МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 681.326

ФОРМАЛИЗАЦИЯ МОДЕЛИ ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.М. Сычев

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: dviu@mail.ru

Рассмотрена задача построения формализованной модели внутреннего нарушителя (инсайдера), которая может применяться как в государственных, так и в коммерческих организациях. Показано, что угрозы характеризуются интегральным набором векторных показателей, как количественных, так и качественных, для формализации которых требуется применение дискретной математики и теории нечетких множеств. Построена формализованная модель внутреннего нарушителя, основанная на многокритериальном ранжировании с применением рейтингового метода. Формализация нечеткой информации проведена на основе лингвистического подхода с переходом к единой количественной шкале. Рассмотрен пример определения уровня инсайдерской угрозы для группы IT-специалистов с построением семантических моделей. Показана невозможность применения традиционных методов экспертных оценок к оценке большинства показателей. Проведен анализ байесовского подхода, показана необходимость анализа большого числа статистических данных. Предложено использовать модель Шортлифа и Бьюкенена, которая позволяет делать выводы на основе неполных сведений об анализируемом объекте.

***Ключевые слова*:** модель внутреннего нарушителя, инсайдер, количественная оценка уровней угроз, рейтинговый метод.

FORMALIZATION OF INFORMATION SECURITY INSIDER MODEL

V.M. Sychev

Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: dviu@mail.ru

The problem is considered to create an insider's formalized model which can be used in the state and commercial organizations. It is shown that the threats are characterized by integral set of both quantitative as qualitative vector indices. To formalize the indices, discrete mathematics and a fuzzy set theory are needed to be used. An insider's formalized model based on multicriterion ranking and applying a rating system, is built. Formalization of fuzzy information is carried out by means of linguistic approach and transfer to an unified quantitative scale. An example of defining an insider's threat level is presented for a group of IT-specialists with building the semantic models. It is shown that traditional methods of expert analysis cannot be applied for assessment of the majority of indices. Analysis of Bayesian approach is performed. Necessity to analyze a great deal of statistical data is demonstrated. It is proposed to use the models of Shortliffe and Buchanan to draw the conclusions based on incomplete data of the object under consideration.

***Keywords*:** insider model, threat level quantitative assessment, rating method.

Повышение требований к обеспечению информационной безопасности (ИБ) различных государственных и коммерческих организаций требует формализации процесса универсальной модели внутренних нарушителей (инсайдеров), позволяющей оценивать их поведение с помощью комплексных показателей. Эти показатели, безусловно, являются интегральными, что позволит выполнять процедуру ранжирования сотрудников.

Учитывая тот факт, что отдельные составляющие показателей имеют нечисловую природу, можно утверждать, что для их формализации требуется применение математического аппарата дискретной математики и теории нечетких множеств.

Цель настоящей статьи — построение формализованной модели внутреннего нарушителя (инсайдера), входящего в коллектив сотрудников организации. Эта модель, учитывающая поведение сотрудников, основана на обработке непротиворечивой структурированной информации об изучаемой предметной области и взаимодействии между ее компонентами.

Постановка задачи. Проведенный в [1] анализ предметной области позволил предложить неформализованную информационную модель внутреннего нарушителя (инсайдера) ИБ организации. Эта модель может быть применена для оценки возможности реализации инсайдерских угроз, ассоциированных с сотрудниками организации. Здесь под возможностью реализации угрозы понимается комплексный показатель, характеризующий:

— объективно существующие условия реализации угрозы, обусловленные уязвимостью занимаемых сотрудниками должностей;

— “инсайдерский потенциал” сотрудников (индивидуальные профессиональные знания, умения, квалификация и опыт, которые могут быть использованы сотрудниками при реализации угрозы);

— личностные особенности сотрудников, влияющие на наличие устремлений (намерений) нарушения ИБ организации или потенциально возможное их возникновение.

Обозначим $S = \{si\}(i = \overline{1,n})$ — множество сотрудников организации, имеющих возможность реализации инсайдерской угрозы в силу уязвимости занимаемых должностей, инсайдерского потенциала и индивидуальных социально-психологических качеств (нелояльности), и $C = \{c^j\}(j = \overline{1,m})$ — множество показателей, используемых в модели нарушителя для характеристики $\forall s_i$. При этом

$$C = C^o \bigcup C^k \bigcup C^l,$$

где C^o — подмножество показателей, характеризующих объективно (objective) существующую уязвимость, ассоциируемую с должностью

сотрудника согласно штатному расписанию, например, осведомленность об обрабатываемых ИС-данных или о системе ИБ; C^k — подмножество показателей, характеризующих профессиональные знания, умения, квалификацию (known), используемые при нарушении ИБ, сведения о значениях этой группы показателей содержатся в персональных данных сотрудников, как правило, предоставляемых работодателю; C^l — подмножество субъективных скрытых (латентных, latent) показателей, характеризующих лояльность (социальные, психологические и другие факторы) или, иными словами, инсайдерский потенциал сотрудников.

