- обеспечение нормального функционирования СТИС в информационной среде;
- выявление и локализацию конфликтных областей СТИС в технологическом процессе использования информационных ресурсов;
- ликвидацию инцидентов конфликтной области.

Первая задача рассматривает проблему выполнения целевых функций. Решение данной задачи основывается на изоморфном перераспределении использования информационных ресурсов в аспекте ИБ и на реорганизации выполнения целевых функций в аспекте ФБ. Вторая задача, ввиду масштабности деятельности в информационной среде СТИС, выявляет конфликтные области за счет логических схем и рассматриваемого языка управления. Третья задача направлена на стратегическое планирование реорганизации СТИС для минимизации возникновения дальнейших конфликтов как на краткосрочный, так и на долгосрочный период функционирования.

В результате данный методологический подход реализации ФДМД на основе особенностей природы функционирования СТИС и среды радикалов направлен на обеспечение информационно-системной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Волобуев С.В.* Философия безопасности социотехнических систем: информационные аспекты. – М.: Вузовская книга, 2004. – 360 с.

2. *Тарасов В.А.* Развитие внутренней структуры базовых логических элементов объектно-ориентированных программных систем. ВІСНИК Донбаської державної машинобудівної академії № 1Е (6), 2006.

3. *Пирогов М.В., Чечкин А.В.* Технология решения задач в нормализованной среде радикалов. Конференция "Интеллектуальные системы и компьютерные науки". – М.: МГУ, 23-27 октября 2006.

4. *Лепешкин О.М., Радько С.А.* Применение теории радикалов как методологического способа обеспечения функциональной и информационной безопасности социотехнических систем управления. Конференция «Управление региональными системами». – Волгоград, Центр прикладных научных исследований, 19 февраля 2008.

5. *Т.С. Соболева, А.В. Чечкин* Дискретная математика с элементами математической информатики [Текст] / под ред. Чечкина А.В. – М.: Учебное пособие для вузов РВСН, 2005. – С. 14.

УДК 004.322.067

М. Б. Гузаиров, И. В. Машкина, Т. Х. Тухватшин

РАЗРАБОТКА МОДЕЛЕЙ ПРИНЯТИЯ РЕШЕНИЙ ПО ОПЕРАТИВНОМУ УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ НА ОСНОВЕ ЧИСЛЕННОЙ ОЦЕНКИ ВЕРОЯТНОСТИ АТАКИ

Любая информационная система функционирует в условиях воздействия угроз, на которые необходимо адекватно реагировать. Современные средства обнаружения вторжений, основанные на сигнатурном анализе, не могут противостоять всему разнообразию атак из-за постоянного их обновления. Средства, основанные на отслеживании аномального поведения, в свою очередь, наоборот, производят большое число ложных срабатываний, что снижает их эффективность. К тому же основная часть присутствующих на рынке средств, имеющих наилучшие показа-

тели эффективности, как правило, является разработкой зарубежных производителей.

В настоящее время требуется комплексное решение и практическая реализация средств оценки подозрительной активности и различных событий в сети, подготовки данных и принятия решений по управлению в реальном масштабе времени для реализации своевременного реагирования на меняющиеся условия информационной среды. Для этого необходимо использовать исключительно упреждающую стратегию защиты, в основе которой должна быть способность адаптации к изменениям условий функционирования, разработать модели принятия решений по реализации оперативного управления (ОУ) защитой информации (ЗИ).

Особенностью принятия решений (ПР) по оперативному управлению ЗИ является то, что информация об атаке характеризуется неопределенностью, которую нельзя описать статистически. Задачей принятия решений является выбор решения из заданного числа альтернатив, которое бы приводило к наиболее благоприятным последствиям. Управляющее воздействие сравнивается по критериям, оценивающим последствия от каждого из них.

Оценить эти последствия и сравнить их можно, если в управляющей системе имеется модель принятия решений, в которой оцениваются последствия (исходы) от управляющих воздействий.

Необходимо стремиться, чтобы на каждое возможное состояние управляемого объекта имелось свое рациональное управляющее воздействие, чтобы существовала возможность использования управляющих воздействий в зависимости от состояния информационной среды.

