УДК 681.3.067

С.А. Воронов, А.Н. Гладков, В.В. Михалев, А.Н. Павлов

Пермский военный институт внутренних войск МВД России, Пермь, Россия

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ

В статье рассмотрены вопросы, связанные с использованием имитационного моделирования для оценки эффективности системы защиты информации в локальных вычислительных сетях. Была разработана имитационная модель для определения зависимости изменения вероятности взлома ЛВС по времени на пяти различных каналах связи персонального компьютера и главного сервера ЛВС. С использованием созданной имитационной модели были проведены вычислительные эксперименты с использованием программного пакета MatLab и проведена статистическая обработка результатов экспериментов с помощью электронных таблиц EXCEL. Получены аналитические графические зависимости для определения количества отраженных атак по времени для одного канала и для всей системы.

Полученные зависимости позволяют определять наиболее уязвимые места в информационных вычислительных системах, выбирать наиболее эффективные технические и программные средства защиты локальных вычислительных сетей. Разработанная методика позволит оказать необходимую помощь разработчикам локальных корпоративных вычислительных сетей при их проектировании для предварительной оценки их эффективности для защиты информации.

Ключевые слова: имитационное моделирование, оценка эффективности, локальная вычислительная сеть, эксперимент, MatLab, аналитическая, графическая зависимость, методика, проектирование

S.A. Voronov, A.N. Gladkov, V.V. Mikhalev, A.N. Pavlov

Perm Military Institute of Internal Troops of the Ministry of Internal Affairs of Russia, Perm, Russian Federation

METHODS OF ASSESSING THE EFFECTIVENESS OF THE PROTECTION OF INFORMATION PROCESSING RESOURCES

The questions related to the use of simulation to evaluate the effectiveness of information protection systems in local area networks. Developed a simulation model to determine the dependence of changes in the probability of breaking LANs over time on five different channels of communication and PC master server LAN. Using the established simulation model have been carried out computational experiments using the software package Matlab and performed statistical analysis of the results of experiments using a spreadsheet EXCEL. Analytical graphic dependences to determine the number of attacks blocked by time for one channel and for the entire system.

The dependences obtained allow to determine the most vulnerable places in the computer information systems, to choose the most effective hardware and software to protect LANs. The developed technique will allow developers to provide the necessary assistance of local corporate computer networks in their design for a preliminary assessment of their effectiveness to protect the information.

Ключевые слова: Simulation, rating efficiency, local computing network, experiment, MatLab, analytical, graphic dependence, technique, design.

В настоящее время во внутренних войсках МВД России актуальна проблема защиты вычислительных ресурсов и ЛВС, используемых в автоматизированной системе управления войсковыми соединениями и частями. Одним из основных мероприятий при выполнении поставленных задач, стоящих перед внутренними войсками, является их защита. Для того чтобы надежно защитить информационные ресурсы ВВ МВД РФ, используются различные методики оценки эффективности защиты информации. Проблема в оценке эффективности состоит в том, что в настоящее время в свободном распространении методов, направленных на оценку защищенности, нет, так как они чаще всего являются коммерческой тайной.

Для управления рабочими процессами защищенности информации вычислительных ресурсов применяется определенное количество средств защиты информации. Эти средства весьма разнообразны по назначению, принципу действия и конструкции. В них сочетаются программные и аппаратные средства, составляющие в общем целый комплекс взаимодействующих звеньев системы. Для создания методики можно использовать один из подходов, предложенный в работе Н.А. Масловой [1]. В этой работе использовались алгоритмы Балаша и алгоритмы ветвей и границ, которые позволяют исследовать параметры модели без учета временных показателей [3].

Для создания динамической модели необходимо использовать специальный программный инструмент, который позволяет в полной мере рассчитать параметры защищенности ЛВС, в том числе и расчеты вероятности отражения атак теми или иными средствами защиты по времени. В разрабатываемой динамической модели необходимо использовать основные постулаты теории массового обслуживания.

Из анализа задачи можно сделать вывод о том, что процессы, протекающие в системе защиты информации ЛВС, являются случайными. Действительно, атака, которая нуждается в отражении, может появиться в любой момент времени. Случайна и продолжительность нахождения вредоносной атаки в ЛВС. Поэтому данную систему можно отнести к классу систем массового обслуживания (СМО). СМО – это разновидность математических схем, разработанных в теории массового обслуживания для формализации процессов функционирования систем с преобладанием массового обслуживания (например, очереди любого вида, работа любой АТС, поток задач в вычислительный центр, поток вредоносных атак на главный сервер

ЛВС и т.д.). Такие системы описываются при помощи терминов Q-схем (непрерывно-стохастических схем) [5]. Потоки требований, потоки обслуженных требований и вообще все потоки в СМО обладают одним свойством – они случайны. Любой элементарный акт обслуживания в СМО можно разделить на две составляющих:

1) ожидание заявкой начала обслуживания;
2) собственно обслуживание заявки.