Нетрудно увидеть, что множество показателей C характеризуют ситуативные предпосылки, условия реализации инсайдерской угрозы. Также можно полагать, что набор показателей, по которым выполняется оценка сотрудников $\forall s_i$, может быть представлен некоторым вектором, который в [2] именуют "информационным":

$$\vec{c}_i = (c_i^1, \ldots, c_i^j, \ldots, c_i^m),$$

где c_i^j — j-я компонента ($j = \overline{1,m}$) информационного вектора s_i-го сотрудника, или иначе: $S_i \Leftrightarrow \vec{c}_i$.

Информационный вектор $\vec{c}_i$ является интегральной характеристикой (описанием) текущего состояния s_i сотрудника, которое определяет уровень, ассоциированной с ним инсайдерской угрозы $t(s_i)$, т.е. $\vec{c}_i \to t(s_i)$. (Существует множество определений этого понятия, например, "Уровень угрозы представляет собой степень ее актуализации или способности наносить ущерб целостности и нормальному функционированию объекта" [3]).

Количественная оценка уровней угроз, ассоциируемых с сотрудниками, позволяет провести их ранжирование по этому показателю, т.е. определить их инсайдерский рейтинг. Другими словами, уровень инсайдерской угрозы характеризует степень соответствия сотрудника понятию "инсайдер".

В общем случае процесс ранжирования (рейтинговой оценки) включает в себя: выбор признака сравнения (в данной задаче — уровень ассоциированной с сотрудником инсайдерской угрозы; определение критериев и показателей, используемых для сравнения (набор показателей модели нарушителя, множество C); разработку методов оценки значений отдельных показателей каждого сотрудника ($\forall c^j$) и общего результата; выработку принципов ранжирования сотрудников в рейтинговой таблице.

Как следует из модели нарушителя [1], в общем случае расчет рейтинга основан на сравнении сотрудников по множеству показателей C, опосредованно характеризующих возможность реализации инсайдерской угрозы, по сравнению с условным эталонным сотрудником, имеющим оптимальные значения по сравниваемым показателям.

Применение рейтингового метода. Таким образом, задача ранжирования сотрудников сводится к сравнению и установлению отношений предпочтения векторов, например,

$$\vec{c}_1, \leq \vec{c}_i, \leq \ldots, \vec{c}_2, \leq \ldots \quad ,$$

что и означает упорядочение, многокритериальное ранжирование элементов множества S, соответственно,

$$s_1, \geq s_i, \ldots, \geq s_2, \ldots, \geq, \ldots \quad ,$$

в порядке снижения уровня инсайдерской угрозы $t(s_i)$ по значениям параметров множества C. (Наиболее простым является *метод доминирующих характеристик*, предполагающий оценку по одному из наиболее значимых показателей оцениваемого объекта. Однако ограничением на применение этого метода в данной задаче является невозможность игнорирования остальных показателей модели нарушителя, т.е. невозможность сведения задачи к однокритериальной.)

Многокритериальное ранжирование, кроме линейного ранжирования сотрудников (присвоения каждому сотруднику рейтинга), предполагает также групповое ранжирование (кластеризацию или классификацию), т.е. отнесение сотрудников в упорядоченные группы (на основе линейного ранжирования).

Главное достоинство рейтингового метода — это комплексный характер оценки уровня инсайдерской угрозы. Однако данный метод также имеет и существенные недостатки.

1. В связи с тем, что модель внутреннего нарушителя содержит большое число показателей, влияющих на уровень инсайдерской угрозы, возникают реальные трудности в комплексной оценке уровня инсайдерских угроз по каждому сотруднику $s_i \in S$. Очевидно, что некоторые из показателей имеют перекрестные корреляционные связи, которые свидетельствуют об избыточности системы параметров. Например, может существовать взаимосвязь такого показателя, как “вредные привычки” (увлечение азартными играми) и показателя “материальные затруднения”. Для разрешения подобных проблемных ситуаций часто используется факторный анализ, который служит для выделения ограниченного числа важнейших скрытых факторов путем обработки большого числа показателей. Однако в настоящей задаче этот метод не применим, поскольку значительная часть параметров модели нарушителя имеет нечисловую природу.

