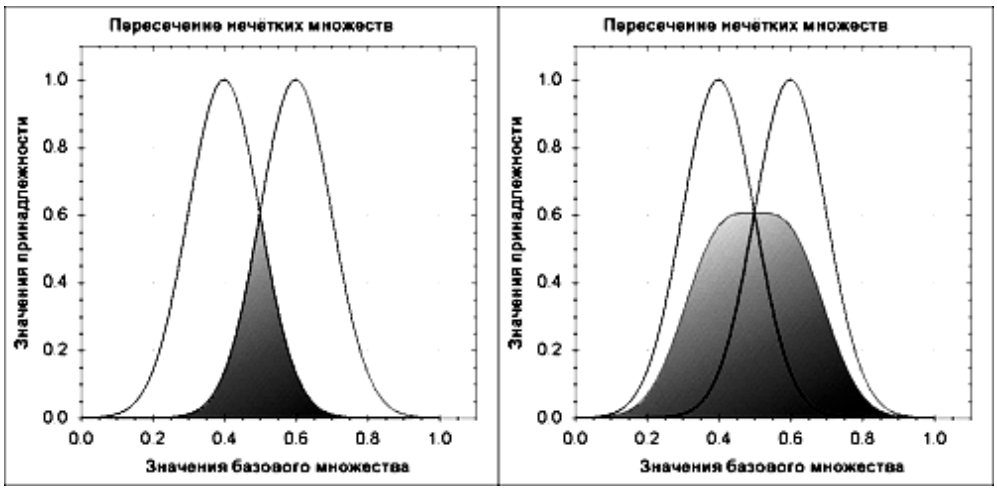

а *б*

Рис. 3. Пересечение нечётких множеств с помощью операции минимума и λ-суммы

Как показано на примерах, *t*- и *s*-нормы служат основой для построения гибких логических и семантических связок между значениями лингвистической переменной. Следует отметить, что результат действия нормы может значительно зависеть от типа и формы функций принадлежности исходных нечётких множеств, а также от расстояния Хэмминга между нечёткими множествами и значения параметров нормы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гаскаров Д. В.* Интеллектуальные информационные системы. – М.: Высш. шк., 2003. – 431 с.

2. *Величковский Б. М.* Когнитивная наука: основы психологии познания: в 2 т.: Т. 2. – М.: Смысл: Academia, 2006. – 447 с.

3. *Заде Л. А.* Понятие лингвистической переменной и его применение к принятию приближённых решений. – М.: Мир, 1976. – 165 с.

4. *Рутковская Д. и др.* Нейронные сети, генетические алгоритмы и нечёткие системы: Пер. с польск. – М.: Горячая линия–Телеком, 2007. – 452 с.

5. *Борисов В. В. и др.* Нечёткие модели и сети. – М.: Горячая линия–Телеком, 2007. – 284 с.

6. *Klir G. J., Bo Y.* Fuzzy sets and fuzzy logic: theory and applications. – New Jersey: Prentice Hall Inc., 1995. – 592 p.

УДК 004.056.5

П.А. Арьков

КОМПЛЕКС МОДЕЛЕЙ ДЛЯ ПОИСКА ОПТИМАЛЬНОГО ПРОЕКТА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Для защиты конфиденциальных данных обрабатывающихся в информационных системах в государственных и частных организациях создаются системы защиты информации (СЗИ). При этом разнообразие предлагаемых средств защиты, в

том числе и выполняющих одни и те же функции, предполагает наличие множества вариантов построения СЗИ. Как следствие возникает задача выбора оптимального проекта СЗИ отвечающего требованиям той или иной организации.

В данной работе предлагается комплекс моделей построенных с использованием теории игр и теории Марковских случайных процессов с помощью которых рассматривается множество проектов СЗИ и угроз для них, рассчитываются риски по каждой угрозе и на основе этих показателей выбирается оптимальный проект.

Архитектура разработанного комплекса моделей представляет собой иерархическую структуру, отображенную на рис. 1. Во главе иерархии находится игровая модель поиска оптимального проекта. Исходные данные для данной модели поставляют модели, лежащие на среднем уровне иерархии – игровые модели противостояния определенному типу злоумышленника. Для которых, в свою очередь, исходные данные поставляются моделями низшего уровня – полумарковскими моделями реализации угроз.