Из данной теории были взяты основные параметры СМО:

- интенсивность потока вредоносных атак;
- интенсивность потока отраженных атак;
- количество каналов, используемых для атак;
- правила воздействия атак на сервер (дисциплина обслуживания);
- вероятность взлома;
- количество атак по каналу связи;
- время наблюдения и т.д.

В свете интенсивного внедрения информационных технологий практически во все сферы жизнедеятельности человека моделирование событий и процессов приобретает огромную актуальность. Расчёт параметров и характеристик моделей позволяет достичь существенной экономической выгоды, сократить расходование материальных, финансовых и временных ресурсов. Моделирование можно считать основным инструментом, обеспечивающим принятие современных и обоснованных решений. Тем не менее актуальным является не столько сам процесс принятия решений, сколько технология применения имитационного моделирования в защите информации [4].

Поскольку основой имитационного моделирования является метод статистических испытаний, наибольший эффект от его применения достигается при исследовании сложных систем, на функционирование которых существенное влияние оказывают случайные факторы.

В настоящее время на рынке программных продуктов существует много программ, которые позволяют их использовать для создания имитационных моделей. Наиболее подходящим инструментом для создания имитационной модели оценки эффективности системы защиты информации является программная среда MatLab [2].

В состав системы MatLab входит пакет моделирования динамических систем Simulink, считающийся одним из лучших пакетов моделирования.

Он дает возможность имитировать функционирование динамических систем и исследовать их работоспособность с учётом изменения состояния системы под воздействием случайных факторов.

В распоряжении пользователей имеются интерактивная графическая среда и настраиваемые библиотеки блоков, которые позволят с высокой точностью проектировать, создавать и тестировать модели цифровых устройств, средств коммуникации и других динамических систем. Была разработана имитационная модель для определения зависимости изменения вероятности взлома системы по времени на пяти различных каналах связи ПК и главного сервера ЛВС.

В результате была построена модель СМО, характеризующаяся следующими параметрами (табл. 1).

Таблица 1

Параметры модели СЗИ

№ п/п	Параметры модели	Значение параметра
1	Количество источников	5
2	Количество каналов	5
3	Дисциплина обслуживания в очереди	FIFO
4	Количество серверов обслуживания	1
5	Время наблюдения в ходе эксперимента	От 100 до 1000

Потоки атак, с которыми работает модель, описываются следующими параметрами (табл. 2).

Таблица 2

Параметры потоков атак

Параметр	Поток заявок	Поток обслуживания
Закон распределения паузы между атаками	Случайное распределение по экспоненциальному закону	Случайное распределение по экспоненциальному закону
Закон распределения интенсивности атак	Случайное распределение по равномерному закону	
Закон распределение приоритетов атак	Случайное распределение по равномерному закону	
Количество атак, пришедших на каждый канал (от каждого источника)	Регулируемое, от 1 до 1000	–

Для проведения экспериментов на модели необходимо задать исходные данные для определения основных характеристик системы защиты информации. В качестве исходных данных для определения этих характеристик были заданы ИД:

– интенсивность атак задается в блоке Uniform Random Number (интенсивность меняется от 0,1 до 1);

– приоритет и время обслуживания атак задаются в блоке SetAtribute;

– время отражения атаки задается в меню окна программного пакета MatLab;

– вероятность взлома задается в блоке Uniform Random Number (от 0 до 0,95).

С использованием представленной модели были проведены численные эксперименты. Результаты численных экспериментов позволили определить аналитические и графические зависимости для определения вероятностей взлома системы в результате смоделированных случайных атак на сервер по пяти каналам связи.

При проведении численных экспериментов на представленной имитационной модели для определения вероятности взлома системы были получены графические зависимости:

– изменения количества отражённых атак по времени для всей СЗИ (рис. 1);

