у мережі вимагає подальшого дослідження.

VI Висновки

Детально розглянуто розподіл послуг безпеки за рівнями моделі архітектури взаємодії відкритих систем.

При формуванні функціонального профілю захищеності інформаційно-телекомунікаційних систем можна виділити групи функціональних послуг безпеки: загальні послуги, які мають бути реалізовані поза інформаційно-телекомунікаційною системою; послуги, які повинні бути розподілені, скоріш рівномірно, по інфраструктурі інформаційно-телекомунікаційної системи; послуги "компенсаційного" типу (такі як конфіденційність і цілісність), для яких дійсна постановка проблеми оптимального розподілу функцій між прикінцевими пунктами та інфраструктурою системи.

Проблема розподілу функцій та механізмів безпеки в інформаційно-телекомунікаційних системах вимагає подальших досліджень у частині формування номенклатури оптимальних показників характеристик системи як початкових даних для аналізу, розробки практичних методик оцінки показників, визначення залежності витрат на систему безпеки від рівня захищеності тощо, а також удосконалення практичних методик оцінки втрат від реалізації загроз інформаційній безпеці.

*Література: **1**. Александров А. М., Кравец Л. З., Петренко С. А., Эркин А. Г. Построение наложенных систем криптографической защиты // "Электросвязь", – М:, № 5, 2003. – С. 41-42. **2.** Мильковский А. Г. Обеспечение безопасности связи в телефонных сетях общего пользования // "Бизнес и безопасность", – К:, № 1, 2000. – С. 12-13. **3.** Кузьмин А. С., Бочков С. И., Ивин Ю. Э. Методы обеспечения информационной безопасности в АТМ-сетях. // "Электросвязь", – М:, № 9, 2001. – С. 28-32. **4.** ETSI TR 101 664: Intelligent Network (IN); IN interconnect security features, 1999. **5**. ETSI ETR 083: Universal Personal Telecommunication (UPT); General UPT security architecture, 1993. **6.** Бондаренко М., Скрыпник Л, Потий А. Перспективы применения международного стандарта ISO/IEC в Украине. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 3, 2001. С 7-26. **7.** Петренко С. Методические основы защиты информационных активов компании // – www.infosecurity.ru/-gazeta/content/031104/article03.-html. **8.** ISO/IEC 17799:2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою. **9.** Гончарок М. Х., Островский В. В. Выбор параметров системы защиты информации в цифровых АТС с функциями ISDN. // "Вестник связи", № 4, 2000, – С. 99-105. **10.** I CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991; **11.** Протоколи информационно-вычислительных сетей: Справочник / С. А .Аничкин, С. А. Белов, А. В. Бернштейн и др. Под ред. И. А. Мизина, А. П. Кулешова. − М.: Радио и связь, 1990. 504 с. **12.** "Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах", затверджений наказом ДСТСЗІ СБУ № 76 від 24. 12.2001 р. **13.** Гладкова И. Г. Живой разговор о NGN // "Вестник связи", № 12, 2003. – С. 37-55. **14.** Панин О. А., Журин С. И. Оптимизация параметров систем охранной сигнализации как задача многокритериального выбора. // Защита информации. Конфидент № 1, 2004. – С. 84-87. **15.** Черноруцкий И. Г. Методы оптимизации и принятия решений. С.-Пб, 2001, С. 248.*

УДК 681.3.06

ПРО ГАРАНТІЇ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Анатолій Антонюк, Віктор Жора*, Віталій Мостовой*, Сергій Пустовіт**

Академія ДПС України

**Інститут програмних систем НАНУ*

***ННДЦ оборонних технологій і воєнної безпеки України*

Анотація: **Вивчається одна з груп критеріїв нормативних документів системи технічного захисту інформації – критерії гарантій. Розглядаються питання їх формалізації та пропонується підхід щодо оцінки рівня захищеності комп'ютерних систем і вартості реалізації систем захисту.**

Summary: **The assurance criteria group of normative documents of technical information protection system is analyzed. The problems of their formalization are considered. The approach to estimation of protectability level of computer systems and protection systems realization cost is also given.**

