УДК 512.563.3

А.А. Воробьев

Алгебраические методы исследования таксономий уязвимостей вычислительных сетей и компьютерных систем

Предложена алгебраическая структура для таксономий на основе концепции измерений. Доказано, что полученная структура является булевой алгеброй, что позволяет использовать при исследовании классификаций уязвимостей аппарат булевых алгебр.

Ключевые слова: булева алгебра, уязвимость, защита информации, таксономия.

Таксономия уязвимостей вычислительных сетей и компьютерных систем

Количество сетевых и компьютерных атак неуклонно растет с каждым годом, приводя к появлению новых уязвимостей в информационных системах. Любой компьютер, подключенный к сети общего пользования Интернет, находится под угрозой вирусов, компьютерных червей и хакерских атак. Доказательством данного факта являются постоянные атаки на пользователей вычислительных устройств. Исходя из данных Computer Emergency Response Team (CERT, рис. 1), количество обнаруженных уязвимостей с 1995 по 2007 г. возросло со 137 до 44,074 тыс.

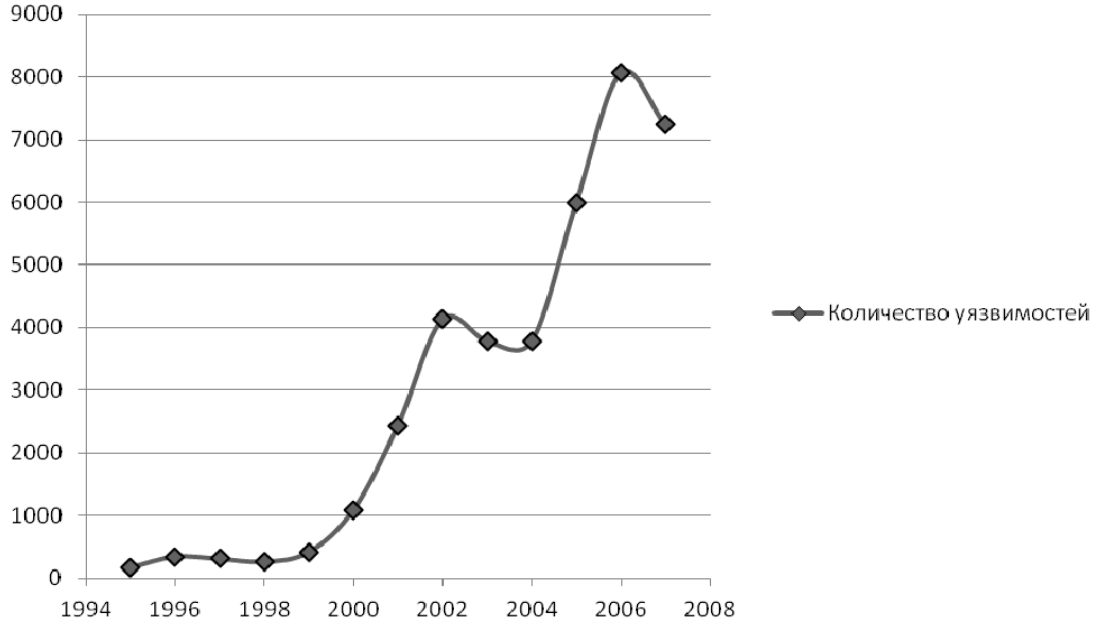

Рис. 1. Количество обнаруженных уязвимостей в зависимости от года

Отмечено было не только повышение количества обнаруженных уязвимостей, а также их сложность и изощренность. Но, с другой стороны, сегодня множество реализаций атак на уязвимости являются относительно «дружественными пользователю», и глубоких технических знаний для проведения атаки не требуется. Более детально данная тема раскрывается в специальном отчете CERT/CC Г.Ф. Липсона [1].

Цель таксономии в создании универсальной и последовательной классификации уязвимостей. На сегодняшний момент, уязвимости по-разному описываются разными организациями, что приводит к недопониманию сути рассматриваемой уязвимости. В работах [2, 3] рассмотрены различные виды таксономий, их недостатки и преимущества, а также сформулирован новый подход к созданию таксономий на основе концепции измерений, при котором классы характеристик уязвимостей располагаются на осях многомерного пространства. Концепция измерений при классификации уязвимостей становится все более популярной, что требует разработки обобщенных математических моделей и методов исследования «пространственных таксономий» вместо локально применимых к конкретным реализациям таксономий.

Построение алгебры уязвимостей

С целью построения обобщенного математического аппарата исследования уязвимостей вычислительных сетей и компьютерных систем с таксономией на основе концепции измерений [1] была поставлена задача о разработке алгебры уязвимостей.