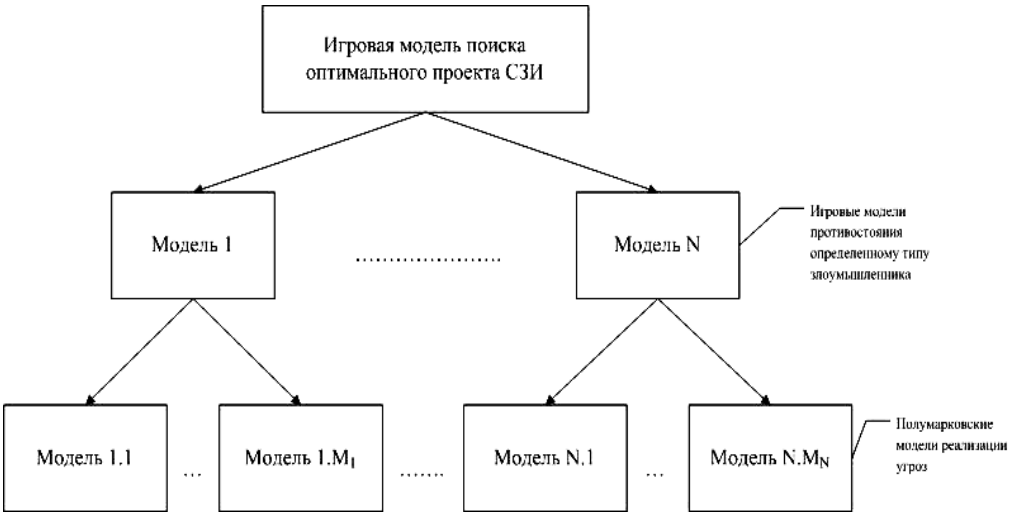

Рис. 1. Иерархическая структура комплекса моделей

Игровая модель поиска оптимального проекта представляет собой игру статистика с природой, где под статистиком понимается владелец ИС, а под природой злоумышленники различных типов. Игра описывается как $\gamma=(X, D, H)$, где H – функция полезности владельца ИС, заданная на $X \times D$, $X=\{x_i\}$ – множество стратегий владельца ИС, т.е. возможные проекты построения СЗИ, $D=\{d_k\}$ – множество типов злоумышленника, т.е. некоторые стратегии поведения присущие тому, или иному типу злоумышленников. Вероятность столкновения с определенным типом злоумышленника определяется распределением вероятностей $P(d_k) = \{p_{d_k}\}$.

Матрица выигрышей G, владельца ИС, в таком случае представляет собой $G = (h(x_i, d_k))$, где $h(x_i, d_k)$ – выигрыш владельца ИС при выборе им i-й стратегии и столкновении с k-м типом злоумышленника, в данном случае под выигрышем понимается информационный риск.

Для расчета выигрыша $h(x_i, d_k)$ используются игровые модели противостояния определенному типу злоумышленника. Данные модели также представляют собой игру статистика с природой, где под статистиком понимается владелец ИС,

а под природой злоумышленник определенного типа. Игра описывается как $\gamma=(X, \Omega, H)$, где H – функция полезности владельца ИС, заданная на $X \times \Omega$, $X=\{x_i\}$ – аналогично матрице G, это множество стратегий владельца ИС, т.е. возможные проекты построения СЗИ, $\Omega=\{\omega_j\}$ – множество угроз доступных данному типу злоумышленника. Вероятность выбора злоумышленником той или иной угрозы для реализации определяется распределением вероятностей $P(\omega_j) = \{p_{\omega_j}\}$.

Тогда матрица выигрышей A_k, k=1,K владельца ИС при игре с k-ым типом злоумышленника представляет собой $A_k = (h(x_i, \omega_{jk}))$, где $h(x_i, \omega_{jk})$ – выигрыш владельца ИС при выборе им i-й стратегии и выборе k-м типом злоумышленника j-й стратегии, в данном случае под выигрышем понимается риск, рассчитываемый как [1]:

$$h(x_i, \omega_{jk}) = P_{ijk}^{угрозы} \cdot C_j, \quad (1)$$

где $P_{ijk}^{угрозы}$ – это вероятность осуществления j-й угрозы k-м типом злоумышленника при i-м реализованном проекте СЗИ, C_j – величина потерь от осуществления j-й угрозы определяемая владельцем ИС.

Для расчета вероятностей осуществления угроз $P_{ijk}^{угрозы}$ используется полумарковская модель реализации угрозы.