Ключові слова: **Комп'ютерна система, гарантії, вимога, дія.**

I Вступ

Як відомо, спроможність комп'ютерної системи (КС) забезпечувати певний рівень захисту оброблюваної

інформації визначається функціональними критеріями [1], які розбиті на чотири групи: конфіденційності, цілісності, доступності і спостереженості. Кожна з груп критеріїв описує послуги певних видів та рівнів, що забезпечують захист відповідно від загроз одного з чотирьох основних типів: конфіденційності, цілісності, доступності і спостереженості. В свою чергу, кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Таким чином, вимоги функціональних критеріїв є необхідними умовами досягнення КС певного рівня захищеності. Однак, зазначені необхідні умови базуються на інших, теж необхідних умовах, якими є вимоги критеріїв гарантій, що дозволяють оцінити коректність реалізації послуг в КС. Критерії гарантій містять вимоги до:

- архітектури комплексу засобів захисту (КЗЗ);
- середовища розробки;
- послідовності розробки;
- середовища функціонування;
- експлуатаційної документації;
- випробування КЗЗ.

В Критеріях введено сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в КС послуги дійсно дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації КС. Звичайно, є певна і очевидна якісна залежність між рівнем гарантій і кількістю та якістю вимог – чим вище рівень, тим більше вимог треба виконувати.

Для виконання наведених вимог в необхідному обсязі, крім якісного їх порівняння, необхідно мати можливість їх кількісного порівняння, яке було б дуже корисним для полегшення процедури призначення певного рівня гарантій, мінімізації витрат на початкових етапах створення КС, при визначенні рівня захищеності КС, а також у задачах щодо визначення можливих витрат на побудову систем захисту інформації (СЗІ). Відповідних нормативних документів стосовно цих питань поки що немає. Проте, як показує аналіз складу вимог до гарантій, навіть за загальними рекомендаціями з [1] можна отримати досить важливі висновки щодо їх подальшого застосування в конкретних КС.

Згідно з [1], гарантії забезпечуються як в процесі розробки, так і в процесі оцінки. В процесі розробки гарантії забезпечуються діями розробника СЗІ щодо забезпечення правильності (коректності) розробки. В процесі оцінки гарантії забезпечуються шляхом перевірки додержання розробником вимог Критеріїв, аналізу документації, процедур розробки і постачання, а також іншими діями експертів, що здійснюють оцінку.

Метою даної роботи є аналіз складу вимог, розробка їх детального і більш точного переліку, розробка математичної моделі шкали, яка дозволила б певним чином оцінювати рівень реалізації вимог щодо гарантій.

II Аналіз вимог щодо гарантій

Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки і більшою мірою відносяться до архітектури програмного забезпечення (ПЗ). Додержання цих вимог забезпечується розробником ще на стадіях проектування КЗЗ. Передусім, вимоги до архітектури покликані забезпечити структурованість КЗЗ відповідно до таких принципів проектування ПЗ, як модульність, інкапсуляція і приховування даних.

Для низьких рівнів критеріїв гарантій розробник може обмежитись описом складових компонент КЗЗ. Для більш високих (проміжних) рівнів вимагається логічне поділення вихідного коду на окремі незалежні компоненти (модулі), що ідентифікуються, та ізоляція компонентів КЗЗ, критичних для безпеки. Для самих верхніх рівнів розробник під час проектування ПЗ повинен зосередити зусилля на зменшенні обсягу КЗЗ до мінімального набору компонентів.

Для полегшення процесу оцінки вимог вважаємо за доцільне наведений в [1] перелік вимог щодо архітектури (це також стосується і всіх інших груп вимог) представити більш детально, внаслідок чого отримано наступну таблицю.

Таблиця 1 – Вимоги до архітектури

	Зміст вимог	1	2	3	4	5	6	7
1	КЗЗ повинен реалізовувати політику безпеки	+	+	+	+	+	+	+
2	Всі компоненти КЗЗ повинні бути чітко визначені	+	+	+	+	+	+	+
3	КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів			+	+	+	+	+

4	Кожний з компонентів КЗЗ повинен бути спроектований відповідно до принципу мінімуму повноважень			+	+	+	+	+
5	Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш низького рівня				+	+	+	+
6	З боку розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки					+	+	+
7	Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту					+	+	+
8	Розробка ПЗ переважно має бути спрямована на мінімізацію складності КЗЗ					+	+	+
9	КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою					+	+	+
10	Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи, як модульність побудови і приховання (локалізація) даних					+	+	+

Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку розробника.