2. Из модели внутреннего нарушителя следует, что значения показателей измеряются как в количественных, так и качественных шкалах. Так, значения параметра “Заработная плата” измеряются по шкале отношений (количественная шкала), параметра “Осведомленность” измеряются по шкале порядка (“высокая”, “средняя”, “низкая”), параметра “Вредные привычки” — по шкале наименований (“азартные

игры", "злоупотребление алкоголем"). Как известно, к результатам таких измерений нельзя применять одни и те же операции, в частности, арифметические операции, например, к значениям параметра "Вредные привычки", хотя данные параметра "Заработная плата" допускают использование таких операций.

3. Использованный в неформализованной модели естественный язык хорошо передает семантику предметной области и понятен аналитику, но практически не позволяет точно и однозначно описать сущности и их взаимосвязи, представленные в модели. При этом уровень инсайдерской угрозы определяется значениями преимущественно качественных показателей, составляющих неформализованную модель внутреннего нарушителя ИБ организации. При оценивании по этим показателям обычно используются слова естественного языка, например, "конфликтность" сотрудника может быть "пониженная", "обычная", "повышенная". Использование нечетких понятий позволяет провести качественные описания, учесть неопределенность, но при этом вносит нечеткость в характеристику сотрудника и усложняет обработку данных.

4. Отсутствует формализованная процедура определения значений показателей. Поэтому представляется логичной необходимость формализации предложенной в [1] естественно-языковой модели в целях выработки непротиворечивой структурированной интерпретации полученной информации об изучаемой предметной области и взаимодействии между ее компонентами.

Формализация нечеткой информации. На основе лингвистического подхода, в рамках которого в качестве значений переменных допускаются как числа, так и слова и предложения естественного языка, может быть проведена формализация нечеткой информации, а ее аппаратом является теория нечетких множеств.

Следует отметить, что несмотря на имеющиеся исследования по данной тематике, остается недостаточно изученной проблема формализованного описания множества значений качественных признаков. При этом применение аппарата теории нечетких множеств получило наибольшее распространение в области финансов, медицины, психологии. Однако для решения сложной слабоструктурированной задачи профилактики инсайдерской угрозы данная теория еще не применялась.

Будем интерпретировать любой показатель c^j как лингвистическую переменную с фиксированным терм-множеством, т.е. множеством названий лингвистических значений переменной c^j (например, высокая, средняя, низкая).

Необходимо определить синтаксическое правило G, интерпретирующее значения лингвистической переменной c^j в значения лингвистической переменной "уровень инсайдерской угрозы" t^j (по показателю

c^j), и семантическое правило M, которое ставит в соответствие каждой нечеткой переменной терм-множества лингвистической переменной t^j нечеткое подмножество универсального множества $U = [0; 1]$.

В качестве синтаксического правила G предлагается использовать конструкцию "если – то". Пример применения правила G приведен в табл. 1.

Таблица 1

Правило соответствия характеристики сотрудника c^j и уровня ассоциированной с ним инсайдерской угрозы t^j

Характеристика сотрудника (лингвистическая переменная c^j)	Терм-множество лингвистической переменной c^j	Правило G	Уровень угрозы (лингвистическая переменная t^j)		
			Высокий	Средний	Низкий
Вредные привычки, c^1	Отсутствуют	Если c^1 отсутствуют, то t^1 — низкий	–	–	+
	Неизвестны	Если c^1 не известны, то t^1 — средний	–	+	–
	Присутствуют	Если c^1 присутствуют, то t_1 — высокий	+	–	–
Материальные затруднения, c^j	Отсутствуют	Если c^j отсутствуют, то t^j — низкий	–	–	+
	Нет данных	Если c^j не известны, то t^j — средний	–	+	–
	Большие	Если c^j большие, то t^j — высокий	+	–	–

Как было отмечено ранее, большая часть сведений о потенциальных инсайдерах измеряется в качественных шкалах и лишь некоторые данные — в количественных. Поэтому для сопоставимости данных и их численного представления перейдем от значений разнотипных параметров к их нечетким оценкам, измеряемым в одной и той же количественной шкале.

Для этого можно использовать так называемые вербально-числовые шкалы, позволяющие измерить степень интенсивности какого-либо свойства, имеющего субъективный характер. Вербально-числовые шкалы отображают (правило M) содержательное (вербальное) описание значения показателей уровня угроз в соответствующие им числовые значения. Для этих целей часто используется таблица Харрингтона [4] (табл. 2).

