Сравнительный анализ систем антивирусной защиты при построении гетерогенных систем

© 2011 Д.А. Строкань
Ростовский государственный экономический университет (РИНХ)
E-mail: dmitrvil@mail.ru

Проводится оценка антивирусной защиты гетерогенных информационных систем по критерию функциональной полноты.

Ключевые слова: распределенные информационные системы, гетерогенные информационные системы, антивирусные системы защиты, вирусная атака.

Чтобы обеспечить информационную безопасность предприятия, необходимо внедрение соответствующих контрмер для сохранения конфиденциальности, целостности и доступности информации. В связи с повышенной вирусной активностью антивирусная безопасность становится самостоятельным направлением. Главной тенденцией последних лет является нацеленность злоумышленников на извлечение нелегальной прибыли из создания и распространения вредоносных программ.

Когда дело касается распределенной локальной вычислительной сети с большим количеством входящих в нее рабочих станций, антивирусная безопасность становится одним из приоритетных направлений. Именно поэтому возникает необходимость создания комплексной антивирусной системы с единым центром управления. Организации, специализирующиеся в области информационной безопасности, разрабатывают специальные комплексы программных продуктов для создания иммуностойкой системы защиты сетей предприятий. На практике при построении иммуностойких систем, помимо схемы развертывания и разработки проектной и эксплуатационной документации, возникает вопрос выбора производителя антивирусных комплексов.

Постановка задачи

Пусть имеется распределенная информационная система, содержащая определенное количество узлов сети (серверов различного назначения, рабочих станций, массивов хранимой информации). Необходимо построить гетерогенную систему антивирусной защиты на основе нескольких программных продуктов.

Предлагаемый метод решения

Путем сбора информации и анализа различных программных продуктов составлен перечень выполняемых ими функциональных операций (табл. 1).

Таблица 1. **Фрагмент перечня функциональных операций**

1. ЦЕНТР УПРАВЛЕНИЯ
1.1. УПРАВЛЕНИЕ ГРУППАМИ АДМИНИСТРИРОВАНИЯ
Создание, перемещение и удаление группы
Создание структуры групп администрирования
Структура групп на основе Active Directory
Структура групп на основе содержимого текстового файла
Просмотр информации о группе
Просмотр и изменение параметров группы
Предоставление прав на работу с группой
Условия определения статуса компьютера
Мониторинг активности клиентских компьютеров
Автоматическая установка программ на клиентские компьютеры
Формирование списка агентов обновлений
1.2. УДАЛЕННОЕ УПРАВЛЕНИЕ ПРОГРАММАМИ
Создание политики
Просмотр и настройка параметров политики
Активация политики
Активация политики по событию
Политика для мобильного пользователя
Удаление политики
…

Произведем расчет для каждого отдельно защищаемого типа узла нашей системы.

Введем следующие обозначения:

$A = \{A_l\}$ - защищаемые узлы сети $(l = 1,2,\ldots,u)$, где u - количество защищаемых узлов сети;

$R = \{R_j\}$ - полезные функциональные операции $(j = 1,2,\ldots,m)$, где m - количество функциональных операций;

$S = \{S_i\}$ - программное обеспечение, ориентированное на защиту отдельного узла сети $(i = 1,2,\ldots,n)$, где n - количество сравниваемых программных продуктов.

Для каждого A :

Сформируем таблицу со строками S и столбцами R и заполним значениями $\{Y_{ij}\}$: Y_{ij}, если i -е программное обеспечение выполняет j -ю функциональную операцию.

Далее выделим программные продукты S_i и S_k $(i,k = 1,2,\ldots,n)$ и найдем

$$P_{ik}^{(11)}, P_{ik}^{(10)}, P_{ik}^{(01)}, P_{ik}^{(00)}.$$

$P_{ik}^{(11)}$ - элементы матрицы, обозначающие число функций, выполняемых S_i и S_k и определяемые как $P_{ik}^{(11)} = |S_i$ **EMBED Equation**.3 $S_k|$ - мощность пересечения 2-х множеств.

$P_{ik}^{(10)}$ - элементы матрицы, обозначающие число функций, выполняемых системой Z_1, но не реализуемых системой Z_2 и определяемых как

$P_{ik}^{(10)} = \left|\frac{S_i}{S_k}\right|$ - мощность разности соответственно 2 множеств.

$P_{ik}^{(01)}$ - элементы матрицы, обозначающие число функций, выполняемых системой Z_2, но не реализуемых системой Z_1 и определяемых как

$$P_{ik}^{(01)} = \left|\frac{S_k}{S_i}\right|.$$

$P_{ik}^{(00)}$ - мощность пересечения двух множеств S_i и S_k.

$$P_{ik}^{(00)} = P_{ik}^{(11)} + P_{ik}^{(10)} + P_{ik}^{(01)}.$$

Для оценки того, какая часть функциональных операций, реализованных в S_i, реализуется также и S_k, можно использовать величину

$$H_{ik} = \frac{P_{ik}^{(11)}}{P_{ik}^{(11)} + P_{ik}^{(10)}}, \left(0 \le H_{ik} \le 1\right).$$

Взаимосвязь между S_i и S_k оценивается по значению $P_{ik}^{(11)}$

и $G_{ik} = \frac{P_{ik}^{(11)}}{P_{ik}^{(00)}}, \left(0 \le G_{ik} \le 1\right)$,

где G_{ik} - мера подобия Жаккарда.