В процесі розробки від розробника вимагається визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги (вимоги, що повинні бути виконані раніше, ніж можна приступати до наступного етапу).

Крім того, повинні бути документовані стандарти, які використовувались під час розробки ПЗ. Використовувані мови програмування і компілятори мають відповідати вимогам національних, міждержавних або міжнародних стандартів. В іншому випадку слід надати повне визначення і опис мови, яка використовувалась. Додатково має бути документовано використання залежних від реалізації або апаратури опцій мови програмування.

Для більш високих рівнів гарантій вимоги до середовища розробки включають вимоги необхідності документування використовуваних методик фізичної, технічної, організаційної і кадрової безпеки.

Керування конфігурацією є необхідною і невід'ємною частиною будь-якої спроби розробки, а особливо захищених КС. Додержання вимог даного розділу критеріїв гарантій дозволяє забезпечити впевненість експертної комісії в тому, що розробник може повністю керувати конфігурацією оцінюваної КС.

Розробник повинен розробити, запровадити і підтримувати в дієздатному стані документовані методики керування конфігурацією КС на всіх стадіях її життєвого циклу. При цьому розробник може розробити і використати систему керування конфігурацією, що найкраще відображає і складність КС, і розміри організації розробника. Критерії керування, можливе використання засобів автоматизації і належний рівень формалізації процедур і перевірок визначаються розробником (і підтверджуються експертною комісією) таким чином, щоб бути настільки сумісним з іншими компонентами середовища розробки, наскільки це можливо. Важливо, щоб усі процедури, ролі і відповідальність всього персоналу, задіяного в керуванні конфігурацією, були чітко визначені і документовані.

Система керування конфігурацією повинна бути орієнтована на вирішення чотирьох основних завдань: визначення конфігурації, регулювання конфігурації, облік стану і перевірка якості конфігурації.

Таблиця 2 – Вимоги до середовища розробки

	Зміст вимог	1	2	3	4	5	6	7
	Процес розробки							
1	Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії	+	+	+	+	+	+	+
2	Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги	+	+	+	+	+	+	+
3	Розробник має описати стандарти кодування, яких необхідно дотримуватися в процесі реалізації, і гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів			+	+	+	+	+

Продовження таблиці 2

4	Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена			+	+	+	+	+
5	Всі залежні від реалізації параметри мов програмування або компіляторів мають бути документовані			+	+	+	+	+
6	Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної та кадрової безпеки				+	+	+	+
	Керування конфігурацією							
7	Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу	+	+	+	+	+	+	+
8	Система керування конфігурацією повинна забезпечувати керування внесенням змін до апаратного забезпечення, програм постійного запам'ятовуючого пристрою, вихідних текстів, об'єктних кодів, тестового покриття і документації	+	+	+	+	+	+	+
9	Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ	+	+	+	+	+	+	+
10	Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вихідного коду і обліку всіх змін з появою нових версій				+	+	+	+
11	Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації				+	+	+	+
12	Повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ, від несанкціонованої модифікації або руйнування						+	+

Послідовність розробки

Вимоги до процесу проектування забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС, і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

Вимоги до гарантій передбачають наявність чотирьох основних рівнів деталізації КС у процесі її створення: функціональна специфікація, проект архітектури, детальний проект, реалізація. Експертна комісія здійснює аналіз для визначення коректності опису КС для кожного рівня деталізації і його відповідності опису попереднього рівня. Для кожної конкретної КС експертна комісія і розробник можуть спільно визначити необхідні рівні деталізації процесу розробки, які можна розглядати як функціональну специфікацію, проект архітектури і детальний проект.