При разработке моделей принятия решений используется модифицированный метод ПР в условиях риска, отличающийся от известного метода [1] тем, что необходимые для расчета целевой функции вероятности исходов рассчитываются как функции вероятности того, что подозрительная активность в сети является атакой. В работе [1] вероятности исходов задаются на основе статистических данных.

Для описания метода воспользуемся представлением задачи ПР в виде графа связи альтернатив, исходов и функции реализации, задаваемой в табличной форме.

Каждый исход задается вещественным числом, которое есть оценка ущерба при выборе той или иной альтернативы C_j.

Необходимые для расчета целевой функции вероятности исходов P_{ij} рассчитываются как функции вероятности (P_a) того, что подозрительная активность в сети является атакой: $P_{ij}= P_{ij}(P_a)$. В случае, когда выбор альтернативы приводит к двум возможным исходам, то вероятность одного из них равна вероятности атаки $P_{ij}=P_a$, другого $P_{ij}=(1-P_a)$. В случае, если исходов более двух, то применим принцип недостаточного основания Бернулли, предполагающий события из полной системы несовместимых событий равновероятными, тогда $P_{ij}=(1-P_a)/(n_i-1)$, где n_i – число возможных исходов при выборе той или иной альтернативы.

Для успешного применения математических методов при анализе сложных процессов информационного противоборства, количественно трудно формализуемых, необходимо использовать средства для учета суждений специалистов-экспертов.

Теория нечетких множеств может быть использована как средство сбора и обработки нечеткой информации, представленной экспертом, особенно те аспекты теории, которые связаны с лингвистической неопределенностью, часто возникающей при работе с экспертами на естественном языке. Под лингвистической неопределенностью подразумеваются качественные оценки естественного языка для логического вывода, принятия решений.

Введем лингвистические переменные (ЛП):

- «число сетевых событий информационной безопасности ИБ на пути распространения атаки»,
- «число событий ИБ на хосте»,
- «число событий ИБ на периметре сети»,
- «вероятность того, что подозрительная активность в сети является атакой».

Введем в рассмотрение нечеткие множества A, B, C, D с функциями принадлежности $\mu_{\tilde{A}}, \mu_{\tilde{B}}, \mu_{\tilde{C}}, \mu_{\tilde{D}}$.

$$A = \{\mu_{\tilde{A}}(x) \mid x : \mu_{\tilde{A}}(x) \in [0,1], x \in X\},$$
$$A = \{\mu_{\tilde{B}}(x) \mid x : \mu_{\tilde{B}}(x) \in [0,1], x \in X\},$$
$$A = \{\mu_{\tilde{C}}(x) \mid x : \mu_{\tilde{C}}(x) \in [0,1], x \in X\},$$
$$A = \{\mu_{\tilde{D}}(p) \mid x : \mu_{\tilde{D}}(p) \in [0,1], p \in X\}.$$

Над нечеткими множествами выполняются операции, введенные для использования нечетких множеств в задачах принятия решений.

Задается область, на которой определены значения каждой лингвистической переменной для пути распространения атаки:

$$X=\{1,2,\ldots x_i\},$$

где X – множество числа индикаторов событий ИБ.

В работе применяются числовые лингвистические переменные (нечеткие числа НЧ). У первых трех ЛП областью определения является интервал, соответствующий оси целых чисел. Множество X области определения НЧ является счетным.

Областью определения ЛП «вероятность того, что подозрительная активность в сети является атакой» является интервал, соответствующий действительной оси от 0 до 1.

Определение степеней принадлежности элементов множества и построение на их основе функции принадлежности (ФП) – основной вопрос, решаемый экспертом. Построение ФП – формализация и интеграция нечетких исходных данных, сформированных экспертом в процессе оценивания параметров событий безопасности в реальных системах защиты информации (СЗИ).

На рис. 1 представлена функция принадлежности одной из входных переменных.

Система нечеткого вывода предназначена для преобразования значений входных переменных – информации о количестве индикаторов – в выходную переменную на основе использования нечетких правил продукций. Для этого система нечеткого вывода должна содержать базу правил нечетких продукций и реализовывать нечеткий вывод заключений на основе посылок или условий, представленных в форме нечетких логических высказываний.

