ДОДАТОК А

Матеріали статей та тез

А.1 Стаття в Всеукраїнському міжвідомчому науково-технічному збірнику “Радіотехніка”

МЕТОД І МЕТОДИКА ФОРМАЛЬНОГО ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ

Нормативними документами (далі – НД) в сфері технічного захисту інформації (далі – ТЗІ) визначено сім ієрархічних критеріїв гарантій від Г-1 до Г-7 включно, які визначають ступінь впевненості в тому, що кожна з функціональних вимог безпеки здатна протистояти певним загрозам. НД ТЗІ 2.5-004.99 висуває вимоги до процесу проектування КСЗІ, де стиль формалізованої (частково формалізованої) специфікації є обов’язковим для отримання рівня гарантій Г-4 та вище.

На даний момент, не існує методик для формального проектування КСЗІ в інформаційно-телекомунікаційних системах (далі – ІТС).

Метою статті є аналіз існуючих мов формального опису системи, які в перспективі можуть використовуватися для проектування КСЗІ в ІТС та створення наукового підґрунтя для подальших досліджень в цій сфері.

Поняття формального проектування

Під терміном формалізованої специфікації слід розуміти таке представлення, яке базується на чітко визначених математичних концепціях. В свою чергу, математичні концепції визначають синтаксис і семантику подання, що дозволяє унеможливити неоднозначність розуміння моделі.

Процес проектування (або послідовність розробки) включає в себе модель політики безпеки та проект архітектури комплексу засобів захисту (далі – КЗЗ).

Методика формального проектування повинна включати:

- формалізоване моделювання політики безпеки;
- формалізований опис ІТС та процесів обробки інформації;
- алгоритм формування комплексу засобів захисту у ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації

Задача формального проектування

Основна задача формального проектування полягає у виборі методу формалізованого моделювання політики безпеки, методу формалізованого опису ІТС та процесів обробки інформації та формування алгоритму формування комплексу засобів захисту у ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації.

Вимоги при розробці формальних описів КСЗІ

Можна виділити такі основні вимоги щодо складу та подання проекту архітектури комплексу засобів захисту:

1) опис усіх базових апаратних, програмно-апаратних та/або програмних засобів, що реалізують комплекс заходів захисту (далі – КЗЗ) з визначенням функцій механізмів захисту;

2) визначення взаємозв'язків між всіма компонентами на рівнях зовнішніх інтерфейсів, підсистем, потоків даних, керування тощо;

3) опис порядку захищеного функціонування кожного компонента КЗЗ – опис будь-яких операцій функціонального компонента КЗЗ, дії якого можуть спричинити зміну захищеного стану об'єкту, у вигляді послідовності дій, які виконуються в кожній підсистемі КЗЗ, як результат впливу на відповідний інтерфейс;

4) опис використовуваних зовнішніх послуг безпеки, що не входять до складу КЗЗ.

Для подання проекту архітектури у формалізованому вигляді (для заявлених рівнів гарантій Г-6 або Г-7), опис порядку захищеного функціонування компонентів КЗЗ має бути викладений згідно з попередньо-визначеними математичними поняттями. Пояснення математичних понять та використана нотація мають бути описані в неформалізованому вигляді. Мають бути визначені критичні властивості безпеки та виконувані над ними операції.

Для перевірки відповідності проекту архітектури та моделлю політики безпеки необхідно формально довести відповідність між захищеним функціонуванням компонентами КЗЗ та правилами політик реалізованих функціональних послуг безпеки (далі – ФПБ).

Критерії методів формалізованого моделювання політики безпеки

Критерії для методу формалізованого моделювання політики безпеки:

- складність реалізації моделі політики безпеки;
- наявність інструментальної підтримки.