Выбирая различные пороговые значения ε элементов матриц P ,G и H , можно построить логические матрицы поглощения P_0, G_0, H_0.

Например, элементы матрицы H_0 получают следующим образом:

$H_{ik}^0 = 1$, если $H_{ik} \ge \varepsilon_h$, $i \ne k$; $H_{ik}^0 = 0$, если $H_{ik} < \varepsilon_h, i \ne k$.

Граф, построенный по логическим матрицам P_0, G_0, H_0, дает наглядное представление о взаимосвязи между сравниваемыми программными продуктами (по реализованным функциональным операциям).

Для оценки степени поглощения тем или иным САЗ соответствующих функциональных операций рассчитывается $P_0 + P_0^2$.

Пример. Фрагмент перечня функционально полезных операций приведен в табл. 2.

Фрагмент-матрица поглощения функциональных операций системами антивирусной защиты представлена в табл. 3.

Таблица 2. **Фрагмент перечня функционально полезных операций**

№ п/п	Функциональные операции
	1. ЗАЩИТА РАБОЧИХ СТАНЦИЙ
	2.1. АНТИВИРУСНАЯ ЗАЩИТА ФАЙЛОВОЙ СИСТЕМЫ КОМПЬЮТЕРА
1	Использование эвристического анализа
2	Проверка составных файлов
3	Проверка составных файлов большого размера
4	Изменение режима проверки
5	Приостановка работы компонента: формирование расписания
6	Приостановка работы компонента: формирование списка программ
7	Восстановление параметров защиты по умолчанию
8	Статистика защиты файлов
9	Отложенное лечение объектов
	2.3. ВЕБ-ЗАЩИТА
10	Изменение уровня безопасности HTTP-трафика
…	…

Таблица 3. **Фрагмент-матрица поглощения функциональных операций системами антивирусной защиты**

	***S*1**	***S*2**	***S*3**	***S*4**	***S*5**
1	1	1	1	1	1
2	1	1	1	1	1
3	1	1	1	1	1
4	1	1	1	1	1
5	1	1	1	1	1
6	1	1	1	1	1
7	1	1	1	1	1
8	1	1	1	1	1
9	1	1	1	1	1
10	1	1	1	0	0
11	1	1	1	1	1
12	1	1	1	0	1
13	1	0	0	1	0
14	1	1	0	0	1
15	0	1	1	1	1
16	1	1	0	0	0
17	1	1	1	1	1
18	1	1	1	0	0
19	1	1	1	1	1
20	1	1	0	0	0
21	0	1	1	1	1
22	1	1	1	1	0
23	1	1	0	1	1
24	1	0	1	0	1
25	1	1	1	1	0
26	0	1	0	1	1
27	1	1	1	0	1
28	1	0	0	1	0
29	1	1	1	1	1
30	1	1	1	0	0
31	0	1	1	0	1
…	…	…	…	…	…

Таблица 4. **Значения функционального веса**

*CA*З	Весовой коэффициент
	ЗАЩИТА РАБОЧИХ СТАНЦИЙ
*S*1	110
S2	48
*S*3	37
*S*4	18
*S*5	75
	ЗАЩИТА ФАЙЛОВЫХ СЕРВЕРОВ
*S*1	40
*S*2	116
*S*3	37
*S*4	56
*S*5	14
	ЗАЩИТА ПОЧТОВЫХ СЕРВЕРОВ
*S*1	68
*S*2	100
*S*3	36
*S*4	25
*S*5	44
	ЗАЩИТА ИНТЕРНЕТ-ШЛЮЗОВ
*S*1	130
*S*2	59
*S*3	35
*S*4	70
*S*5	27

В результате расчета $P_0 + P_0^2$ для каждого защищаемого узла сети были получены следующие значения функционального веса (табл. 4).

Вывод

Таким образом, наиболее оптимальная система антивирусной защиты в данном случае будет гетерогенной. Безопасность рабочих станций и интернет-шлюзов в такой системе будет обеспечивать программное обеспечение S1, а безопасность файловых и почтовых серверов - программное обеспечение S2. Центр управления такой гетерогенной системы будет состоять из двух систем управления S1 и S2.

1. *Тищенко Е.Н.* Анализ защищенности экономических информационных систем: монография / РГЭУ “РИНХ”. Ростов н/Д, 2003.

2. *Тищенко Е.Н., Строкачева О.А.* Оценка параметров надежности защищенной платежной системы в электронной коммерции // Вестн. Ростов. гос. экон. ун-та “РИНХ”. 2006. □2 (22).

3. *Тищенко Е.Н.* Инструментальные методы анализа защищенности распределенных экономических информационных систем: дис. ... д-ра экон. наук. Ростов н/Д, 2003.

4. *Тищенко Е.Н., Строкачева О.А.* Модель аудита информационной безопасности систем электронной коммерции // Научная мысль Кавказа / Северо-Кавказский научный центр высшей школы. 2006. Приложение □ 14 (98).

5. *Коротаев Н.В.* Методы сравнительного анализа программных средств реализации инфраструктуры открытых ключей в экономических информационных системах: дис. ... канд. экон. наук. М., 2009.

Поступила в редакцию 06.04.2011 г.