Экспертом задаются функции принадлежности лингвистической переменной «вероятность того, что подозрительная активность в сети является атакой». Область, на которой определена лингвистическая переменная, P∈[0,1]. Терм – множество лингвистической переменной: низкая, ниже средней, средняя, выше средней, высокая.

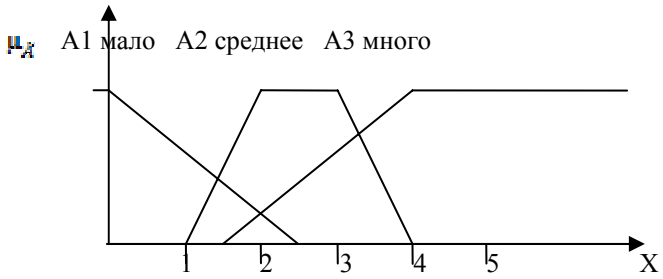

Рис. 1. Функции принадлежности лингвистических переменных «число сетевых событий ИБ»

На рис. 2 представлены функции принадлежности выходной переменной.

Дефаззификация в системах нечеткого вывода представляет собой процедуру или процесс нахождения обычного (не нечеткого) значения выходных лингвистических переменных. Дефаззификацию называют приведением к четкости. Действительно, применяемые в системах управления модули способны воспринимать команды в форме количественных значений соответствующих переменных. Традиционно используется метод центра тяжести (рис. 3).

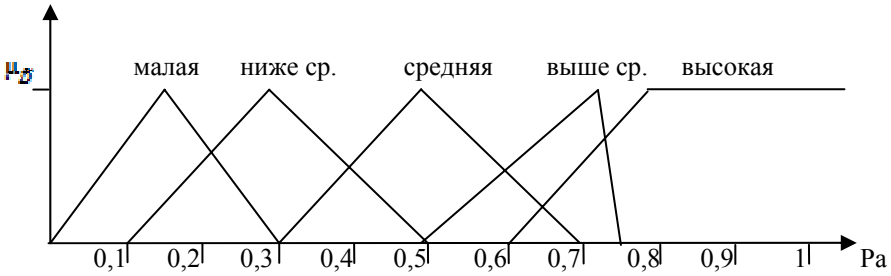

Рис. 2. Функции принадлежности лингвистической переменной «вероятность того, что подозрительная активность в сети является атакой»

Информацией, которая поступает на вход системы нечеткого вывода, являются измеренные некоторым образом входные переменные, – число признаков аномальных событий. Эти переменные соответствуют реальным процессам в сети. Информация, которая формируется на выходе системы нечеткого вывода, соответствует выходной переменной, которая является коэффициентом уверенности в том, что аномальные события в сети являются атакой.

Достоинством метода является то, что он позволяет минимизировать ущерб, с одной стороны, от возможной атаки, с другой – от того, что ответные действия могут повлиять на нормальное функционирование системы.

Вводится переменная Z, описывающая неопределенность, при задании которой однозначно известен исход при выборе каждой из альтернатив. Используя эти данные, можно составить таблицу – функцию реализации, в которой сделаны численные оценки исходов в термине «ущерб».

Далее рассчитывается математическое ожидание ущерба, в случае реализации каждой из альтернатив.

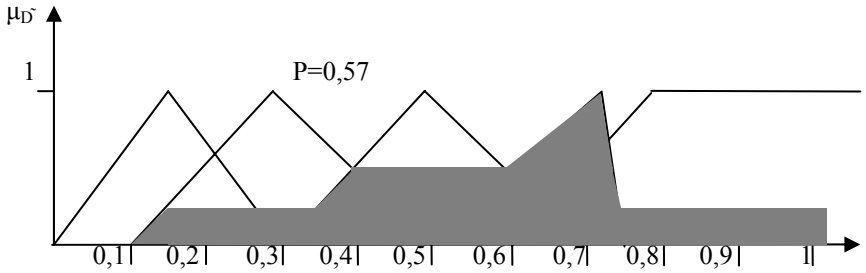

Рис. 3. Пример дефаззификации методом центра тяжести функции принадлежности выходной лингвистической переменной в случае численной оценки вероятности внутренней межсегментной атаки при следующих значениях входных НЧ: A=2, B=3

Поскольку оценка производится в термине «ущерб», то в соответствии с методом ПР выбирается альтернатива, при которой значение целевой функции J(U,Z) минимально: J(U,Z)→min

Рассмотрим разработку модели принятия решений для внутренней межсегментной атаки.