Пусть $\{X_i\}$ – конечное семейство классов характеристик уязвимостей, откладываемых на координатных осях некоторого пространства $G, i \in [1;n], n \in N$. Известно, что $|X_i| = m_i$. Некоторая произвольная уязвимость $a \in G$ описывается как совокупность

$$a = \{\alpha_1, \alpha_2, ..., \alpha_n\}, \alpha_i \subseteq X_i. \quad (1)$$

Введем две операции сложения и умножения соответственно на множестве G.

Сложение: $\forall a \in G \forall b \in G : a \oplus b = \left\{\alpha_1^{(a)} \cup \alpha_1^{(b)}, \alpha_2^{(a)} \cup \alpha_2^{(b)}, ..., \alpha_n^{(a)} \cup \alpha_n^{(b)}\right\}$.

Умножение: $\forall a \in G \forall b \in G : a \otimes b = \left\{\alpha_1^{(a)} \cap \alpha_1^{(b)}, \alpha_2^{(a)} \cap \alpha_2^{(b)}, ..., \alpha_n^{(a)} \cap \alpha_n^{(b)}\right\}$.

Тогда пространство G является декартовым произведением множеств всех подмножеств классов характеристик

$$G = 2^{X_1} \times 2^{X_2} \times ... \times 2^{X_n}.$$

Докажем некоторые свойства введенных операций.

1. Идемпотентность. $\forall a \in G$ выполнимо

$$a \oplus a = \left\{\alpha_1^{(a)} \cup \alpha_1^{(a)}, \alpha_2^{(a)} \cup \alpha_2^{(a)}, ..., \alpha_n^{(a)} \cup \alpha_n^{(a)}\right\} = a,$$

$$a \otimes a = \left\{\alpha_1^{(a)} \cap \alpha_1^{(a)}, \alpha_2^{(a)} \cap \alpha_2^{(a)}, ..., \alpha_n^{(a)} \cap \alpha_n^{(a)}\right\} = a.$$

2. Коммутативность. $\forall a \in G \forall b \in G$ выполнимо

$$a \oplus b = \left\{\alpha_1^{(a)} \cup \alpha_1^{(b)}, ..., \alpha_n^{(a)} \cup \alpha_n^{(b)}\right\} = \left\{\alpha_1^{(b)} \cup \alpha_1^{(a)}, ..., \alpha_n^{(b)} \cup \alpha_n^{(a)}\right\} = b \oplus a,$$

$$a \otimes b = \left\{\alpha_1^{(a)} \cap \alpha_1^{(b)}, ..., \alpha_n^{(a)} \cap \alpha_n^{(b)}\right\} = \left\{\alpha_1^{(b)} \cap \alpha_1^{(a)}, ..., \alpha_n^{(b)} \cap \alpha_n^{(a)}\right\} = b \otimes a.$$

3. Ассоциативность. $\forall a \in G \forall b \in G \forall c \in G$ выполнимо

$$(a \oplus b) \oplus c = \left\{\left(\alpha_1^{(a)} \cup \alpha_1^{(b)}\right) \cup \alpha_1^{(c)}, ..., \left(\alpha_n^{(a)} \cup \alpha_n^{(b)}\right) \cup \alpha_n^{(c)}\right\} =$$

$$= \left\{\alpha_1^{(a)} \cup \left(\alpha_1^{(b)} \cup \alpha_1^{(c)}\right), ..., \alpha_n^{(a)} \cup \left(\alpha_n^{(b)} \cup \alpha_n^{(c)}\right)\right\} = a \oplus (b \oplus c),$$

$$(a \otimes b) \otimes c = \left\{\left(\alpha_1^{(a)} \cap \alpha_1^{(b)}\right) \cap \alpha_1^{(c)}, ..., \left(\alpha_n^{(a)} \cap \alpha_n^{(b)}\right) \cap \alpha_n^{(c)}\right\} =$$

$$= \left\{\alpha_1^{(a)} \cap \left(\alpha_1^{(b)} \cap \alpha_1^{(c)}\right), ..., \alpha_n^{(a)} \cap \left(\alpha_n^{(b)} \cap \alpha_n^{(c)}\right)\right\} = a \otimes (b \otimes c).$$

4. Поглощение. $\forall a \in G \forall b \in G$ выполнимо

$$(a \otimes b) \oplus a = \left\{\left(\alpha_1^{(a)} \cap \alpha_1^{(b)}\right) \cup \alpha_1^{(a)}, ..., \left(\alpha_n^{(a)} \cap \alpha_n^{(b)}\right) \cup \alpha_n^{(a)}\right\} = \left\{\alpha_1^{(a)}, ..., \alpha_n^{(a)}\right\} = a,$$

$$(a \oplus b) \otimes a = \left\{\left(\alpha_1^{(a)} \cup \alpha_1^{(b)}\right) \cap \alpha_1^{(a)}, ..., \left(\alpha_n^{(a)} \cup \alpha_n^{(b)}\right) \cap \alpha_n^{(a)}\right\} = \left\{\alpha_1^{(a)}, ..., \alpha_n^{(a)}\right\} = a.$$

5. Дистрибутивность. Очевидно исходя из доказательств свойств ассоциативности и поглощения.