Залежно від рівня гарантій і рівня деталізації передбачається можливість використання трьох способів (стилів) специфікації: неформалізований, частково формалізований і формалізований. Неоднозначність специфікацій зменшується з використанням більш високого рівня формалізації.

Неформалізована специфікація має стиль текстового документа мовою повсякденного спілкування. Для неформалізованої специфікації вимагається представити визначення термінів, що використовуються в контексті, які відрізняються від звичайних, що використовуються у повсякденній мові. Частково формалізована специфікація складається мовою з обмеженим синтаксисом і доповнюється поясненнями, написаними мовою повсякденного спілкування. Мова з обмеженим синтаксисом може являти собою повсякденну мову з жорсткою структурою речення і ключовими словами, що мають спеціальне значення, або бути діаграматичною (наприклад, діаграми потоків даних, станів або переходу). Для побудови частково формалізованої специфікації як на базі діаграм, так і на базі мови повсякденного спілкування необхідно сформулювати набір угод, що визначають обмеження синтаксису. Формалізовані специфікації мають представлення, яке базується на добре встановлених математичних концепціях, і супроводжуються поясненнями звичайною мовою. Ці математичні концепції використовуються для визначення синтаксису і семантики подань і несуперечливих правил доказу, які підтримуються логічними посиланнями. Властивості, критичні для безпеки, повинні виражатися мовою формалізованої специфікації. Формалізовані представлення повинні дозволяти описати і ефект (результат) виконання функції, і всі зв'язані з нею виняткові або помилкові умови. Якщо використовуються ієрархічні специфікації, то необхідно показати, що кожний рівень включає властивості, встановлені для попереднього рівня.

Критерії гарантій включають також вимоги до відповідності специфікацій рівня деталізації. Рівень

зусиль, необхідних для досягнення такої відповідності, зростає разом з рівнем гарантій. Для його характеристики використовують терміни “показати”, “продемонструвати” або “довести”.

Якщо від розробника вимагається показати повну відповідність між представленнями КС, це означає, що є необхідністю наявність відповідності тільки між основними елементами кожної специфікації. Прикладом може бути використання таблиці, елементи якої відображають відповідність, або використання належного представлення діаграми проекту. Якщо від розробника вимагається продемонструвати повну відповідність між представленнями КС, то вимагається наявність відповідності між більш дрібними елементами кожної специфікації. Демонстрація відповідності виконується на основі аналізу з використанням структурованого наукового підходу, що дає переконливі аргументи на користь того, що існує повна відповідність між елементами двох специфікацій. Якщо від розробника вимагається довести повну відповідність між представленнями КС, то необхідною є наявність відповідності між ще більш дрібними елементами кожної специфікації. Відповідність між елементами має бути виражена формально.

Функціональні специфікації повинні описувати, які послуги надає КС у разі мінімуму або повної відсутності інформації про те, як вони представлені. Послуги безпеки описуються у формі політики безпеки і моделі політики безпеки.

Політика безпеки описує КС як набір послуг безпеки. Кожна послуга описується відповідно до вимог функціональних критеріїв для певного рівня даної послуги і з урахуванням необхідних умов. Для всіх рівнів гарантій політика безпеки подається у стилі неформалізованої специфікації і показується її відповідність більш деталізованій специфікації. Фактично, політика безпеки може бути визначена в технічному завданні на КС. Модель політики безпеки дозволяє точніше виразити вимоги політики безпеки. Стиль специфікації моделі політики безпеки варіюється залежно від рівнів гарантій від неформалізованого до формалізованого.

Проект архітектури є старшим або верхнім рівнем специфікації проекту, який відображає функціональну специфікацію в основні компоненти проекту КС. Для кожного з основних компонентів КС проект архітектури описує його призначення і функції, визначає послуги безпеки, що реалізуються ним, а також взаємодію всіх компонентів. Проект архітектури описує, яку функцію виконує кожний компонент.