Критерії методу формалізованого опису ІТС та процесів обробки інформації

Для проектування систем використовують різні мови, різні підходи, тому необхідно ввести критерії та показники для відбору найкращих кандидатів з ухилом на опис процесів безпеки та виконання вимог НД ТЗІ. Пропонується наступний перелік:

1) Складність. Показник складності характеризує, в першу чергу, здатність до адекватного опису потрібного параметру чи операції. Необхідність введення показника зумовлена тим, що при оцінюванні коректності реалізації рівня гарантій експерт може неправильно зрозуміти формальну модель, її формалізований вигляд або ж математичні концепції.

2) Орієнтованість на опис процесів обробки інформації. Під процесами обробки інформації найкраще тлумачення можна надати з [1] – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

3) Орієнтованість на опис процесів безпеки. Опис процесів безпеки можна поділити на чотири типи:

- конфіденційності;
- цілісності;
- доступності;
- спостереженості.

Кожна з чотирьох властивостей забезпечує захист від певної множини загроз.

4) Наявність інструментальної підтримки. Наявність готових програмних пакетів значно спрощує та прискорює процес розробки методики формального проектування. З іншого боку, готові інструменти для роботи можуть бути застарілі на даний момент, не підтримуватися розробниками чи багато коштувати.

Вибір методу формалізованого моделювання політики безпеки

Існують наступні методи формалізованого моделювання політики безпеки:

- UMLSec;
- Ponder2.

При виборі методу формалізованого моделювання політики безпеки далі наведено властивості методів UMLsec, Ponder2 та надано їх порівняльну характеристику за визначеними вище критеріями.

Проектування з використанням нотації UMLsec

Основа ідея UMLsec – розширення існуючої моделі UMLsec, шляхом додавання спеціальних міток – стереотипів, які додають відомості щодо безпеки. Відомості можуть бути наступного типу [3]:

- припущення щодо безпеки на фізичному рівні, наприклад як стереотип $||Internet||$;
- вимоги щодо безпеки на логічному рівні системи, наприклад як стереотип $||secrecy||$ (конфіденційність);
- вимоги політики безпеки, які накладаються на систему, наприклад як стереотипи $||secure\ links||$ (захищені зв'язки), $||no\ down\ flow||$ (керування потоком) .

Стереотип визначає новий тип елементів моделювання, розширюючи семантику вже існуючого типу або класу в моделі UML. Нотація стереотипу складається з імені стереотипу, взяті в подвійні прямі дужки || ||. Перелік стереотипів UMLsec наведено в Таблиці 1.

Таблиця 1

Стереотип	Базовий клас	Тег	Обмеження	Опис
fair exchange	subsystem	start, stop, adversary	Після старту з часом досягне зупинки	Реалізація чесного обміну
provable	subsystem	action, cert, adversary	Незаперечна дія	Вимоги до відмов
rbac	subsystem	protected, role, right	Виконується тільки для дозволених дій	Реалізація контролю доступу на основі ролей
Internet	link			Інтернет
encrypted	link			Зашифроване з'єднання
LAN	link, node			Локальна мережа
wire	link			кабель
smart card	node			Вузол смарт карти
POS device	node			POS-термінал
issuer node	node			Вузол постачальника
secrecy	dependency			Конфіденційність
integrity	dependency			Цілісність
high	dependency			Висока чутливість
critical	object, subsystem	Secrecy, integrity, authenticity, high, fresh		Критичний об'єкт
secure links	subsystem	adversary	Безпека залежностей відповідає посиланням «call», «send» відносно безпеки даних	Реалізація захищених ліній зв'язку
secure dependency	subsystem			Структурна взаємодія безпеки даних
data security	subsystem	adversary, integrity, authenticity	Забезпечує конфіденційність, цілісніть, автентичність,	Базові вимоги до безпеки даних

			свіжість (новизна)	
no-down flow	subsystem	(data, origin)		Стан потоку інформації
no-up flow	subsystem	object name		Стан потоку інформації
guarded access	subsystem		Доступ до захищених об'єктів через механізми захисту	Контроль доступу з використанням захищених об'єктів
guarded	object	guard		Захищений об'єкт

Розширити модель можна значенням тегів елементу моделі. Теги можуть розширити можливості при описі властивостей даних. Перелік тегів UMLsec наведено в Таблиці 2.

