУ, 1999. – Вып. 4. – С. 66-67.

12. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.

13. Зегжда Д.П. Как построить защищенную информационную систему? / Д.П. Зегжда, А.М. Ивашко; под ред. Д.П. Зегжды и В.В. Платонова. – СПб.: Мир и семья, 1997. – 320 с.

14. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.

15. Зегжда П.Д. Теория и практика обеспечения информационной безопасности / П.Д. Зегжда. – М.: Яхтсмен, 1996. – 192 с.

16. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности / А.Ю. Щербаков. – М.:, 2001. – 352 с.

17. Гаценко О.Ю. Защита информации. Основы организационного управления / О.Ю. Гаценко. – СПб.: Сентябрь, 2001. – 228 с.

18. Мелихов А.Н. Ориентированные графы и конечные автоматы / А.Н. Мелихов. – М.: Наука, 1971. – 416 с.

19. Львович Я.Е. Способы комплексной оценки эффективности при проектировании прогаммных систем защиты информации в автоматизированных системах управления критических приложений / Я.Е. Львович, Е.А. Рогозин // Прикладные задачи моделирования и оптимизации: сб. науч. тр. – Воронеж: ВГТУ, 2000. – С. 31-39.

20. Гостехкомиссия РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционирован1юго доступа к информации. Классификация автоматизированных систем и требования по защите информации. – М.: Воениздат, 1992. – 136 с.

21. Гостехкомиссия РФ. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. – М.: Воениздат, 1992. – 88 с.

22. Типовой стенд исследования каналов несанкцио-

нированного доступа к информации, обрабатываемой в информационных системах / Е.А. Рогозин, А.Ф. Саморковский, С.А. Смирнов, Р.П. Понякин // Организационно-правовые и информационно-технические проблемы обеспечения безопасности в современных условиях: Тезисы докладов III Всерос. научн.-практ. конф. «Охрана-99». – Воронеж, 1999. – 145 с.

23. Казакова Н.Ф. Розробка та дослідження ефективних алгоритмів визначення надійності пристроїв управління резервним обладнанням інформаційних мереж: дис... канд. техн. наук: 05.12.02 / Н.Ф. Казакова.. – К.: Український НДІ зв'язку, 2005. – 215 с.

Надійшла до редколегії 5.02.2009

Рецензент: д-р техн. наук, проф. А.І. Рибак, Міжнародний гуманітарний університет , Одеса.

АНАЛИЗ РАЗВИТИЯ СОВРЕМЕННЫХ НАПРАВЛЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

А.А. Скопа, Н.Ф. Казакова

Приведен анализ развития концепции информационной безопасности автоматизированных систем. Показано, что одной из причин неудач при решении проблем повышения защищенности автоматизированных систем является тот факт, что современные модели угроз имеют вербальный характер. Это объясняется тем, что отсутствующие реальные формальные модели оценок информационных потерь от действия угроз. Показывается, отсутствие формализированных оценок для слабо структурированных проблем не позволяют провести количественный и качественный анализ убытков и даты практические рекомендации по выявлению и сокращению уязвимых мест в автоматизированных системах на этапе их разработки в защищенном выполнении.

Ключевые слова: *информационная безопасность, автоматизированная система, несанкционированный доступ, конфиденциальность.*

ANALYSIS OF DEVELOPMENT OF MODERN DIRECTIONS OF INFORMATIVE SAFETY OF THE AUTOMATED SYSTEMS

O.O. Skopa, N.F. Kazakova

The analysis of development conception of informative safety in the automated systems is resulted. It is rotined that at the decision of problems increase of protected the automated systems is one of reasons failures circumstance that the modern models of threats have verbal character. It is explained to those, that the absent real formal models of estimations informative losses from action of threats. It is shown, absence of the formalized estimations for the poorly structured problems does not allow to conduct the quantitative and high-quality analysis of losses and date practical recommendations on the exposure and reduction of vulnerable places in the automated systems on the stage of their development in the protected implementation.

Keywords: *information safety, automated system, unauthorized access, confidentiality.*