Детальний проект є нижнім і найбільш детальним рівнем специфікації, який поділяє проект архітектури на менші за обсягом проекти його компонентів. Детальний проект повинен мати достатню міру деталізації, щоб дозволити почати реалізацію. Для кожного компонента детальний проект повинен містити опис його призначення і функцій. Має бути визначений порядок взаємодії всіх компонентів. Ця взаємодія представляється на рівні зовнішніх інтерфейсів потоків даних, керування і т. ін. Детальний проект описує і те, яку функцію виконує кожний компонент, і те, як він це робить, включаючи алгоритми і внутрішні інтерфейси.

Реалізація є завершальним представленням КС, що складається з програмного, програмно-апаратного і апаратного забезпечення. Кожний компонент реалізації повинен бути створений і документований відповідно до вимог процесу проектування. Інтерфейси та інші компоненти, що згадуються, мають бути описані в документації.

Таблиця 3 – Вимоги до послідовності розробки

	Зміст вимог	1	2	3	4	5	6	7
	Функціональні специфікації (політика безпеки)							
1	На стадії розробки технічного завдання розробник повинен розробити функціональні специфікації КС	+	+	+	+	+	+	+
2	Представлені функціональні специфікації КС повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ	+	+	+	+	+	+	+
3	Політика безпеки повинна містити перелік і опис послуг безпеки, що надаються КЗЗ	+	+	+	+	+	+	+
	Функціональні специфікації (модель політики безпеки)							
4	Функціональні специфікації повинні включати модель політики безпеки		+	+	+	+	+	+
5	Стиль специфікації: неформалізована		x					
6	частково формалізована			x				
7	формалізована				x	x	x	x
8	Відповідність політиці безпеки		1	1	2	2	2	2
	Проект архітектури							
9	На стадії розробки ескізного проекту розробник повинен розробити проект архітектури КЗЗ	+	+	+	+	+	+	+

10	Представлений проект архітектури КЗЗ повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними	+	+	+	+	+	+	+
11	Повинні бути описані будь-які використовувані зовнішні послуги безпеки	+	+	+	+	+	+	+
12	Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення	+	+	+	+	+	+	+
13	Стиль специфікації: неформалізована	x	x					
14	частково формалізована			x	x	x		
15	формалізована						x	x
16	Відповідність моделі політики безпеки		1	1	1	2	3	3
	Детальний проект							
17	На стадіях розробки технічного проекту або робочого проекту розробник повинен розробити детальний проект КЗЗ	+	+	+	+	+	+	+
18	Представлений детальний проект КЗЗ повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму	+	+	+	+	+	+	+
19	Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ	+	+	+	+	+	+	+
20	Стиль специфікації: неформалізована	x	x	x				
21	частково формалізована				x	x	x	
22	формалізована							x
23	Відповідність проекту архітектури		1	1	1	1	2	3
	Реалізація							
24	Розробник повинен подати вихідний код: частини КЗЗ			+	+	+	+	+
25	всього КЗЗ					+	+	+
26	всіх бібліотек часу виконання							+
27	Відповідність детальному проекту			1	1	1	1	2

Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється замовнику без несанкціонованих модифікацій, а також інсталюється і ініціалізується замовником так, як це передбачається розробником. Оцінка КС забезпечує гарантії того, що КС правильно реалізує політику безпеки, правильно функціонує і будується на припущенні, що функціонування КС починається з безпечного стану.

При цьому розробник повинен гарантувати, що конфігурація, яка поставляється замовнику даної КС, є сертифікованою конфігурацією. Крім того, під час постачання розробник повинен забезпечити захист КС від несанкціонованої модифікації. Цей захист за своєю природою може бути технічний, організаційний або фізичний. Технічний захист може полягати, наприклад, у використанні шифрування або криптографічних контрольних сум, паролів, що відкривають доступ до критичного ПЗ, перевірок на відповідність ПЗ еталону і т. ін. Організаційний захист може полягати, наприклад, у перевірці конфігурації для досягнення впевненості в тому, що замовнику поставлена потрібна версія, для чого можуть застосовуватися процедури керування якістю, задіяні розробником при пакуванні КС. Фізичний захист може полягати, наприклад, у використанні вакуумної упаковки компонентів ПЗ і документації і використанні інших оболонок, що запобігають або фіксують спроби фізичного доступу. Коли КС доставлена і її цілісність перевірена, замовнику необхідні інструкції з інсталяції і ініціалізації КС. Наведені вказівки повинні описувати всі параметри конфігурування і можливі обмеження.

