На базе предложенной ФПАС ДП-модели КС также построена ДП-модель сетевых дискреционных КС с уязвимостями (СДУ ДП-модель). В ней предполагается, что нарушители могут использовать различные уязвимости (ошибки в системных и прикладных процессах, доверие, доступ к паролям, раскрытие параметров КС), позволяющие получать контроль над субъектами КС, в том числе и доверенными. В рамках построенной СДУ ДП-модели формализованы основные требования по тестированию возможности проникновения семейства к доверию «Анализ уязвимостей» руководящего документа ФСТЭК «Критерии оценки безопасности информационных технологий», а именно: формально описаны модели нарушителя (нарушителя с низким, умеренным и высоким потенциалом нападения) и дано математическое определение стойкости КС к проникновению. Рассмотрены также существующие подходы к построению потенциально возможных путей нарушения безопасности сетевых КС с дискреционным управлением доступом при компьютерном моделировании их безопасности и показано, каким образом в этих подходах может быть применена СДУ ДП-модель.

Таким образом, для теоретического анализа безопасности современных КС с дискреционным управлением доступом с функционально или параметрически ассоциированными сущностями разработана математическая модель, которая может быть использована и уже используется другими учёными [4] в дальнейших исследованиях по теории компьютерной безопасности, а также для формального анализа уязвимостей и моделирования политик управления доступом и информационными потоками в КС с дискреционным управлением доступом с высоким уровнем доверия к их безопасности и для разработки методов управления, администрирования и настройки параметров КС, позволяющих обеспечить защиту от нарушения их безопасности.

ЛИТЕРАТУРА

1. ФСТЭК России. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации. М., 2004.
2. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Ч. 1–3. М., 2002.
3. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
4. *Буренин П. В.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. 2009. №1(3). С. 93–113.

УДК 004.56(06)

МНОГОЗНАЧНАЯ ЛОГИКА В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ НА ПРЕДПРИЯТИИ

М. М. Кучеров, А. А. Кытманов

В современной логике предложения иногда считаются не истинными и не ложными. Эта идея восходит еще к Аристотелю, который высказывался относительно будущего, в частности о не вполне определенных событиях, и реализована в системах многозначной логики. Существует также и «дуальная» идея, состоящая в том, что некоторые предложения могут рассматриваться как имеющие одновременно оба истинностных значения. Этот взгляд также имеет многочисленные плодотворные применения в информатике.

В управлении информационной безопасностью информация часто поступает из разных противоречивых источников, и в этом случае дедуктивное рассуждение может привести к скрытым несогласованностям. Существующие подходы составления политики безопасности с учетом неопределенности обычно разрабатываются для конкретного случая. Теория решеток и многозначная логика могут быть рассмотрены как структура, на которой может быть основана система контроля целостности на предприятии.

Наиболее простая 4-значная логика для выражения практических дедуктивных процессов имеет четыре истинностных значения «T, F, Both, None». Смысл этих значений описывается следующим образом:

— предложение считается только истинным (T);
— предложение считается только ложным (F);
— предложение считается одновременно как истинным, так и ложным (Both);
— статус предложения — неопределенный (ни истина, ни ложь) (None).

Любая двойная решетка может рассматриваться как структура, которая представляет уровни двух основных свойств, являющихся наиболее существенными для ее элементов. Наиболее фундаментальным свойством является свойство информированности. Чем больше элементов включает подмножество, тем больше информации в нем содержится. Вторым фундаментальным свойством качественной информации является конфиденциальность. Каждый элемент двойной решетки имеет каждое из этих двух свойств в определенной степени. И два частичных порядка — $\leqslant_i$ и $\leqslant_s$ — «организуют» элементы согласно обладаемой степени информированности и конфиденциальности соответственно.

В подходе, основанном на использовании одного уровня для целостности и для конфиденциальности, уровень секретности обрабатывается в соответствии с моделью Белла и Лападулы, но при этом обеспечивается также контроль целостности. Закон Гроша говорит о том, что компьютерная экономика прямо связана со скоростью вычислений, что возможно только при условии размещения на нижней ступени иерархии безопасности субъектов и объектов с высокой целостностью. В этом случае обобщенное истинностное пространство имеет в качестве базы множество $I = \langle T, F, t, f \rangle$, которое содержит следующие истинностные значения:

— T — высокий уровень секретности;
— F — низкий уровень секретности;
— t — объект допускает изменения, низкий уровень целостности;
— f — объект не допускает изменений, высокий уровень целостности.

Множество подмножеств I дает до 16 обобщенных истинностных значений. Пустая мультиоценка обозначается как N, и A представляет множество, которое содержит все начальные истинностные значения T, F, t, f:

$$P(I) = \{\{\}, \{T\}, \{F\}, \{t\}, \{f\}, \{T, F\}, \{T, t\}, \{T, f\}, \{F, t\}, \{F, f\}, \{t, f\},$$

$$\{T, F, t\}, \{T, F, f\}, \{T, t, f\}, \{F, t, f\}, \{T, F, t, f\}\}.$$

Каждая метка классификации, комбинируя субъективное и объективное значения, приписывает каждому результирующему обобщенному значению не только некоторый уровень информированности, конфиденциальности и целостности, но также определенную семантику. Это означает, что мы получаем новое частичное упорядочение —

$\leqslant_f$, которое представляет рост (или убывание) субъективной оценки, т. е. основанной на качестве самого сообщения, между элементами $P(I)$. Это новое частичное упорядочение также дает полную решетку, и таким образом можно ввести понятие тройной решетки.

Определение тройной решетки находится в согласии с определением двойной решетки как множества с двумя частичными порядками, каждый из которых формирует решетку на этом множестве, т. е. генерируя собственные операторы пересечения и объединения, а также унарные операторы инверсии.

Грани, относящиеся к трем частичным порядкам, показаны в табл. 1.

Таблица 1

Грани, относящиеся к трем частичным порядкам

Относительный порядок	Грани	Наибольшие и наименьшие элементы в $P(I)$
$\leqslant_k$	A, N	Информационные
$\leqslant_s$	Tt, Ff	Конфиденциальные
$\leqslant_f$	TF, tf	Объективности

Полученная решетка имеет пять информационных уровней, пять уровней конфиденциальности и пять уровней объективной оценки, показанных в табл. 2.

Таблица 2

Уровни информированности, секретности и объективности

	Информированность	Секретность	Объективная оценка
1	N	Ff	TF
2	T, F, t, f	F, f, TFf, Ftf	T, F, TFt, TFf
3	TF, Tf, Tt, Ff, Ft, tf	A, TF, Tf, Ft, tf, N	A, Tt, Tf, Ft, Ff, N
4	TFf, TFt, Ttf, Ftf	T, t, TFt, Ttf	t, f, Ttf, Ftf
5	A	Tt	tf

На практике это позволяет разместить важные системные файлы в нижней части иерархии модели Белла и Лападулы. За счет правила «нет записи вниз» осуществляется защита целостности от троянских коней. Указанный подход можно использовать при разграничении доступа для составных субъектов и объектов, а также для разработки общей политики безопасности системы, составленной из отдельных политик безопасности для ее подмножеств.

УДК 519.8

АНАЛИЗ ЗАЩИЩЕННОСТИ СЕТИ С ИСПОЛЬЗОВАНИЕМ ЦЕПЕЙ МАРКОВА

В. П. Кушнир, И. Н. Кирко

Входными параметрами информационных систем являются информационные потоки, контролируемые техническими, программными и организационными средствами. Результаты анализа прохождения информационных потоков по телекоммуника-