Модель представляет собой полумарковский процесс с конечным множеством состояний $\{V\} = \{Vl\} \cup T \cup F$, где $\{Vl\}$ – множество уязвимостей СЗИ, T – угроза ИС, F – провал попытки реализации угрозы. При этом исходя из специфики моделируемого процесса все состояния являются невозвратными, а состояния T и F – поглощающими. Переходы из состояния i в состояние j представляют собой способ эксплуатации i-й уязвимости системы защиты. Согласно [2] полумарковский процесс определяется как ступенчатый случайный процесс $\upsilon(t)$, $t \geq 0$, со следующими свойствами. В полуинтервале $[0, t_1)$ $\upsilon(t) = \upsilon_1$, в полуинтервале $[t_1, t_2)$ $\upsilon(t) = \upsilon_2$ и т.д. При фиксированной реализации цепи Маркова $\upsilon_n = i_n$, $n \geq 1$, длительности t_1, t_2-t_1, t_3-t_2,… пребывания $\upsilon(t)$ в состояниях i_1, i_2, i_3… положительны и независимы, причем каждая из этих величин зависит лишь от состояния, в котором находится процесс и от следующего состояния. Тогда можно задать следующие функции распределения времени пребывания в состоянии, где для общности положено $t_0=0$:

$$P\{t_n - t_{n-1} < x \mid \upsilon_n = i, \upsilon_{n+1} = j\} = F_{ij}(x), \quad n \geq 1. \quad (2)$$

В рамках рассматриваемой модели время пребывания в состоянии интерпретируется как время необходимое злоумышленнику на эксплуатацию i-й уязвимости при условии, что в дальнейшем он перейдет в j-е состояние (уязвимость, к реализации угрозы, или атака провалится). Кроме того, задается начальное распределение $p_i^{(0)} = P\{\upsilon_1 = i\}$, определяющее из какого состояния злоумышленник начнет преодоление СЗИ, и матрица вероятностей выбора следующего перехода $(p_{ij}^{перех})$, которая определяет вероятность выбора пути преодоления СЗИ злоумышленником. Учитывая, что при том или ином способе эксплуатации уязвимости есть вероятность неудачи и провала атаки в целом, для каждого перехода рассматриваемого процесса задаются вероятности успешной эксплуатации i-й уязвимости $P_{ij}^{усп}$ и вероятность провала атаки при попытке эксплуатации i-й уязвимости $P_{ij}^{пров}$. При

этом $P_{ij}^{усп} + P_{ij}^{пров} = 1$. Тогда элементы матрицы переходных вероятностей (p_{ij}) полумарковского процесса, где $j \in \{Vl\} \cup T \cup F$ представляют собой следующее:

$$p_{ik} = p_{ik}^{перех} P_{ik}^{усп}, \text{ при } k \in \{Vl\} \cup T, \tag{3}$$

$$p_{iF} = \sum_j p_{ij}^{перех} P_{ij}^{пров} \text{ при } j \neq F. \tag{4}$$

Вместо матрицы переходных вероятностей (p_{ij}) и матрицы времен пребывания ($F_{ij}(x)$) можно задать лишь функцию [2]:

$$P_{ij}(x)=p_{ij}F_{ij}(x). \tag{5}$$

Функция (5) имеет следующую интерпретацию. Если в данный момент времени злоумышленник вошел в состояние эксплуатации i-й уязвимости, то с вероятностью $P_{ij}(x)$ следующий его переход произойдет за время меньшее, чем x в состояние эксплуатации j-й уязвимости или если j-е состояние это состояние T или F, то он соответственно перейдет к реализации угрозы или атака на информационную систему провалится.

Согласно [3] для описания времени затрачиваемого на выполнение какой-либо задачи используется логнормальное распределение. То есть функция $F_{ij}(x)$ описывается логнормальным распределением.

Поиск решения проводится моделированием описываемого полумарковского процесса. Моделирование проводится:

- до истечения заранее заданного времени моделирования $t_м$, чтобы определить вероятность P_t осуществления угрозы за заданное время:

$$P_t = \frac{N_T}{N}, \tag{6}$$

где N_T – количество экспериментов в которых за время $t_м$ было достигнуто состояние T, N – общее количество экспериментов;

- до достижения одного из поглощающих состояний, чтобы определить среднее время затрачиваемое на осуществление угрозы $t_{угр}$ и вероятность P осуществления злоумышленником угрозы при отсутствии ограничений времени:

$$t_{угр} = \frac{\sum_i t_i}{N_T}, \tag{7}$$

где t_i – время достижения состояния T в i-м эксперименте (t_i=0, если в эксперименте было достигнуто состояние F), N_T – количество экспериментов в которых было достигнуто состояние T;

P – рассчитывается по (6), но соответственно при $t_м \to \infty$.

При этом в (1) в качестве $P_{ijk}^{угрозы}$ используются как P, так и P_t, в зависимости от требований владельца ИС.