Таблица 2

Таблица Харрингтона

Значения показателей лингвистической переменной t^j	Числовое значение (из множества U)
Очень высокий	0,8–1,0
Высокий	0,64–0,8
Средний	0,37–0,64
Низкий	0,2–037
Очень низкий	0–0,2

Из табл. 2 следует, что шкала измерения определена интервалом вещественных чисел [0,1], на котором для каждого сотрудника s_i по лингвистическому значению каждого параметра (c^j) можно установить числовую оценку $u^j(s_i) \in [0,1]$, которая характеризует уровень инсайдерской угрозы этого сотрудника по j-му параметру.

В результате каждый сотрудник s_i формализуется не множеством лингвистических значений параметров C, а множеством $\{u^1(s_i), \ldots, u^j(s_i), \ldots, u^m(s_i)\}$ соответствующих им числовых оценок. При этом все они измеряются по одной и той же числовой шкале (интервал [0,1]) и, следовательно, могут быть использованы в численных расчетах.

Также для каждого показателя $c^j \in C$ имеется множество функций подмножества $\{u^j(s_1), u^j(s_2), \ldots, u^j(s_n)\}$, каждый элемент которого определяет уровень инсайдерской угрозы сотрудника s_i по этому параметру (табл. 3).

Таблица 3

Числовые оценки степени соответствия сотрудника понятию “инсайдер”

Сотрудники	Показатели		
	c^1	c^j	c^m
s_1		$u^j(s_1)$	
s_i	$u^1(s_i)$	$u^j(s_i)$	$u^m(s_i)$
s_n		$u^j(s_n)$	

Таким образом, последовательно отображается значение нечеткой переменной (например, “отсутствует”) лингвистической переменной $c^j(s_1)$ в значение нечеткой переменной (например, “большой”) лингвистической переменной $t^j(s_1)$ [правило G] и числовое значение $u^j(s_1)$ из диапазона [0,1] [правило M].

Следовательно, понятие инсайдер (состояние сотрудника) можно представить нечетким множеством, заданным на универсальном множестве сотрудников S,

$$\tilde{A}^j = \{u^j(s_1)/s_1,\ u^j(s_2)/s_2, \ldots, u^j(s_n)/s_n\}$$

с функцией принадлежности $u^j(s_i)$, характеризующей соответствие любого сотрудника $s_i \in S$ данному понятию.

При введении в модель показателя важности параметров ранжирование сотрудников можно провести на основе следующего выражения:

$$u_{\tilde{c}}(s_i) = \sum_{j=1}^{m} b^j u^j(s_i),$$

где $b^1, b^2, \ldots, b^m$ — неотрицательные числа $\left(\sum_{j=1}^{m} b^j = 1\right)$, характеризующие относительную важность параметров $c^1, c^j, \ldots, c^m$ или их удельный вес в модели нарушителя; $u^j(s_i)$ — значение функции принадлежности из [0,1] для каждого сотрудника $s_i \in S$ по значению каждого параметра c^j $(j = \overline{1,m})$, которая характеризует, насколько этот сотрудник соответствует понятию "инсайдер по j-му параметру".

Тогда, наибольшую инсайдерскую угрозу для организации представляет сотрудник, имеющий максимальное значение функции принадлежности

$$u_{\tilde{c}}(s^*) = \max_{s_i \in S} u_{\tilde{c}}(s_i).$$

Пример определения уровня инсайдерской угрозы. Для примера рассмотрим задачу определения уровня инсайдерской угрозы для группы IT-специалистов: s_1 — системный администратор; s_2 — администратор одной из подсистем; s_3 — оператор баз данных, составляющих универсальное множество S. Упрощенные семантические модели внутреннего нарушителя для сотрудников этой группы приведены в табл. 4.

Таблица 4

Параметры модели внутреннего нарушителя информационной безопасности

Параметр	Значения		
Осведомленность, c^1	Низкая	Средняя	Высокая
Компрометирующий круг общения, c^2	Криминальная среда, наркоманы и т.д.		
Заинтересованность в результатах труда, c^3	Низкая	Средняя	Высокая
Заработная плата, c^4	(0,∞), руб		
Вредные привычки, c^5	Азартные игры, злоупотребление алкогольными напитками, наркотики		

Еще раз отметим, что для решения задачи используются данные, измеряемые в различных шкалах:

— количественной шкале отношений (“Заработная плата”);

— качественной шкале порядка (“Осведомленность”, “Заинтересованность результатах труда”);

— качественной шкале наименований (“Компрометирующий круг общения”, “Вредные привычки”).

Возможные значения параметров для IT-специалистов приведены в табл. 5.