Таблиця 2

Тег	Стереотип	Тип	Опис
start	fair exchange	state	Стан старту
stop	fair exchange	state	Стан зупинки
adversary	fair exchange	adversary model	Тип порушника
action	provable	state	Операція/дія, що потребує підтвердження
cert	provable	expression	Сертифікат
adversary	provable	adversary model	Тип порушника
protected	rbac	state	Захищені ресурси
role	rbac	(actor, role)	Призначення ролі
right	rbac	(role, right)	Призначення прав до ролі
secrecy	critical	data	Конфіденційність даних
integrity	critical	(variable, expression)	Цілісність даних
authenticity	critical	(data, origin)	Автентичність даних
high	critical	message	Повідомлення високого рівня
fresh	critical	data	Нові дані
adversary	secure links	adversary model	Тип порушника
adversary	data security	adversary model	Тип порушника
integrity	data security	(variable, expression)	Цілісність даних
authenticity	data security	(data, origin)	Автентичність даних
guard	guarded	object name	Захищений об'єкт

Таким чином, використання нотації UMLsec дозволяє доповнити вже існуючу модель UML за допомогою надбудов безпеки. До реалізованих в UML нотацій, додаються параметри безпеки, які дозволяють реалізувати вимоги політики безпеки та встановити відповідність між проектом архітектури та моделлю політики безпеки.

Використання нотацій Ponder2

Ponder2 поєднує в собі розподілену систему управління об'єктами загального призначення із службою домену, інтерпретатора зобов'язальної політики, інтерпретатора команд та застосування дотримання авторизації.

Ponder2 – це назва мови специфікації політики. Розробниками мови було розроблено набір інструментів та послуг для специфікації, аналізу та забезпечення застосування політик. Таким чином, Ponder – не тільки мова, а й набір інструментів.

Мова Ponder2 забезпечує загальний засіб визначення політик безпеки, які відображаються на різних механізмах реалізації контролю доступу для брандмауерів, операційних систем, баз даних тощо. Підтримується, в першу чергу, два типи політик: політики авторизації, що визначають, які дії дозволені за певних обставин та політики зобов'язань, що визначають, які дії слід виконувати у відповідь на подію, що відбувається, при виконанні конкретних умов.

Ponder2 визначає політики у форматі "предмет-дія-ціль" (subject-action-target, SAT). Ponder2 надає два типи політики авторизації, а саме позитивну авторизацію auth + та негативну авторизацію auth-. У Ponder2 зазначено лише один тип політики зобов'язань, в якому зазначено, що суб'єкт зобов'язаний виконати певні дії щодо цієї цілі. Політика зобов'язань може бути застосована лише за умови, що відповідна політика авторизації була вказана в системі. Поле події визначає активатор зобов'язання. Необов'язкові обмеження можуть застосовуватися до обох типів політик. Ці обмеження оцінюються щодо стану системи.

Порівняння методів формалізованого моделювання політики безпеки

1) Порівняння методів формалізованого моделювання політики безпеки виконано за двома основними критеріями – наявність програмного забезпечення методу розробки та складність реалізації:UMLsec та Ponder мають в своєму складі готове програмне забезпечення для розробки;

2) реалізація вимог політики безпеки, які будуть засновані на логіці методу Ponder2, не є інтуїтивно-зрозумілими і, як наслідок, їх не легко відобразити механізмами мови. В свою чергу, UMLsec використовує базові механізми з відомого методу UML, що робить UMLsec більш привабливим методом формалізованого моделювання політики безпеки.

Отже, за критерієм складності UMLsec був обраний, як метод для формалізованого моделювання політики безпеки, бо має більш зрозумілу та чітку нотацію.

Вибір методу формалізованого опису ІТС та процесів обробки інформації

Існує один промислово розповсюджений метод опису – UML. Інформаційна система в моделі UML зображується за допомогою основних елементів – компонентів, інтерфейсів та залежностей між ними. Формалізований опис ІТС подається у вигляді діаграми компонентів UML.