После расчета всех выигрышей владельца ИС по матрицам игр $A_k = (h(x_i, \omega_{jk}))$ рассчитывается $\{h(x_i, d_k)\}$ информационный риск по i-му проекту СЗИ при столкновении с k-м типом злоумышленника. Он рассчитывается как:

$$h(x_i, d_k) = \sum_j h(x_i, \omega_{jk}) p(\omega_{jk}). \quad (8)$$

Данные информационные риски при $x_i \in X$ представляют собой соответствующий столбец в матрице G. Рассчитав в матрицах $\{A_k\}$ все возможные значения $h(x_i, d_k)$, в матрице G для каждого проекта рассчитываются обобщенные риски по каждому проекту СЗИ R_{x_i}:

$$R_{x_i} = \sum_k h(x_i, d_k) p(d_k). \quad (9)$$

Затем в матрице G из множества проектов СЗИ $\{x_i\}$ выбирается множество Парето $\{x_i\}_п$ по следующим критериям:

1. $S_{x_i} \le S_{\max}$, где S_{x_i} – стоимость внедрения i-го проекта СЗИ, $S_{\max}$ – максимальное количество средств выделенных на создание СЗИ.
2. $R_{x_i} \le R_{\max}$, где R_{x_i} – обобщенные информационные риски при внедрении i-го проекта СЗИ, $R_{\max}$ – максимально допустимые обобщенные информационные риски.
3. $\{h(x_i, \omega_{jk}) \le R_j^{доп}\}$, где $h(x_i, \omega_{jk})$ – информационный риск от осуществления j-й угрозы k-м типом злоумышленника при i-м проекте СЗИ, $R_{jk}^{доп}$ – максимально допустимое значение информационного риска от осуществления j-й угрозы.
4. $\{t_{ijk}^{угр} \ge t_{jk}^{доп}\}$, где $t_{ijk}^{угр}$ – время затрачиваемое k-м типом злоумышленника при i-м проекте СЗИ на реализацию j-й угрозы, $t_{jk}^{доп}$ – минимально допустимое время затрачиваемое k-м типом злоумышленника на реализацию j-й угрозы;

Причем критерии 3 и 4 устанавливаются или для всех угроз ИС и типов злоумышленников, или только для наиболее критичных.

Для определения оптимального проекта рассматривается матрица G`, которая строится на основе матрицы G и включает только проекты из множества $\{x_i\}_п$.

Так как стратегии злоумышленника не являются чистыми, то владелец ИС, в простейшем случае, может использовать максиминную стратегию и ограничить свои максимальные риски. Но при этом максиминная стратегия в условиях смешанных стратегий злоумышленника может не являться оптимальной. Тогда в случае рандомизированной игры, т.е. когда известно распределение вероятностей $P(d_k)$, владелец ИС может воспользоваться Байесовской стратегией x_b в качестве оптимального проекта СЗИ, которая находится как:

$$H(x_b \mid P(d_k)) = \min_i H(x_i \mid P(d_k)) = \min_i \sum_k h(x_i, d_k) p(d_k) = \min_i R_{x_i}. \quad (10)$$

Фактически Байесовская стратегия это наилучшая чистая стратегия владельца ИС в осредненной игре против злоумышленника. Также согласно [4], если Байесовская стратегия совпадает с максиминной, то она является оптимальной.

В случае игры с неопределенностью, т.е. с неизвестным распределением $P(d_k)$, для нахождения оптимальной стратегии владельцу ИС фактически приходится выбирать оптимальную стратегию экспертным путем, при этом можно воспользоваться одним из критериев: Вальда, Сэвиджа, Лапласа или Гурвица [4].

Программный комплекс реализующий описанный комплекс моделей поиска оптимального проекта СЗИ разработан в среде Microsoft Visual Studio 2005 на языке C++.

Используя разработанный программный комплекс было проведено моделирование проектов системы защиты для локальной вычислительной сети факультета. Была рассмотрена модель существующей системы защиты, а также рассмотрены два проекта расширяющие её возможности.

Существующая система защиты (проект «Windows») основана на встроенных средствах защиты установленных операционных систем (Windows XP Professional SP2 и Windows 2003 Server SP1) и действующей политике безопасности.

Проект «Windows (усиленная)» представляет собой замену на серверах антивирусов и систем обнаружения вторжений на более эффективные, установку последних обновлений, чтобы закрыть обнаруженные уязвимости, а также исключение возможности использования сторонних носителей информации.

Проект «Windows+Антивирус» представляет собой, помимо мер описанных в проекте «Windows (усиленная)», замену антивирусов на всех рабочих станциях в сети, и усиление политики использования паролей пользователей.