Таблиця 4 – Вимоги до середовища функціонування

	Зміст вимог	1	2	3	4	5	6	7
1	Розробник повинен представити засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану	+	+	+	+	+	+	+
2	Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску	+	+	+	+	+	+	+
3	Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється замовнику, точно відповідає еталонній копії			+	+	+	+	+
4	Для підтримки відповідності між КЗЗ, що поставляється замовнику, і еталонною копією повинна існувати система керування розповсюдженням захищеної КС						+	+

Документація

Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються КС для реалізації політики безпеки, встановленої в його організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

У складі експлуатаційної документації розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ оцінюваної КС, настанови адміністратору щодо послуг безпеки і настанови користувачу щодо послуг безпеки. Зміст цих документів залежить від політики безпеки, що реалізується КС. Ніяких особливих вимог до назв, формату або структур документів дані критерії не ставлять.

Документація може бути загальною або в ній можуть бути явно виділені документи (розділи), призначені для адміністратора безпеки і для звичайного користувача. В будь-якому випадку наведеної в документації інформації повинно бути достатньо для того, щоб і адміністратор, і звичайні користувачі мали змогу виконувати свої функції.

Вимоги до документації є загальними для всіх рівнів гарантій.

Випробування КЗЗ

Для демонстрації того, що КЗЗ оцінюваної КС піддавався випробуванням, і доказу повноти цих випробувань розробник повинен надати експертам документально оформлені результати випробувань. При організації випробувань послуг безпеки і механізмів захисту і документуванні їх результатів треба керуватися вимогами ДСТУ 2853-94, ДСТУ 2851-94 та ін. Вимоги до випробувань визначають такі основні елементи планування і проведення випробувань розробником: план випробувань, програма і методика випробувань і результати випробувань (журнал випробувань, звіт, протокол випробувань).

В плані випробувань повинна бути викладена стратегія випробувань розробника. План повинен надавати детальний опис всіх тестованих частин КЗЗ. Сюди входять зовнішні інтерфейси КЗЗ, всі політики, привілеї, механізми послуг захисту і специфічних викликів системних функцій, бібліотечного ПЗ і т. Ін. План має також відображати середовище випробувань, будь-які особливі умови, що створюються для проведення випробувань, і засоби випробувань. Повинні бути наведені аргументи на користь повноти тестового покриття.

Програма і методика випробувань повинні визначати процедури тестування кожного елемента, визначеного у плані випробувань (наприклад, системних викликів). Для кожного окремого тесту має бути докладно описано використання засобів випробувань, необхідне оточення і особливі умови. Рівень деталізації процедур випробувань має бути достатнім для наступного повторення випробувань експертами. Розробник повинен також описати очікувані результати кожного тесту.

Інформація, що міститься в документах, які представляють результати випробувань, дозволяє експертам оцінити реальну ефективність і повноту проведених випробувань, їх відповідність плану, програмі і методиці, а також організувати проведення сертифікаційних випробувань.

Таблиця 5 – Вимоги до випробувань КЗЗ

	Зміст вимог	1	2	3	4	5	6	7
1	Розробник повинен надати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки	+	+	+	+	+	+	+
2	Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	+	+	+	+	+	+
3	Розробник повинен надати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	+	+	+	+	+	+
4	Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з’явилися нові “слабкі місця”		+	+	+	+	+	+
5	Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку розробника				+	+	+	+

III Оцінки реалізації вимог критеріїв гарантій

В практичних задачах важливим є визначення для вимог критеріїв гарантій двох чинників: оцінок їх повноти (або якості) та вартості реалізації.