Діаграми UML доволі прості для розуміння після ознайомлення з його синтаксисом. Також існує можливість додавати власні текстові та графічні стереотипи, що значно розширює можливості застосування UML.

Завдяки розповсюдженості методу існує багато програмних середовищ для розробки UML-діаграм.

Алгоритм формування КЗЗ в ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації

Вхідні дані алгоритму:

- діаграма компонентів UML (формалізований опис ІТС та процесів обробки інформації);
- формальний опис політики безпеки.

Діаграмою компонентів UML визначено вузли та інтерфейси системи. Усі інтерфейси кожного вузла перевіряються та висуваються необхідні вимоги політики безпеки. Проект архітектури КЗЗ, в підсумку, містить усі інтерфейси, правила їх взаємодії та вимоги політики безпеки.

Висновки

В ході проведення досліджень була запропонована методика формального проектування КСЗІ в ІТС, що включає в себе формальний опис ІТС та процесів обробки інформації, формальну модель політики безпеки та алгоритм формування комплексу засобів захисту в ІТС.

Були обрані метод формального опису ІТС та метод формального опису моделі політики безпеки, що можуть бути застосовані в алгоритмі формування КЗЗ в ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації.

Список літератури:

1. J. J¨urjens Secure Systems Development with UML. Springer – Verlag, 2005.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. 61с.

А.2 Тези восьмої міжнародної науково-технічної конференції «Проблеми інформатизації»

Секція 2

Метод і методика формального проектування КСЗІ в ІТС

Гвоздьов Р.Ю., Заболотний В.І.

Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком інформаційних технологій, наданням електронних послуг, в країні проектуються та вводяться в експлуатацію все більше інформаційних систем, до яких висуваються вимоги до захисту інформації. Одним із шляхів для задовільнення вимог до безпеки таких систем є побудова комплексної системи захисту інформації (далі – КСЗІ).

Нормативними документами в сфері технічного захисту інформації визначено сім ієрархічних критеріїв гарантій від Г-1 до Г-7 включно, які визначають ступінь впевненості в тому, що кожна з функціональних вимог безпеки здатна протистояти певним загрозам. НД ТЗІ 2.5-004.99 висуває вимоги до процесу проектування КСЗІ, де стиль формалізованої (частково формалізованої) специфікації є обов'язковим для отримання рівня гарантій Г-4 та вище.

На даний момент, не існує методик для формального проектування КСЗІ в інформаційно-телекомунікаційних системах (далі – ІТС).

Процес проектування включає в себе модель політики безпеки та проект архітектури комплексу засобів захисту. Основна задача формального проектування полягає у виборі методу формалізованого моделювання політики безпеки, методу формалізованого опису ІТС та процесів обробки інформації та формування комплексу засобів захисту у ІТС з формальної моделі політики безпеки та з формалізованого опису ІТС та процесів обробки інформації.

Метою доповіді є аналіз існуючих мов формального опису системи, які в перспективі можуть використовуватися для проектування КСЗІ в ІТС та створення наукового підґрунтя для подальших досліджень в цій сфері.

Список літератури

1. НД ТЗІ 2.5-004.99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
3. НД ТЗІ 2.7-010-09. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

№ док.	Позначення	Найменування	Дод. відом.
1		Текстові документи	
	ГЮІК.ХХХХХ1412Ст.4ПЗ	Пояснювальна записка	84 с.
2		Графічні документи	
		Презентаційний матеріал	11 А4.
3		Інші документи	
		Відзив керівника	1 с.
		Рецензія	1 с.

					ГЮІК. ХХХХХ1412Ст.4ВД	
Изм.	Лист	№ докум.	Підпис	Дата		
Розроб.		Гвоздьов Р.Ю.			Методика формального проектування КСЗІ в інформаційно-телекомунікаційних системах	Лит. Т / Лист 1 / Листів 1
Перевір.		Олійников Р.В.				
						ХНУРЕ Кафедра БІТ
Н.контр.		Конєва Н.Ф.				
Затверд.		Халімов Г.З.				