УДК 004.056

Пфо О.М.
Кіровоградський національний технічний університет

Основні проблеми теорії захисту інформації

Захист інформації – галузь знань, яка має відповідну теорію, що складає її фундаментальне підґрунтя. Теорія захисту інформації – це наука про загальні принципи та методи побудови захищених інформаційно-комунікаційних систем.

Теорія захисту інформації – природнича наука, яка має відповідні аксіоматику, понятійний та формальний апарат. Основним методологічним інструментом теорії захисту інформації, яка оперує складними системами, є методи системного аналізу для вивчення систем і теорії прийняття рішень для розв'язання задач синтезу систем захисту інформації. Всі положення теорії захисту інформації мають базуватися на доказовому підході та відповідати вимогам несуперечності, повноти і розв'язаності.

Несуперечність– властивість теорії, коли перетворення формул не ведуть до виникнення двох і більше результатів, які спростовують один одне. Повнота– властивість теорії, в якій не виникають твердження, що не вдається ні довести ані спростувати. Розв'язаність– властивість теорії, в якій існує єдиний механізм (алгоритм) для визначення істинності або фальшивості будь якого твердження в цієї теорії.

На поточний час в теорії захисту інформації використовуються два підходи для аналізу та синтезу систем безпеки – формальний та неформальний (описовий).

Традиційно формальний підхід теорії захисту інформації складають етапи визначення сукупності політики безпеки, критерію безпеки та моделі безпеки ІКС у формальному вигляді. Важливим етапом формального підходу є проведення доказу відповідності системи безпеки критерію безпеки при дотриманні встановлених правил та обмежень. За умови виконання останнього етапу у теорії захисту інформації говорять про "гарантованість" захисту інформації. Зазначимо, що у теорії захисту інформації також існують розділи, які не оперують поняттям гарантованості таки як методи оптимального проектування систем захисту інформації, аналіз ризиків, моделювання окремих процесів захисту та інші.

На поточний час найбільш розвинутими формальними розділами теорії захисту інформації є математичні методи криптографії та моделювання політик безпеки. Сучасний формальний базис теорії захисту інформації у великої мірі сформувався під впливом криптографії, яка почала сформуватись значно раніше. Формальний підхід теорії захисту інформації знаходиться у стадії становлення і не може задовольнити всіх завдань, які виникають при дослідженні та створенні систем захисту інформації. Тому, цій підхід доповнюється традиційним неформальним (описовим) підходом.

Неформальний (описовий) підхід теорії захисту інформації носить характер опису методів і механізмів, які використовуються для захисту інформації в автоматизованих системах.

Цій підхід використовується у випадку, якщо формальні методи з будь-яких причин не можуть бути використані при аналізі і синтезі систем захисту інформації, чи взагалі не розроблені.

Треба зазначити, що теорія захисту інформації до цього часу залишається відносно замкнутою науковою дисципліною у частині розробки та впровадження формальних методів. Розвиток цих методів не завжди є синхронізованим із досягненнями як класичних, так і

сучасних наук. Цим пояснюється дуже розповсюджені ілюзії користувачів інформаційних технологій про те, що якість захисту інформації визначається виключно кількістю і надійністю механізмів захисту, а формальний підхід мало що дає.

Теорія захисту інформації як наука, що знаходиться на стадії розвитку, зіткнулась з колом проблем. Частина з цих проблем вже є розв'язаною, інші очікують розв'язання. Розглянемо декілька базових проблем теорії захисту інформації, які на поточний час розв'язані.

Важливою проблемою теорії захисту інформації є проблема складності задачі вивчення (аналізу) систем захисту інформації. У сучасній теорії захисту інформації цю проблему розв'язують, застосовуючи метод ієрархічної декомпозиції складних систем. З використанням цього методу, загальну складну систему розкладають на низьку рівнів ієрархії. При цьому, верхній рівень ієрархії складає політика безпеки, другий рівень – системи підтримки політики безпеки, третій рівень – механізми захисту, четвертий рівень – реалізація механізмів безпеки. Вивчення цих підсистем проводять із застосуванням специфічних для кожного рівня ієрархії методів аналізу.

Наступною проблемою теорії захисту інформації є проблема побудови (синтезу) "гарантовано захищеної системи". Проблема полягає у протиріччі між вимогами до гарантованості і принциповою неможливістю побудувати "гарантовано захищену систему" у класі відкритих систем. В теорії відкритих систем проблему гарантованої безпеки відносять до алгоритмічно нерозв'язних проблем.

Алгоритмічно нерозв'язною проблемою є клас задач, для якого не можна запропонувати ніякого єдиного алгоритму, який розв'язував би усі задачі з указаного класу.

Доказове обґрунтування відсутності гарантованої безпеки у відкритих системах надає, наприклад, теорема про неможливість розв'язати задачу забезпечення безпеки довільної системи у загальному випадку за умови загального завдання на доступ, сформульована в роботі М. Харрісона, В. Руззо, Дж. Ульмана. Рішення цієї проблеми проводиться шляхом декомпозиції загальної вихідної проблеми гарантованого захисту інформації у комп'ютерних системах на сукупність двох задач. Перша з цих задач полягає у коректному формулюванні політики безпеки, а друга – у побудові (синтезі) системи захисту інформації, яка гарантовано підтримує політику безпеки.

Наведені вище підходи до розв'язання проблем аналізу і синтезу систем захисту інформації вперше були впроваджені у Критеріях оцінки захищених комп'ютерних систем Міністерства оборони США (англ. – TrustedComputerSystemEvaluationCriteria,TCSEC), відомих також як "Оранжева книга", у 80-х роках минулого сторіччя та складають теоретичний базис багатьох сучасних стандартів захисту інформації.

На закінчення хотілося б підкреслити, що ніякі апаратні, програмні і будь-які інші рішення не зможуть гарантувати абсолютну надійність і безпеку даних в комп'ютерних мережах. У той же час звести ризик втрат до мінімуму можливо лише при комплексному підході до питань безпеки

Список використаних джерел

1. *Уфимцев А. С. Методика информационной безопасности / А. С. Уфимцев. — М. : Экзамен, 2004. — 544 с. 2. Щеглов А. Ю.*
2. *Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. — СПб: Наука и техника, 2004. — 384 с. 3. Гайворонський М. В.*
3. *Безпека інформаційно-комунікаційних систем / М. В.Гайворонський. — К. : Видавнича група BHV, 2008. — 608 с.*