УДК 681.3.04

ОЦЕНКА СТЕПЕНИ ВЛИЯНИЯ СОПУТСТВУЮЩИХ ФАКТОРОВ НА ПОКАЗАТЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ш.Г. Магомедов, к.т.н., доцент

Кафедра КБ-4 «Автоматизированные системы управления», Институт комплексной безопасности и специального приборостроения,
Московский технологический университет (МИРЭА), Москва, 107996 Россия
Автор для переписки, e-mail: msgg@list.ru

В статье рассмотрена задача повышения достоверности оценок показателей обеспечения информационной безопасности на основе построения когнитивных моделей сопутствующих факторов, связанных с процессом формирования и развития разных типов угроз. Введены новые типы оценок показателей безопасности, обеспечивающие определенный гарантированный уровень интервала возможных значений показателя. Сформирована процедура построения когнитивных моделей сопутствующих факторов, а также оценки показателей безопасности на основе построенной когнитивной модели. Указанная процедура продемонстрирована на конкретном примере. Анализ уровня обеспечения информационной безопасности является важной составляющей проблемы обеспечения и даже повышения эффективности функционирования объекта защиты. Существующие методики оценки уровня безопасности чаще всего опираются на использование экспертных методов непосредственно для оценки показателей, что даже для относительно не сложных объектов и систем обработки данных дает достаточно приблизительные оценки ввиду наличия достаточно большого числа неопределенных и случайных факторов. С целью повышения качества оценок предлагается уточнить процесс формирования угроз разных типов на основе построения когнитивных моделей, описывающих зависимость рассматриваемой угрозы от факторов, способных оказать значимое влияние на показатели информационной безопасности.

Ключевые слова: безопасность информации, когнитивная модель, сопутствующие факторы, гарантированные, экстремальные и средние оценки показателей, оценка степени влияния факторов на угрозы.

ASSESSMENT OF THE IMPACT OF CONFOUNDING FACTORS IN THE PERFORMANCE INFORMATION SECURITY

Sh.G. Magomedov

Institute of Integrated Security and Special Instrumentation
Moscow Technological University (MIREA),
Moscow, 107996 Russia
@Corresponding author e-mail: msgg@list.ru

The paper considers the problem of improving the reliability of estimates of indicators providing information-without danger on the basis of constructing cognitive models related factors are associated with the process of formation and development of various types of information security threats. There are new types of assessments of safety performance to ensure a certain guaranteed level of the range of possible values of the index, which provides a more responsive and more accurate assessment of safety performance. Formed procedure for constructing cognitive models related factors, as well as evaluation of safety performance based on the cognitive model built. This procedure is demonstrated by a specific example.

Problem analysis of the level of information security is an important component of the problem and ensure even improve the functioning of the object of protection. However, existing methods of assessing the safety level often rely on the use of expert methods for direct assessment of information security indicators that have relatively less complex objects and data systems makes it quite rough estimates due to the availability of a sufficiently large number of uncertain and random factors. Here to solve the problem of improvement of quality evaluation is proposed to clarify the process of formation of various types of threats on the basis of the construction of cognitive models describing the dependence of the considered threats to a variety of factors that can have a significant effect on the consideration of information without the threat-risk.

Keywords: information security, cognitive model, related factors, guaranteed, extreme and average estimates of indicators, assessment of the degree of influence of factors on the threat.

1. Формирование значений исходных показателей, связанных с безопасностью

Существующие процедуры и методики оценки показателей информационной безопасности обычно опираются либо на усредненные значения исходных характеристик, определяющих состояние информационной безопасности на объекте защиты, либо на их экстремальные значения, особенно в случае критических систем безопасности. В первом случае получающиеся конечные оценки показателей безопасности носят усредненный характер. Указанный подход не может обеспечить адекватности поведения системы защиты в случае появления больших всплесков значений отдельных факторов, способных оказать значимое влияние на процессы возникновения атак и противодействия им: назовем эти факторы сопутствующими. При использовании экстремальных показателей конечные оценки показателей безопасности нередко бывают избыточными и порождают существенные дополнительные затраты, которые мало влияют на изменение уровня обеспечения безопасности. Назовем эти показатели целевыми, поскольку они предназначены и востребованы как параметры, используемые в процессе анализа состояния системы безопасности и формирования политики безопасности, при выборе варианта совершенствования системы безопасности, построении интегральных характеристик систем обеспечения информационной безопасности, при оптимизации структуры построения и технологии функционирования системы безопасности.

Таким образом, оба описанных выше подхода (на основе средних и экстремальных значений) к выбору целевых показателей имеют серьезные недостатки: имеет место либо недооценка уровня опасности, либо избыточность и связанные с ней дополнительные затраты, которые тем значимее, чем больше разница между средними и экстремальными значениями показателей безопасности.