Данный тип атаки предусматривает нахождение нарушителя в пределах сети объекта информатизации. Нарушитель уже имеет доступ к сети, но его права и полномочия регламентированы политикой безопасности. В нормальном режиме функционирования сети доступ к информации возможен в том случае, если права субъекта соответствуют уровню критичности информации либо выше его. Внутренняя, или межсегментная атака – это попытка превышения данных прав с целью доступа к информации более высокого уровня критичности.

При обнаружении атаки необходимо своевременно и точно на нее среагировать, выбрав ответное действие, адекватное угрозе. Для описываемой внутренней атаки выбраны следующие варианты реагирования и приведены возможные исходы.

Варианты управляющих воздействий {Ui}:

1) реконфигурирование маршрутизаторов и систем сетевой защиты с целью блокировать пакеты от IP-адреса нападающего; 2) закрытие сетевого доступа к ЭВМ; 3) отсутствие реагирования.

Возможные варианты исходов{Vj}:

1) ущерб отсутствует (ущерб равен 0); 2) ущерб незначительный (ущерб равен 0,2); 3) ущерб средний (ущерб равен 0,55); 4) ущерб значительный (ущерб равен 1).

Строим граф связи альтернатив и исходов (рис. 4), на котором отмечены вероятности каждого исхода при выборе той или иной альтернативы.

В случае выбора альтернативы U1:

- с вероятностью, равной вероятности атаки (Pa), ущерб отсутствует, так как пресечены действия нарушителя;
- с вероятностью, равной вероятности ошибки пользователя ((1-Pa)/2), будет нанесен ущерб ниже среднего, так как произойдет временная потеря работоспособности заблокированного хоста, но в то же время будет предотвращен возможный ущерб от непреднамеренных действий;

- с вероятностью, равной вероятности ошибочной интерпретации сигналов с сенсоров ((1-Pa)/2), будет нанесен средний ущерб из-за нарушения функционирования сети, за атаку восприняты нормальные параметры работы сети, а пользователь заблокирован безосновательно.

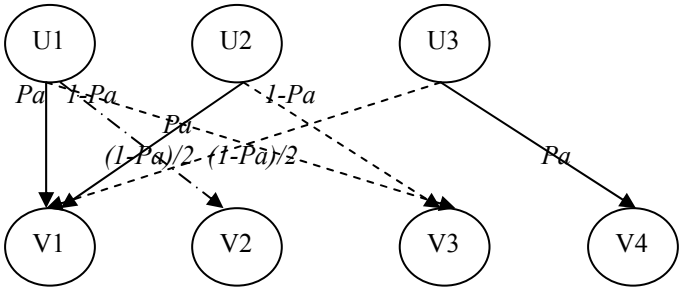

Рис. 4. Граф связи альтернатив и исходов для случая межсегментной атаки

Pa – вероятность атаки
1-Pa – ошибка любого характера
(1-Pa)/2 – ошибка пользователя
(1-Pa)/2 – ошибочная интерпретация сигналов с сенсоров (системы).

В случае выбора альтернативы U2:

- с вероятностью, равной вероятности атаки (Pa), ущерб будет отсутствовать, так как пресечены действия нарушителя;
- с вероятностью, равной вероятности срабатывания вследствие ошибки (1-Pa), ущерб средний, так как при отсутствии реальной угрозы принята мера, блокирующая ресурсы данной ЭВМ для работы другим пользователям.

В случае выбора альтернативы U3:

- с вероятностью, равной вероятности атаки (Pa), ущерб будет максимальным, так как атакующие действия нарушителя не будут блокированы системой;
- с вероятностью, равной вероятности ошибки пользователя или системы (1-Pa), ущерб будет отсутствовать вследствие отсутствия угрозы и отсутствия вмешательства в работу сети.