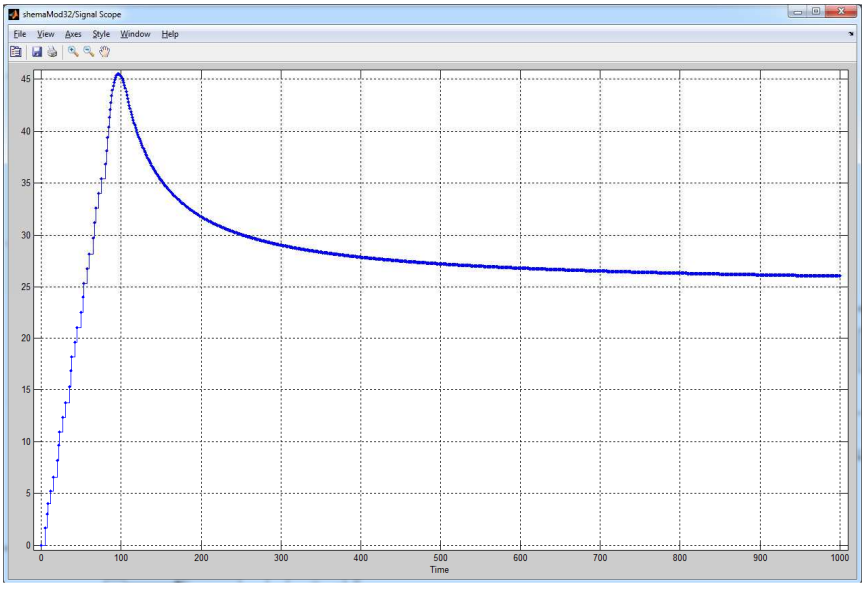

Рис. 1. Изменение количества отраженных атак по времени для всей системы

– изменения количества отражённых атак по времени для одного канала (рис. 2);

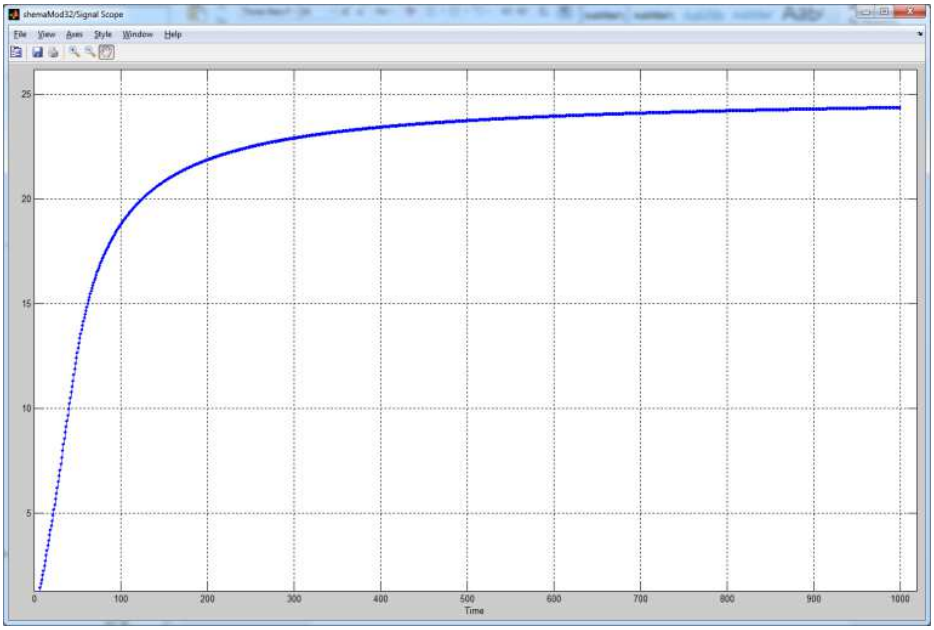

Рис. 2. Изменение количества отражённых атак по времени
в первом канале (самом ненагруженном)

– графические и аналитические зависимости изменения отраженных и неотражённых атак по времени (рис. 3).

Вероятность взлома системы защиты вычислительных ресурсов для отдельного канала определяется по формуле

$$p_i = \frac{N_{\text{отраж}}}{N_{\text{общ}}}.$$

С учётом результатов проведённых численных экспериментов можно определить вероятность взлома всей системы.

Были получены вероятности взлома системы для каждого канала:

– в первом канале $p_1 = 0{,}37$;

– во втором канале $p_2 = 0{,}52$;

– в третьем канале $p_3 = 0{,}61$;

– в четвертом канале $p_4 = 0{,}78$;

– в пятом канале $p_5 = 0{,}98$.