Таблица 5

Характеристики IT-специалистов

Параметр			IT-специалист		
Наименование	b^j	β^j	s_1	s_2	s_3
Осведомленность, c^1	7	0,23	Высокая (0,9)	Средняя (0,65)	Средняя (0,65)
Компрометирующий круг общения, c^2	6	0,2	Неизвестен (0,1)	Неизвестен (0,1)	Неизвестен (0,1)
Заинтересованность в результатах труда, c^3	3	0,1	Средняя (0,65)	Низкая (0,3)	Высокая (0,85)
Заработная плата, c^4	8	0,27	40000 (0,8)	30000 (0,6)	20000 (0,25)
Вредные (опасные) привычки, c^5	6	0,2	Отсутствуют (0)	Игра в карты на деньги (0,8)	Неизвестны (0,1)
$u_{\tilde{c}}(s_i)$			0,508	0,52	0,342

Далее каждому IT-специалисту поставим в соответствие число из интервала [0,1], которое отражает уровень угрозы (степень соответствия понятию “инсайдер”).

Кроме этого, можно оценить важность каждого параметра в числовых значениях $b^1, \ldots, b^m$ из интервала [0,10] и вычислить по этим данным значения коэффициентов важности $\beta^j = b^j \Big/ \sum_{k=1}^{m} b^k$, удовлетворяющие условию $\sum_{j=1}^{m} \beta^j = 1$. Полученные результаты также представлены в табл. 5.

Итоговые значения $u^j(s_i)$ функции принадлежности из [0,1] для каждого сотрудника $s_i \in S$ характеризуют степень его соответствия понятию “инсайдер по j-му параметру”.

Ранее при определении уровня инсайдерской угрозы персонала организации по умолчанию предполагалось, что построение функции принадлежности не связано с какими-либо трудностями. Однако в силу различных причин решение этой задачи нетривиально как в научном, так и в прикладном плане. Основные методы ее решения, а также

возможные подходы к их совершенствованию рассмотрены в работе [5]: балльные шкалы, опрос единственного эксперта, опрос группы экспертов и др.

Особенностью данной прикладной задачи является невозможность применения к большинству показателей традиционных методов экспертных оценок. Основные причины заключаются в следующем.

1. Оценки сотрудников (как в явном, так и неявном виде) по множеству параметров C содержатся в массиве вербальных и документальных источников информации.

2. Для большинства сотрудников значения различных показателей c_j отсутствуют и не могут быть получены, следовательно, значения u^j не могут быть определены. Задача решается на множествах C^o, C^k, C^l, состав которых и значения элементов есть функции времени.

3. Приведенные ранее особенности создают затруднения в распределении значений коэффициентов $\forall b^j$, характеризующих относительную важность параметров $c^1, c^j, \ldots, c^m$ (удельный вес в модели нарушителя).

Из описанных особенностей следует вывод, что рейтинговый подход можно применить к "объективной" части модели, которая описывается набором показателей уязвимости C^o, и для каждого показателя можно определить значение уровня инсайдерской угрозы ("степень *уязвимости*" для конкретных должностей).

Видимо, можно определить значения уровня инсайдерской угрозы ("*инсайдерский потенциал*") и по показателям C^k. Данные для их расчета относительно стабильны во времени и могут быть получены из официальных источников ("*степень квалификации или профессионализма*").

Однако для показателей C^l какая-либо предопределенность отсутствует как в части набора показателей, так и в части наличия их значений. Поэтому в целом классический рейтинговый подход нельзя использовать для комплексной оценки возможности нарушения ИБ конкретным сотрудником, поскольку нарушается идея рейтинга — оценка по одинаковому и некорелированному набору показателей.

Байесовский подход. Теоретической базой преодоления рассмотренных проблем рейтинговой оценки возможности реализации инсайдерской угрозы может служить известный байесовский подход. Пусть существуют две гипотезы:

- h_i — возможность реализации инсайдерской угрозы, ассоциированной с s_i-сотрудником;
- $\tilde{h}_i$ — невозможность реализации инсайдерской угрозы, ассоциированной с s_i-сотрудником. Гипотезы h_i и $\tilde{h}_i$ несовместны и образуют полную группу событий H. Будем полагать, что известны априорные вероятности гипотез $p(h_i)$ и $p(\tilde{h}_i)$, тогда $p(h_i) + p(\tilde{h}_i) = 1$.

В общем случае в качестве вероятности $p(h_i)$ можно использовать имеющиеся статистические данные об инсайдерских нарушениях ИБ различными категориями сотрудников. Однако более достоверными и доступными для конкретной организации представляются данные оценки возможности реализации инсайдерской угрозы, определенные на множестве показателей C. Здесь вероятность рассматривается как мера возможности появления события, выражаемая действительным числом из интервала от 0 до 1, где нуль соответствует невозможному, а единица — достоверному событию [6].