Исходя из построения множества G, введенных операций сложения и умножения, для которых выполняются свойства 1–5, совокупность $\langle G, \oplus, \otimes \rangle$ – дистрибутивная решетка [4].

Рассмотрим элемент из $0_G \in G$, такой, что

$$0_G = \{\varnothing, \varnothing, ..., \varnothing\}_n.$$

Так как $\forall i \in [1;n], \varnothing \in 2^{X_i} \xrightarrow{def} \forall g \in 2^{X_i} : g \cap \varnothing = \varnothing$, то $\forall a \in G : 0_G \otimes a = 0_G$. Таким образом, элемент 0_G является нижней гранью дистрибутивной решетки $\langle G, \oplus, \otimes \rangle$.

Рассмотрим элемент из $1_G \in G$, такой, что

$$1_G = \{X_1, X_2, ..., X_n\}.$$

Так как $\forall i \in [1;n], X_i \in 2^{X_i} \xrightarrow{def} \forall g \in 2^{X_i} : g \cup X_i = X_i$, то $\forall a \in G : 1_G \oplus a = 1_G$. Таким образом, элемент 1_G является верхней гранью дистрибутивной решетки $\langle G, \oplus, \otimes \rangle$.

Отсюда следует, что совокупность $\langle G, \oplus, \otimes, 0_G, 1_G \rangle$ является дистрибутивной ограниченной решеткой.

Рассмотрим некоторый элемент a дистрибутивной ограниченной решетки $\langle G, \oplus, \otimes, 0_G, 1_G \rangle$. Дополнением $^{-}$ к элементу a назовем элемент $\overline{a}$, такой, что

$$\overline{a} = \{\overline{\alpha_1}, \overline{\alpha_2}, ..., \overline{\alpha_n}\},$$

где $\alpha_i \in X_i$. Очевидно, что $a \otimes \overline{a} = 0_G, a \oplus \overline{a} = 1_G$.

Так как по теореме о свойствах дополнения в ограниченной дистрибутивной решетке [5] $\forall a \in G \exists! \overline{a}$ – дополнение к a, значит, $\langle G, \oplus, \otimes, 0_G, 1_G, \overline{\ } \rangle$ – булева алгебра.

Данный факт позволяет использовать алгебраические методы исследования таксономий уязвимостей, представленных в виде классов характеристик на осях некоторого многомерного пространства.

Заключение

На основе проведенных исследований возможно сделать следующие выводы:

1. Предложена алгебраическая система $\langle G, \oplus, \otimes, 0_G, 1_G, \overline{\ } \rangle$.

2. Доказано, что $\langle G, \oplus, \otimes, 0_G, 1_G, \overline{\ } \rangle$ является булевой алгеброй, что позволяет использовать аппарат булевых алгебр.

3. При дальнейшем исследовании возможно построить связь данной булевой алгебры с теорией меры и теорией вероятностей.

Литература

1. Lipson H.F. Tracking and tracing cyber attacks: technical challenges and global policy issues – November 2002 [Электронный ресурс]. – Режим доступа: www.cert.org/archive/pdf/02sr009.pdf, свободный (дата обращения: 26.03.2012).

2. Garshva E. Computer System Attack Classification / E. Garshva, N. Paulauskas // Electronics and Electrical Engineering. – Kaunas: Technology, 2006. – № 2 (66). – P. 84–87.

3. Hansman S. A taxonomy of network and computer attacks / S. Hansman, R. Hunt // Computer & Security. – 2005. – Vol. 24, issue 1. – P. 31–43.

4. Новиков Ф.А. Дискретная математика для программистов / Ф.А. Новиков. – 2-е изд. – СПб.: Питер, 2006. – 364 с.

5. Владимиров Д.А. Булевы алгебры. – М.: Наука, 1969. – 320 с.

Воробьев Антон Александрович
Аспирант каф. информационной безопасности автоматизированных систем Комсомольский-на-Амуре государственный технический университет
Тел.: 8 (909) 845-58-72
Эл. почта: zeromem@mail.ru

Vorobyov A.A.

Algebraic methods of analysis taxonomies of vulnerabilities of computer networks and systems

We propose an algebraic structure for taxonomies based on the dimension concept. It is proved that the resulting structure is a Boolean algebra, which allows the study of classifications of vulnerabilities apparatus of Boolean algebra.

Keywords: Boolean algebra, vulnerability, information security, taxonomy.