Проиллюстрируем этот тезис примерами.

Пример 1. Предположим, что в локальной сети организации обрабатывается информация ограниченного доступа. Тогда необходимо обеспечить физическую защиту поме-

щений (входных дверей, окон и др. – сопутствующие факторы), где эта информация обрабатывается. Требования по степени защиты помещений зависят от оценки вероятности нарушения требований по информационной безопасности. Оценки этой вероятности находятся преимущественно на уровне их средних значений по всем узлам сети, однако в определенные промежутки времени возможно появление информации особой важности. Тогда принятие мер по усилению системы физической защиты помещений на основе средних значений может оказаться недостаточным для тех помещений и ситуаций, где и когда будет обрабатываться указанная информация. Принятие же мер повышенной защиты помещений может потребовать значительных средств.

Пример 2. Пусть в процессе обработки данных участвует определенный штат сотрудников, имеющих одинаковые права доступа к закрытой информации. Тогда при построении системы безопасности (например, при построении модели злоумышленника) можно опираться на средние значения возможной опасности, исходящей от каждого из сотрудников (они рассматриваются как сопутствующий фактор обеспечения безопасности). Однако среди прочих может оказаться сотрудник, который с существенно большей вероятностью, чем среднее значение, способен совершить злоумышленное деяние. Следовательно, модель злоумышленника, использующая средние значения при построении системы безопасности, может оказаться неспособной адекватно противостоять этому злоумышленнику. Использование же экстремальных значений указанной вероятности может потребовать не только дополнительных затрат, но приведет к построению модели злоумышленника, которую нельзя будет использовать для выявления возможных источников злоумышленных атак среди персонала.

Приведенные примеры показывают, что с точки зрения повышения эффективности системы обеспечения информационной безопасности целесообразно использовать адаптивные оценки отдельных факторов, если имеется такая возможность. Если же ее нет, например, вследствие большого числа сопутствующих факторов, то в качестве целевых показателей предлагаются величины, равные сумме среднего значения этого фактора и его среднеквадратического отклонения, по аналогии с методами стохастической оптимизации [1].

Пусть p – оцениваемый целевой параметр системы, имеющий абсолютное измерение (например, средняя величина промежутка времени до ближайшей атаки на информационные ресурсы, величина ожидаемого ущерба); $p_1, p_2, \ldots, p_n$ – набор статистических наблюдений либо экспертных данных по параметру p, где n – число наблюдений или экспертных оценок. Тогда средние значения $p_{ср}$ целевого показателя p и его экстремальное значение $p_э$ равны, соответственно

$$p_{ср} = \frac{1}{n}\sum_{i=1}^{n} p_i \ , \ \ p_э = \max\{p_i; 1 \le i \le n\}$$

Вместо $p_{ср}$ и $p_э$ предлагается использовать значение $p_г$, в определенной степени дающее гарантию учета и значительной части всплесков значений параметра p, которое равно:

$$p_г = p_{ср} + \sigma_p \, , \ \sigma_p = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(p_i - p_{ср})^2} \qquad (1)$$

В случае относительных (безразмерных) показателей (например, вероятности $P_{усп}$

успешного противодействия атаке либо желаемого изменения сопутствующего фактора в течение заданного регламентного промежутка времени T) использование соотношения (1) неприемлемо, поскольку при определенных значениях p_i вероятность $P_{усп}$ может оказаться больше единицы. Для получения при относительных целевых показателях оценки, аналогичной (1), можно воспользоваться следующей процедурой. При оценке вероятности $P_{усп}$ предполагают, что имеет место следующая зависимость указанной вероятности от интенсивности λ_p атак:

$$P_{усп} = C(\lambda_p, T)\cdot\exp\{-K(\lambda_p, T)\,\lambda_p T\}, \qquad (2)$$

где $C(\lambda_p, T)$ и $K(\lambda_p, T)$ − некоторые ограниченные функции.

Так как при отсутствии атак (то есть при $\lambda_p = 0$), видимо, $P_{усп} = 1$, то из (2) следует, что $C(\lambda_p, T) = 1$. Функция $K(\lambda_p, T)$, вообще говоря, не является константой: она зависит от параметров конкретных средств противодействия, используемых в системе. Однако, как правило, при проведении общего анализа системы, не привязанной к конкретным средствам противодействия, принимают $K(\lambda_p, T) = K$ постоянным. Отметим, что K характеризует степень эффективности использования имеющихся средств противодействия атаке на информационные ресурсы или другие ценности. Предположив, что соотношение (2) справедливо для каждого отдельного наблюдения P_i ($i = \overline{1;n}$), из (2) получаем:

$$\lambda_{Pi} = -\frac{1}{K\,T}\ln(P_i)$$

По аналогии с (1), заменяя текущие интенсивности λ_{Pi} их гарантированными оценками $\lambda_{Pг} = \overline{\lambda_P} + \sigma_\lambda$, получаем следующую гарантированную оценку $P_г$ для вероятности успешного противодействия атакам:

$$P_г = \exp\{-K\,\lambda_{Pг}T\},\ \lambda_{Pг} = \overline{\lambda_P} + \sigma_\lambda,\ \overline{\lambda_P} = \frac{1}{n}\sum_{i=1}^{n}\lambda_{Pi},\ \sigma_\lambda = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\lambda_{Pi} - \overline{\lambda_P})^2} \qquad (3)$$

Отметим, что в оценках (1) и (3) для увеличения доли атак, которые успешно нейтрализованы с помощью имеющихся средств противодействия, значения вторых слагаемых σ_P и σ_λ могут быть увеличены путем введения множителей, больших единицы, то есть использования слагаемых $\mu\sigma_p$ и $\mu\sigma_2$, $\mu > 1$ – константа. В частности, при $\mu = 3$ и предположении о нормальном законе распределения оценок P_i по закону «трех сигма» для нормального закона [2] выводим, что для 99.7% всех атак значения вероятностей успешного противодействия этим атакам будут меньше $P_г$.

2. Формирование когнитивной модели влияния сопутствующих факторов на угрозы безопасности

Систематические исследования, опирающиеся на анализ угроз информационной безопасности и основанные на построении когнитивных моделей, как показывает рассмотрение литературных данных, практически не проводились. Близкой по идеологии моделирования процесса формирования и развития угроз является монография [3]. Отметим также публикации [4−7], где рассматриваются сетевые модели развития угроз.

В то же время, как нам представляется, факторы, которые оказывают и окажут влияние на процесс обеспечения безопасности объектов защиты, могут быть описаны при-

менительно к каждому типу угроз с помощью когнитивной модели, то есть взвешенного ориентированного графа, у которого веса ребер векторные, а веса вершин отсутствуют. Конечные вершины графа соответствуют угрозам, для анализа которых и строится граф, а все остальные вершины находятся под определенным фактором. Под фактором здесь понимается определенное состояние элементов, связанных с процессом обеспечения безопасности на объекте защиты.

Для более детального пояснения сформулированного выше тезиса приведем пример. Пусть в многоэтажном здании, где расположен объект защиты, в результате аварии или злоумышленного действия прорвало трубы отопления или водопроводные трубы, по которым подается горячая и холодная вода в здание, или нарушена герметичность крыши и потолочных перекрытий, в результате чего здание заливает водой. Поступающая вода массированно затапливает нижние этажи. Не исключена возможность короткого замыкания в системе электроснабжения, в результате чего возник пожар. Сотрудники и другие лица, находившиеся в здании, стали активно его покидать. Воспользовавшись чрезвычайной ситуацией, злоумышленник через один из работающих компьютеров проник в информационную систему организации и совершил злоумышленное действие: или похитил определенную ценную информацию, или изменил информацию, или уничтожил эту информацию, отдельные программные и аппаратные системы обработки данных, системы обеспечения безопасности, или вынес один из носителей информации, где хранились ценные данные. Описанные ситуации могут быть представлены в виде графа, приведенного на рис. 1.