Розглянемо перший чинник. Детальний аналіз складу всіх вимог критеріїв гарантій показує, що оцінку

повноти їх реалізації зручно робити в термінах ймовірностей, тобто величина ймовірності може характеризувати певний рівень реалізації вимоги. Проте безпосередньо для більшості вимог таку оцінку отримати дуже важко, оскільки фактично вони мають характер рекомендацій щодо їх виконання, формулювання майже всіх вимог мають досить розпливчастий та різнорідний характер, внаслідок чого іноді дуже важко зафіксувати рівень їх реалізації. Отже фактично мова може йти тільки про певний рівень їх виконання. Наприклад, перша вимога до архітектури [1] формулюється наступним чином: „КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені". Тут відразу ж виникає цілий ряд питань:

- який саме тип політики безпеки має реалізовуватися;
- наскільки детально вона має реалізовуватися;
- коли можна констатувати, що КЗЗ реалізує політику безпеки;
- що головне: політика безпеки чи визначення компонент;
- наскільки детально визначаються компоненти;
- що означає „чітко визначені".

До того ж, відсутні нормативні документи, що регламентують процес реалізації вимог, отже фактично мова може йти тільки про певний рівень їх виконання. Тому для більш зручного користування наведений в [1] перелік всіх вимог доцільно було представити більш детально**.**

Звернемо увагу на те, що в більшості випадків кожну вимогу можна розглядати як ланцюжок певних незалежних і ще більш конкретних та наглядних дій чи операцій (в подальшому – дій), для яких ймовірності їх реалізації оцінити набагато простіше [2]. Більше того, такий процес деталізації можна поглибити ще на одну чи навіть більше ступенів. Звичайно, така конкретизація суттєво полегшує процес їх оцінки – оцінки таких ймовірностей отримати набагато легше, ніж для вимоги в цілому, оскільки поняття дії є більш конкретним та наглядним порівняно з поняттям вимоги. Проте задача отримання оцінок відповідних ймовірностей все ж залишається, і розв'язується вона в основному за допомогою експертних оцінок, і лише в деяких випадках – за допомогою методів моделювання. Деякі міркування щодо вирішення такої задачі розглядаються в [3].

Зупинившись на рівні деталізації дій, позначимо ймовірність реалізації k-ої дії p_{ijk}, де: i – номер рівня гарантій, i=1,…,7; j – номер групи вимог, j=1,…,6; k-– номер дії для даної вимоги, k=1,…, n_{ij}. Індекси в числах n_{ij} підкреслюють їх залежність від рівня гарантій та групи вимог. Як зазначено в [1], всі наведені групи вимог, а також самі вимоги в основному є незалежними одна від одної. Вважаючи також незалежними дії, обчислимо ймовірності p_{ij} кожної з вимог за формулою:

$$p_{ij} = \prod_{k=1}^{n_{ij}} p_{ijk} \,. \tag{1}$$

В свою чергу ймовірність реалізації p_i i-го рівня гарантій дорівнює:

$$p_i = \prod_{i=1}^{6} p_{ij} = \prod_{i=1}^{6} \prod_{k=1}^{n_{ij}} p_{ijk} \,, \tag{2}$$

оскільки всього визначено 6 груп вимог. Саме ця ймовірність може використовуватися для отримання оцінки рівня захищеності конкретної АС, яка має i-ий рівень гарантій.

Розглянемо питання оцінки вартості реалізації вимог критеріїв гарантій. Можна сформулювати наступні зауваження:

1. З точки зору витрат вимоги вищих рівнів гарантій повинні бути більш вагомими (більш витратними з точки зору їх практичної реалізації) порівняно з нижчими рівнями. Такий висновок ґрунтується на простому міркуванні: для реалізації вищих рівнів треба більше зусиль та витрат, ніж для нижчих.
2. Деталізація вимог на дії суттєво полегшує проведення оцінок значень витрат для реалізації окремих дії, ніж для вимог в цілому, причому об'єктивніше і точніше.
3. Для кожної дії визначимо величину витрат c_{ijk} (звичайно, в певних умовних одиницях) щодо її реалізації, де: i – номер рівня гарантій, i=1,…,7; j – номер групи вимог, j=1,…,6; k – номер дії для даної вимоги, k=1,…,n_{ij}.