В качестве единственного опасного типа злоумышленника рассматривались внутренние злоумышленники – студенты университета.

В качестве угроз рассматривались раскрытие и уничтожение конфиденциальной информации на файл-сервере факультетской сети.

Были определены следующие ограничения: стоимость проекта не должна превышать 160 000 руб. и максимально допустимые риски не должны быть больше 5 000.

На рис. 2 приведены результаты моделирования. Результаты представлены в виде гистограммы отображающей величины обобщенных рисков по каждому проекту. Более подробные результаты моделирования приведены в табл. 1.

Таблица 1

Результаты моделирования проектов СЗИ факультетской сети

Название проекта	Стоимость внедрения	Обобщенные риски	Вероятность реализации угрозы	
			Раскрытие	Уничтожение
Windows	95000	10485,3	0,77	0,76
Windows (усиленная)	100000	8601,3	0,64	0,63
Windows+ Антивирус	150000	271,9	0,02	0,02

Из результатов видно, что оптимальным проектом признан проект «Windows+Антивирус», так как он обеспечивает минимальные риски и единственный удовлетворяет всем ограничениям.

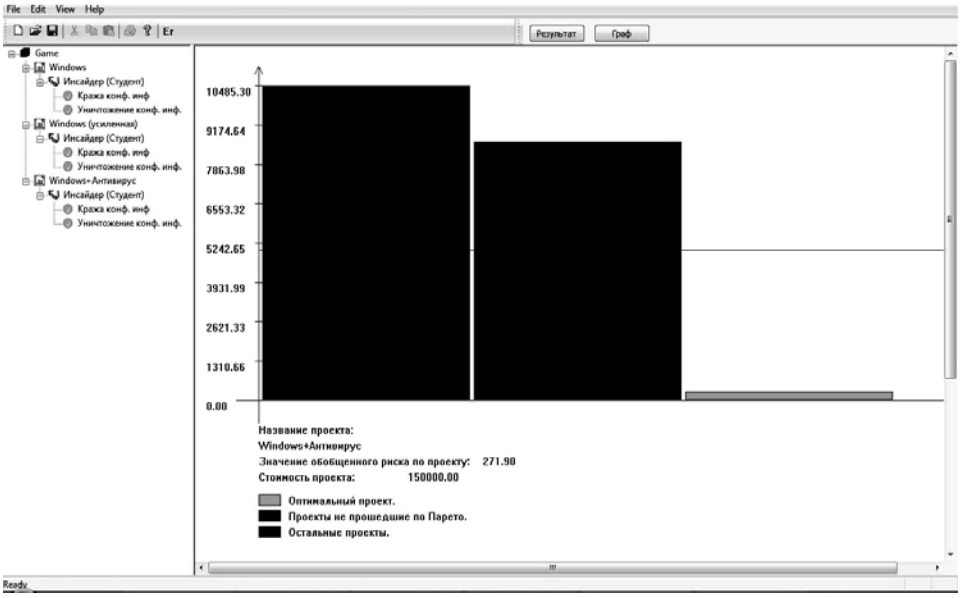

Рис. 2. Результаты моделирования (экранная копия)

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Петренко С.А. Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. – М.: Компания АйТи; ДМК Пресс. 2004.

2. *Гнеденко Б.В., Коваленко И.Н.* Введение в теорию массового обслуживания – М.: КомКнига, 2005.

3. *Кельтон В., Лоу А*. Имитационное моделирование. Классика CS. 3-е издание. – СПб.: Питер; Киев: Издательская группа BHV, 2004.

4. *Протасов И.Д.* Теория игр и исследование операций: Учебное пособие. – М.: Гелиос АРВ, 2003.

УДК 681.3.034

С.Г. Данилюк, В.Г. Маслов

ОБОСНОВАНИЕ НЕЧЕТКОГО СИТУАЦИОННОГО ПОДХОДА К СОЗДАНИЮ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ЛОЖНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

Бурное развитие информационных технологий и внедрение последних в процессы управления критически важными системами привело к острой необходимости защиты информационных ресурсов от злонамеренного вторжения с целью вывода их из строя или получения доступа к информации ограниченного пользования. Указанная проблема привела к необходимости поиска путей и решений защиты информационных систем от деструктивного, как внешнего так и внутреннего воздействия. Защита информационных систем – сложная комплексная задача, призванная решать вопросы обеспечения конфиденциальности, целостности и доступности информации. Решение вопроса обеспечения защиты информации может достигаться как программными (межсетевые экраны, анализаторы уязвимостей