О. С. Бондаренко, Е. А. Малиновская

Имитационная модель «хакер-администратор»

В статье описан основной принцип построения имитационной модели «хакер-администратор»: характеристики с учетом возможных видов угроз и степени защищенности компьютерной системы.

С о времен возникновения первых компьютерных сетей стал очень актуальным вопрос их защиты. Как известно, первые сети возникли в конце 60-х годов XX века, и за прошедшие 40 лет данная сфера претерпела сильные изменения, связанные с развитием и усовершенствованием технологий. С каждым годом количество людей, пользующихся Интернетом, увеличивается, так, по данным отчета исследовательской компании *comScore*, в 2009 году количество людей, пользующихся глобальной сетью Интернет, превысило 1 миллиард.

Выбор правильной методологии оценки возможных угроз информационной безопасности является одним из важных условий при создании комплекса защиты. Для этой цели немаловажную роль играет визуальное представление угроз и методов защиты, так сказать, «макет поля битвы». Для этого необходимо сначала представить все возможные варианты угроз, а затем отобрать наиболее применимые к конкретному случаю. Метод анализа и оценки возможностей реализации угроз информационной безопасности должен быть основан на построении модели угроз, классификации, анализе и оценке источников угроз, уязвимостей (факторов) и вариантов реализации.

Определение всего множества угроз информационной безопасности практически невозможно, но относительно полное их описание, применительно к рассматриваемому объекту, может быть достигнуто при детальном составлении модели.

Под информацией будем понимать различные пакеты данных, файлы, учетные записи, программное обеспечение и т. д., тогда угрозы безопасности можно разделить на четыре основных и наиболее часто встречающихся вида:

1. Кража (копирование) информации;
2. Подмена (несанкционированный ввод) информации;
3. Уничтожение (разрушение) информации;
4. Перехват (несанкционированный съем) информации.

В данной статье показан один из способов создания модели «хакер-администратор», помогающей правильно оценить возможность атаки и методы ее предотвращения. В качестве входных параметров приняты следующие характеристики:

- тип угрозы;
- тип атаки «хакера»;
- тип защиты системы;
- степень защищенности элемента компьютерной сети, подверженной угрозе.

Однако нагрузка на узлы сети неодинакова. Как показывают исследования, для сети *World Wide Web* распределение выходящих связей $P_{out}(k)$ (вероятность того, что документ имеет k выходящих гиперссылок) имеет степенной характер

$$P_{out}(k) \sim k^{-\gamma_{out}}, \text{ где } \gamma_{out} = 2{,}5. \qquad (1)$$

Исходя из этого факта, с учетом входных параметров можно оценить вероятность взлома P по формуле:

$$P = L\frac{k^{-\gamma_{out}}}{Z}, \qquad (2)$$

где L — некоторый сетевой параметр, Z — уровень подготовленности атаки хакера,