В качестве состояния среды z берётся множество возможных, согласно графу связей альтернатив и исходов Zj: U→V.

Исходя из максимального числа подграфов, вводятся 12 состояний среды Z, и для каждого состояния среды рассчитывается вероятность его реализации P(Zj). Вероятность состояния среды P(Zj) определяется произведением вероятностей возможных комбинаций альтернатив и соответствующих им исходов в совокупности.

Зададим функцию реализации в виде табл. 2.

Численные расчеты показали, что:

- при **Pa=0,238** рациональным будет выбор альтернативы U_3 – ***отсутствие реагирования***, поскольку $J(U_1)=0,177;\ J(U_2)=0,286;\ J(U_3)=0,148$, и следовательно $J(U_3) < J(U_1) < J(U_2)$.
- при **Pa=0,57** рациональным будет выбор альтернативы U_1 – ***блокировка пакетов от IP-адреса нападающего***, поскольку $J(U_1)=0,164;\ J(U_2)=0,237;\ J(U_3)=0,578$, и следовательно $J(U_1) < J(U_2) < J(U_3)$.

- при **Pa=0,8** рациональным будет выбор альтернативы U_2 – ***закрытие сетевого доступа к ЭВМ***, поскольку $J(U_1)=0,06;\ J(U_2)=0,05;\ J(U_3)=0,72,$ и следовательно $J(U_2) < J(U_1) < J(U_3)$.

Таблица 2

Функция реализации.

	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7	Z_8	Z_9	Z_{10}	Z_{11}	Z_{12}
	$P(Z_1)$	$P(Z_2)$	$P(Z_3)$	$P(Z_4)$	$P(Z_5)$	$P(Z_6)$	$P(Z_7)$	$P(Z_8)$	$P(Z_9)$	$P(Z_{10})$	$P(Z_{11})$	$P(Z_{12})$
U_1	C_1	C_1	C_1	C_1	C_2	C_2	C_2	C_2	C_3	C_3	C_3	C_3
U_2	C_1	C_1	C_3	C_3	C_1	C_1	C_3	C_3	C_1	C_1	C_3	C_3
U_3	C_1	C_4	C_1	C_4	C_1	C_4	C_1	C_4	C_1	C_4	C_1	C_4

Из приведенных расчетов видно, что в зависимости от вероятности того, что подозрительная активность в сети является атакой, изменяется рациональный вариант управляющего воздействия – реагирования на аномальные события в информационной сфере.

Подобные модели ПР разработаны для случаев внешних атак через периметр.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Черноруцкий И. Г.* Методы принятия решений. – СПб.: Петербург, 2005. – 416 с.

2. *Леоненков А. В.* Нечеткое моделирование в среде MATLAB и FuzzyTECH. – СПб.: БХВ - Петербург, 2005. – 736 с.

УДК 681.037

М. И. Тенетко, О. Ю. Пескова

КОНЦЕПЦИЯ ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ НА ОСНОВЕ НЕЧЁТКИХ МНОЖЕСТВ*

Введение

При оценивании информационных рисков корпорации аналитик собирает сведения об информационной системе, строит её модель и затем анализирует полученную модель с точки зрения предметной области информационной безопасности и собственного профессионального опыта. Особенности данного подхода можно выразить следующими пунктами.

1. Предметная область информационной безопасности состоит преимущественно из сущностей, выраженных не в строгом, формализованном виде, а в виде утверждений на естественном языке. Таким утверждениям присуща лингвистическая неопределённость. Под лингвистической неопределённостью в данном случае понимаются качественные оценки естественного языка для тех или иных количественных или качественных характеристик, а также для логического вывода, принятия решений и планирования [1].

2. Профессиональный опыт эксперта состоит из сущностей, которые в силу особенностей мозга выражены в форме вербальных и невербальных когнитивных образов. Когнитивный образ представляет собой субъективную репрезентацию опыта и не имеет чётких, определённых границ [2].

* Работа выполнена при поддержке гранта РФФИ № 07-07-00138а