Тоді виникає можливість легко оцінювати вартість реалізації будь-якої вимоги в цілому – простим сумуванням витрат (з певними ваговими коефіцієнтами a_{ijk}) спочатку за кількістю дій, що визначають деяку вимогу (це буде оцінка для даної вимоги), а в подальшому – за вимогами:

$$c_i = \sum_{j=1}^{6} \sum_{k=1}^{n_{ij}} a_{ijk} c_{ijk} \qquad (3)$$

Практично ця величина може слугувати базою для отримання більш точних оцінок вартості створення всієї СЗІ. Вагові коефіцієнти характеризують певну залежність між різними діями при їх реалізації. Їх значення, а також значення відповідних вартостей є предметом експертних оцінок.

Із запропонованого підходу випливає досить проста схема його можливої комп'ютерної реалізації. Вона є практично аналогічною змісту критеріїв [1], в яких у формі таблиць детально описані як самі послуги за рівнями, так і відповідні їм функції. Для отримання кількісних оцінок застосовуються формули (1) та (2). Якщо необхідно введення ще одного (чи більше) ступеню деталізації, то це проводиться цілком аналогічно. Розробка такої системи є предметом подальших досліджень.

Введені таким чином ймовірності та витрати фактично є критеріями, що дозволяють розв'язувати важливу практичну проблему – проблему порівняння різних рівнів гарантій, причому не тільки якісно, а навіть кількісно.

V Висновки

Таким чином, в роботі проведено аналіз вимог критеріїв гарантій на предмет їх складу та властивостей. Здійснено формальний опис вимог, а також визначено важливий підхід щодо проведення процесу порівняння вимог критеріїв гарантій за певною шкалою. Саме завдяки сформульованому підходу виявилася можливість отримати загальні оцінки рівня захищеності конкретних АС в термінах ймовірностей, а також оцінки трудомісткості побудови СЗІ. Причому слід підкреслити, що запропонований формалізм базується на основі лише детального аналізу існуючих нормативних документів і досить загальних міркувань.

*Література: **1**. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - НД ТЗІ 2.5-004-99, ДСТСЗІ СБ України, Київ, 1999. **2**. Антонюк А. О. Про деякі важливі поняття захисту інформації в автоматизованих системах // Наукові записки НаУКМА. – 2002. – №2. – 8 с. **3**. Мельников В. В. Защита информации в компьютерных системах. - М.: Финансы и статистика, 1997.*

УДК 681.3

СПОСІБ ВИЯВЛЕННЯ ПРОНИКНЕННЯ ЛАЗЕРНОГО ВИПРОМІНЮВАННЯ У ВИДІЛЕНЕ ПРИМІЩЕННЯ

Віктор Гришко, Михайло Прокофьєв
НДЦ "ТЕЗІС" НТУУ "КПІ"

Анотація: **Проаналізовано конструкції пристрою для виявлення проникнення лазерного випромінювання через шибки виділеного приміщення. Надано рекомендації щодо вибору елементів конструкції для зменшення вірогідності витоку мовної інформації.**
Summary: **The theoretical analysis of a device's construction for revealing the exposure of laser penetration through the window-panes of the selected apartment was conducted. Some recommendations were also given as for choosing the elements of such construction for the aim of diminishing authenticity of linguistic information's flowing out through laser devices.**
Ключові слова: **Лазерне випромінювання, захист інформації.**

Захист акустичної (мовної) інформації є однією з найважливіших задач у загальному комплексі заходів щодо забезпечення безпеки об'єкту інформаційної діяльності (ОІД).

Для перехоплення мовної інформації може використовуватися широкий арсенал портативних технічних засобів розвідки, що дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, електроакустичному і оптико-електронному (акустооптичному) каналам.

Найефективнішими вважаються лазерні системи акустичної розвідки, які дозволяють відтворювати мову, будь-які інші звуки, акустичні шуми шляхом локаційного зондування лазерним променем шибок і інших поверхонь, що відбивають лазерний промінь. Розвідка може вестися з сусідніх будівель або автомашин, що можуть знаходитись на дорогах або автостоянках, прилеглих до будівлі.

На сьогоднішній день створено сімейство лазерних засобів акустичної розвідки. Як приклад можна привести систему SIPE LASER 3-DA SUPER [1]. Вона складається з джерела випромінювання (гелій-