Отметим, что значения показателей множества C, определяющие должностную уязвимость, инсайдерский потенциал и лояльность s_i-го сотрудника — события условно независимые. Тогда справедливо выражение

$$\tilde{p}(h_i) = p^o(h_i) * p^k(h_i) * p^l(h_i),$$

где $p^o(h_i)$ — вероятность реализации инсайдерской угрозы, ассоциируемая с уязвимостью j-й должности, определяется на подмножестве C^o показателей; $p^k(h_i)$ — вероятность реализации инсайдерской угрозы, обусловленная инсайдерским потенциалом s_i-го сотрудника, определяется на подмножестве показателей C^k; $p^l(h_i)$ — вероятность возникновения (проявления) инсайдерской угрозы, обусловленная личными социально-психологическими характеристиками (нелояльностью) s_i-го сотрудника, определяется на подмножестве C^l показателей.

Для количественной оценки вероятности (возможности) реализации инсайдерской угрозы можно применить рассмотренный ранее подход оценки уровня угроз (см. табл. 1 и 2) и считать $p^o(h_i)$ и $p^k(h_i)$ численно равным уровням угроз, определяемым на множествах C^o и C^k соответственно.

Таким образом, значения $p^o(h_i)$ и $p^k(h_i)$ могут быть определены на основе метода рейтинговых оценок. Однако, как уже указывалось, оценки рейтинга $p^l(h_i)$ и рейтингов иных сотрудников по множеству показателей C^l не дают сопоставимых результатов.

В этом случае можно рассматривать $p(h_i) = p^o(h_i)p^k(h_i)$ в качестве априорной вероятности реализации инсайдерской угрозы t_i; значения социально-психологических показателей (показателей нелояльности) $\forall c^j$ для s_i-го сотрудника — как свидетельства, которые могут подтвердить истинность гипотезы h_i.

Тогда в соответствии с теоремой Байеса имеем

$$p(h_i/e_1) = \frac{p(e_1/h_i)p(h_i)}{p(e_1/h_i)p(h_i) + p(e_1/\bar{h}_i)p(\bar{h}_i)}, \qquad (1)$$

где $p(h_i)$ — априорная вероятность (возможность) реализации инсайдерской угрозы; $p(h_i/e_1^l)$ — апостериорная вероятность (возможность) реализации инсайдерской угрозы t_i при наличии свидетельства $e^1 \in E$

($E = \{e^m\}$ — множество всех свидетельств, характеризующих нелояльность сотрудников в комплексной модели внутреннего нарушителя); $p(e^1/h_i)$ — вероятность поступления свидетельства e^1 при условии истинности гипотезы h_i; $p(e^1/\bar{h}_i)$ — вероятность поступления свидетельства e^1 при условии истинности гипотезы $\bar{h}_i$.

При наличии m независимых свидетельств апостериорная вероятность гипотезы h_i оценивается следующим образом {байес04}:

$$p(h_i/e^1, e^2, \ldots, e^m) = \\ = \frac{p(e^1/h_i)p(e^2/h_i)\ldots p(e^m/h_i)p(h_i)}{p(e^1/h_i)p(e^2/h_i)\ldots p(e^m/h_i)p(\bar{h}_i)+p(e^1/\bar{h}_i)p(e^2/\bar{h}_i)\ldots p(e^m/\bar{h}_i)p(\bar{h}_i)}.$$

Данное равенство связывает гипотезу h_i с множеством подкрепляющих ее свидетельств E. Интерпретация равенства предполагает знание априорной вероятности $p(h_i)$ как вероятности, приписываемой h_i до появления каких-либо свидетельств, а также вероятности свидетельств из E при наличии гипотезы h_i.

Отметим, что при низких априорных вероятностях любое положительное свидетельство значительно увеличивает вероятность гипотезы. Если же априорная вероятность относительно велика, то положительное свидетельство лишь незначительно увеличивает ее.

Выражение для условной вероятности с точки зрения теории принятия решений можно рассматривать как выражение правила принятия решения и интерпретировать выражение $p(h_i/e_k) = \alpha$ как утверждение: если характеристика c^j сотрудника s_i принимает значение e^k, то можно полагать, что с вероятностью α справедлива гипотеза h_i.

Формула Байеса теоретически бесспорна, однако в исследуемой задаче ее применение ограничено отсутствием данных, необходимых для оценки условных вероятностей.