Вероятность взлома всей системы

$$p_C = 1 - p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 = 1 - 0,369 \cdot 0,522 \cdot 0,608 \cdot 0,782 \cdot 0,978 = 0,91.$$

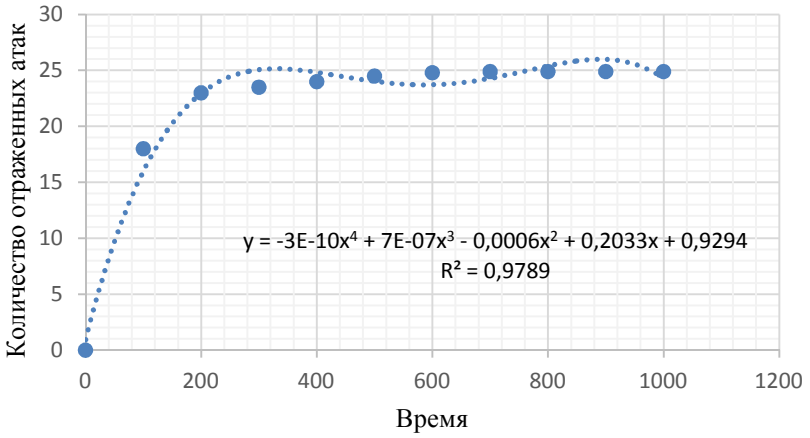

Рис. 3. Изменение количества отраженных атак по времени для одного канала

Таким образом, полученные графические и аналитические зависимости позволяют определить вероятность взлома главного сервера, наиболее опасные источники вредоносных атак. Используя в дальнейшем экспериментальные данные и сравнивая их с полученными, можно определить погрешность полученных результатов и выбрать необходимые дополнительные средства защиты главного сервера.

Библиографический список

1. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем. – Донецк, 2008.

2. MatLab. Самоучитель. Практический подход. – СПб.: Наука и техника, 2012. – 448 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

4. Введение в математическое моделирование / В.Н. Ашихмин, М.Г. Бояршинов, М.Б. Гитман [и др.]; под ред. П.В. Трусова. – М.: Интернет Инжиниринг, 2000. – 336 с.

5. Вентцель Е.С., Овчаров Л.А. Прикладные задачи теорий вероятностей. – М.: Радио и связь, 1983. – 416 с.

References

1. Maslova N.A. Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem [Valuation methods of efficiency of systems of protection of information systems]. Donetsk, 2008.

2. Vasil'ev A.N. MatLab. Samouchitel'. Prakticheskii podkhod [MatLab. Self-instruction manual. Practical approach]. Saint Petersburg: Nauka i tekhnika, 2012. 448 p.

3. Shcheglov A.Iu. Zashchita komp'iuternoi informatsii ot nesanktsionirovannogo dostupa [Protection of computer information against illegal access]. Saint Petersburg: Nauka i tekhnika, 2004. 384 p.

4. AshikhminV.N., Boiarshinov M.G., Gitman M.B. [et al.] Vvedenie v matematicheskoe modelirovanie [Introduction to mathematical simulation]. Moscow: Internet Inzhiniring, 2000. 336 p.

5. Venttsel' E.S., Ovcharov L.A. Prikladnye zadachi teorii veroiatnostei [Application-oriented tasks of probability theory]. Moscow: Radio i sviaz', 1983. 416 p.

Сведения об авторах

Воронов Сергей Александрович (Пермь, Россия) – начальник службы технической защиты информации регионального командования внутренних войск МВД России (614112, Пермь, ул. Гремячий Лог, 1).

Гладков Алексей Николаевич (Пермь, Россия) – кандидат технических наук, заместитель начальника кафедры вычислительных машин, комплексов, систем и сетей Пермского военного института внутренних войск МВД России (614112, Пермь, ул. Гремячий Лог, 1).

Михалев Вадим Валерьевич (Пермь, Россия) – преподаватель кафедры вычислительных машин, комплексов, систем и сетей Пермского военного института внутренних войск МВД России (614112, Пермь, ул. Гремячий Лог, 1).

Павлов Александр Николаевич (Пермь, Россия) – кандидат технических наук, доцент кафедры вычислительных машин, комплексов, систем и сетей Пермского военного института внутренних войск МВД России (614112, Пермь, ул. Гремячий Лог, 1).

About authors

Voronov Sergey Aleksandrovich (Khankala, Russian Federation) – Head of technical protection of information of the regional command of internal troops of the Russian Interior Ministry (614112, Perm, ul. Gremyachy Log, 1).

Gladkov Alexey Nikolaevich (Perm, Russian Federation) – Ph.D., Deputy Head of the Department of computers, complexes, systems and networks Perm Military Institute of Internal Troops of Russia (614112, Perm, ul. Gremyachy Log, 1).

Mikhalev Vadim Valeryevich (Perm, Russian Federation) – Lecturer of computers, complexes, systems and networks Perm Military Institute of Internal Troops of Russia (614112, Perm, ul. Gremyachy Log, 1).

Pavlov Alexander Nikolaevich (Perm, Russian Federation) – Ph.D., Associate Professor, Department of computers, complexes, systems and networks Perm Military Institute of Internal Troops of Russia (614112, Perm, ul. Gremyachy Log, 1).

Получено 20.02.2015