Следует отметить, что в общем случае байесовский подход требует значительного числа статистических данных не просто для каждого значения e^k, но также для описания взаимосвязей e^k с каждой гипотезой. Поэтому практически непреодолимая в исследуемой задаче трудность заключается в установлении непосредственной связи гипотез и соответствующих им признаков. Кроме того, в исследуемой задаче характер таких взаимосвязей является функцией времени.

Практическая уникальность оценок возможности реализации инсайдерской угрозы для каждого сотрудника s_i, исключающая наличие генеральной совокупности или представительности выборки показателей C^l, обусловила актуальность замены понятия вероятности иными, доступными оценками.

Модель Шортлифа и Бьюкенена. Приведенные ограничения байесовского подхода к определению возможности реализации инсайдерской угрозы обусловливают необходимость рассмотрения альтер-

нативных решений, одним из которых может быть подход, предложенный Шортлифом (Shortliffe) и Бьюкененом (Buchanan) [7].

В модели Шортлифа и Бьюкенена введены понятия: *мера уверенности* (*Measure Believe, MB*), *мера неуверенности* (*Measure Distrust, MD*) и *фактор уверенности* (*Certainty Factors, CF*), предназначенные для оценки весомости свидетельств. (К недостаткам данного метода можно отнести тот факт, что коэффициенты уверенности не являются вероятностями и для работы с ними предложены уникальные формулы, не встречающиеся в какой-либо математической теории. Как отмечается в работе [8], слабая теоретическая обоснованность — самый серьезный недостаток этого метода.)

Так, $\mathrm{MB}[h, e] = \alpha$ означает, что степень (мера) уверенности в гипотезе h, основанная на свидетельстве e, есть α, а $\mathrm{MD}[h, e] = \beta$ — степень неуверенности в гипотезе h, основанная на свидетельстве e, равна β.

В нашем случае мера уверенности $\mathrm{MD}[h_i, e^k]$ равна нулю, так как по определению уменьшение уверенности в h_i не может быть проведено на основании e^k, поскольку семантически модель внутреннего нарушителя сконструирована так, что содержит только показатели, свидетельствующие о возможности реализации инсайдерской угрозы (не содержит данных подтверждающих лояльность сотрудника).

При этом одно и то же свидетельство не может выступать как в пользу, так и против гипотезы, т.е. при $\mathrm{MB}[h, e] \geq 0$, $\mathrm{MD}[h, e] = 0$. Отсюда следует, что в исследуемой задаче $CF = MB[0, 1]$. $CFe^k = 0$, если свидетельство e^k отсутствует.

Для описания вероятностных характеристик истинности гипотез можно применять коэффициент уверенности в истинности гипотезы, который будем трактовать как вероятность того, что выдвинутая в качестве решения гипотеза истинна.

Следует отметить, что свидетельства $e^k \in E$ $(k = \overline{1, m})$ с вероятностью α могут быть не только наблюдаемыми событиями, но и гипотезами, т.е. предположениями о значениях характеристик сотрудника C^l. Таким образом, можно записать $\mathrm{MB}[h_1, h_2]$, чтобы указать на меру увеличения уверенности в гипотезе h_1 при условии, что гипотеза h_2 является истинной.

В общем случае модель Шортлифа и Бьюкенена позволяет делать выводы на основе неполных сведений об анализируемом объекте; по существу аппроксимирует условные вероятности; предполагает оценку экспертами данных с точки зрения подтверждения или отрицания гипотезы.

В процессе накопления данных по каждому сотруднику s_i будут постепенно появляться данные по подмножеству показателей C^l, свидетельства, с той или иной степенью уверенности подтверждающие гипотезу h_i о возможности реализации инсайдерской угрозы t_i.

Это означает, что для обобщенного суждения об истинности данной гипотезы может быть использовано несколько итераций. Применение каждого из них — отдельная гипотеза — характеризуется некоторым значением коэффициента уверенности. Например, из одного правила следует, что сотрудник s_i — нелояльный, причем коэффициент уверенности этой гипотезы CFe^k равен 0,8. Другое правило, принимая во внимание другие характеристики анализируемого субъекта (гипотеза e^{k+1}), приводит к заключению, что этот же сотрудник — нелояльный с $CFe^{k+1} = 0{,}2$.

Пусть CFe^k и CFe^{k+1} — коэффициенты уверенности одинаковых свидетельств, полученные при применении разных правил. Тогда результирующий коэффициент уверенности

$$CF(e^k, CFe^{k+1}) = CFe^k + CFe^{k+1} - CFe^k CFe^{k+1} \qquad (2)$$

при CFe^k, $CFe^{k+1} > 0$.

При наличии нескольких гипотез итоговое значение CF может быть получено в результате последовательного применения правила (2), которое имеет свойство коммутативности, т.е. порядок, в котором обрабатываются гипотезы, значения не имеет.

Заключение. Таким образом, разработана универсальная формализованная модель внутреннего нарушителя информационной безопасности, которая может применяться как в государственных, так и в коммерческих организациях. Угроза характеризуется интегральным набором векторных показателей.

Модель предполагает групповое ранжирование и содержит большое число показателей, имеющих кластеризационные связи. Значения показателей оцениваются как в количественных, так и в качественных шкалах. Предложены способы формализации информации с помощью теории нечетких множеств. При рассмотрении байесовского подхода отмечено, что в данном случае потребуется значительный объем статистических данных.

ЛИТЕРАТУРА

1. *Карпычев В.Ю.*, *Сычев В.М.*, *Минин Ю.В.* Новые подходы к моделированию внутреннего нарушителя информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2013. № 7. С. 32–39.
2. *Гараев Я.Г.*, *Рязанцева М.В.* Оценка интеллектуальной собственности и нематериальных активов сравнительным подходом с применением экспертно-математических методов // НПЖ “Современные научные исследования и инновации”. http://web.snauka.ru/issues/2012/10/17777 (дата обращения 21.08.2013).
3. *Распоряжение* Правительства Москвы от 16 апреля 2010 г. № 707-РП “Об утверждении Концепции комплексной безопасности города Москвы”.
4. *Литвак Б.Г.* Экспертные технологии в управлении. М.: Дело, 2004. 400 с.
5. *Полещук О.М.* Методы формализации и обработки нечеткой экспертной информации: Дис. . . . д-ра техн. наук. М., 2004. 278 с.

6. *ГОСТ Р 51897*. Менеджмент риска. Термины и определения. М.: Стандартинформ, 2012.
7. *Buchanan B.G.* and *Shortliffe E.H.* ed. Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project. Reading, MA: Addison-Wesley, 1984.
8. *Бакаев А.А.*, *Гриценко В.И.*, *Козлов Д.Н.* Интервальный вероятностный подход к работе с неопределенностью в базах знаний // Управляющие системы и машины. № 4. 1990. С. 40–48.

REFERENCES

[1] Karpychev V.Yu., Sychev V.M., Minin Yu.V. New approaches to modeling an insider of information security. *Pribory i sistemy. Upravlenie, kontrol', diagnostika* [Instruments and Systems: Monitoring, Control, and Diagnostics], 2013, no. 7, pp. 32–39 (in Russ.).
[2] Garaev Ya.G., Ryazantseva M.V. Assessment of intellectual property and intangible assets by means of comparative approach using expert and mathematical methods. *Nauchn.-praktich. zhurnal "Sovremennye nauchnye issledovaniya i innovatsii"* [Scientific & practical journal "Modern scientific researches and innovations"]. Available at: http://web.snauka.ru/issues/2012/10/17777 (accessed 21.08.2013).
[3] Moscow City Government Executive Order dated April 16, 2010 no. 707-РП "On approval of the Concept of comprehensive security in the city of Moscow".
[4] Litvak B.G. Ekspertnye tekhnologii v upravlenii [The expert technology in management]. Moscow, Delo Publ., 2004. 400 p.
[5] Poleshchuk O. M. Metody formalizatsii i obrabotki nechetkoy ekspertnoy informatsii: Diss. Dokt. tekhn. nauk [Methods of formalization and processing fuzzy expert information. Dr. eng. sci. diss.]. Moscow, 2004. 278 p.
[6] Standard RF GOST R 51897. Menedzhment riska. Terminy i opredeleniya [State Standard R 51897 Risk management. Terms and Definitions]. Moscow, Standartinform Publ., 2012.
[7] Buchanan B. G., Shortliffe E.H. ed. Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project. Reading, MA: Addison-Wesley, 1984.
[8] Bakaev A.A., Gritsenko V.I., Kozlov D.N. Interval probabilistic approach to dealing with uncertainty in knowledge databases. Upravlyayushchie sistemy i mashiny [Control systems and machines], 1990, no. 4, pp. 40–48 (in Russ.).

Статья поступила в редакцию 4.12.2014

Сычев Владимир Михайлович — ассистент кафедры "Защита информации" МГТУ им. Н.Э. Баумана. Автор пяти научных работ в области информационной безопасности.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

Sychev V.M. — assistant lecturer of "Information Security" department of the Bauman Moscow State Technical University. Author of 5 publication in the field of cybercrime defenses.
Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.