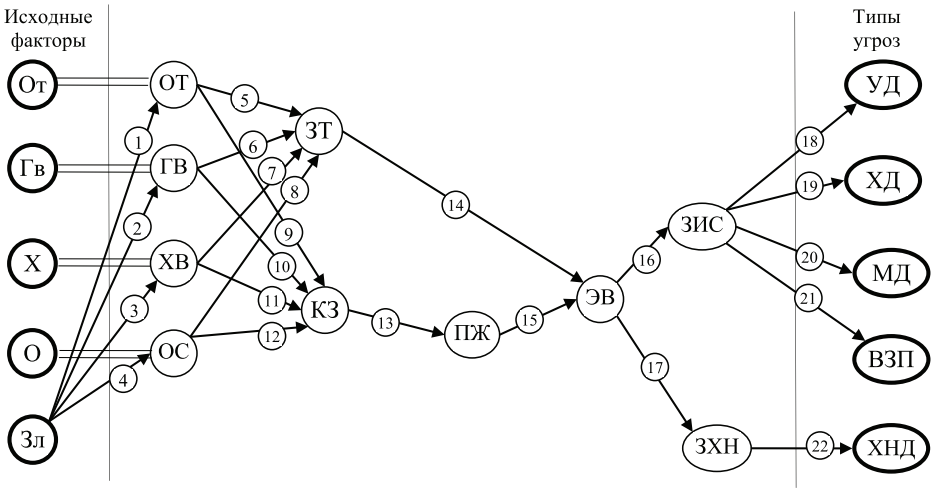

Рис. 1. Пример фрагмента графа сценариев, описывающего взаимосвязь сопутствующих факторов и угроз: ОТ (От) – нарушение герметичности системы отопления; ГВ (Гв) – нарушение герметичности системы подачи горячей воды; ХВ (Хв) – нарушение герметичности системы подачи холодной воды; ОС (Ос) – нарушение герметичности крыши и верхних перекрытий; Зл – злоумышленное действие; ЗТ – затопление помещений; КЗ – короткое замыкание в системе электропитания; ПЖ – пожар, вызванный коротким замыканием в системе электропитания; ЭВ – экстренная эвакуация персонала и других лиц, находящихся в здании; ЗИС – злоумышленное хищение данных из информационной системы объекта защиты; ЗХН – физическое хищение носителей информации; УД, ХД – уничтожение или хищение части или всех данных; МД – модификация данных на объекте защиты; ВЗП – внедрение злоумышленных программ; ХНД – физическое хищение носителей данных.

В указанных сценариях развития событий прорыв отопления (водоснабжения), затопление помещений, короткое замыкание, пожар, экстренная эвакуация всех субъектов из здания – это сопутствующие факторы; хищение, уничтожение, модификация данных, внедрение злоумышленных программ, физическое хищение носителей данных – это угрозы, переросшие в атаки.

В качестве весовых коэффициентов для каждого ребра графа может быть выбран набор из следующих трех параметров:

- вероятность реализации перехода от одного фактора к другому (то есть перехода состояний);
- среднее время реализации этого перехода;
- ожидаемый ущерб.

Отметим, что значения указанных параметров для каждой из перечисленных угроз могут быть разными. Поэтому необходимо, например, разделить граф на несколько экземпляров в соответствии с числом рассматриваемых угроз и соответствующими этой угрозе весовыми параметрами каждого ребра, т.е. для каждой угрозы составить свой граф. Можно также усложнить весовые коэффициенты, добавив в качестве нулевого параметра код одной из рассматриваемых угроз и представив для каждой из угроз свой набор значений остальных параметров. В таком случае каждый весовой коэффициент содержит k скалярных параметров, где k – число рассматриваемых угроз. В приведенном выше случае (рис. 1) таких угроз не меньше пяти:

1) хищение данных;
2) уничтожение данных;
3) модификация данных;
4) внедрение злоумышленных программ;
5) физическое хищение носителей данных или информации.

3. Оценка показателей угроз на основе когнитивной модели влияния

Оценим показатели угроз на основе построенной когнитивной модели влияния сопутствующих факторов на угрозы. Для простоты ограничимся только одним (но наиболее важным) скалярным показателем – вероятностью проявления одной из перечисленных выше угроз. Прежде всего, важно оценить вероятности проявления факторов-источников, то есть возникновения соответствующих им событий, а также вероятности соответствующих переходов, отображаемых на рис. 1, для всех пяти типов угроз. Вероятности переходов есть фактически вероятности того, что фактор, соответствующий началу ребра, повлечет проявление фактора, являющегося концом ребра. Указанные вероятности существенно зависят от специфических особенностей конкретного объекта защиты. В приводимом ниже примере в качестве объекта защиты выбрано серверное помещение одного из вузов, и на этом примере продемонстрирована предлагаемая процедура оценки вероятности угроз. На сервере расположена, в частности, биллинговая система с паролями всех пользователей локальной сети вуза, что является закрытой информацией. Кроме того, повреждение программного обеспечения сервера явилось целью злоумышленных атак, чтобы, допустим, парализовать доступ к сети при проведении различных контрольных мероприятий по оценке знаний студентов [8].

Поскольку не все эксперты знакомы со специфическими особенностями объекта защиты, при том, что необходимо получать качественные оценки вероятностей переходов, целесообразно сначала организовать обсуждение в виде «круглого стола». Речь идет о

совместном обсуждении проблемы экспертами, на котором, в частности, должны быть раскрыты возможные способы и механизмы влияния сопутствующих факторов на процесс формирования угрозы в соответствии с диаграммой на рис.1. Полученная в ходе обсуждения информация позволит экспертам более содержательно и полно оценить влияние рассматриваемого фактора на процесс зарождения угрозы с учетом особенностей объекта защиты [9−11].

Итак, было привлечено пять экспертов, двое − из системы образования, специалистов по информационной безопасности, и трое – лица, непосредственно связанные с процессом обеспечения информационной безопасности. Оценки переходов проводили по стобалльной шкале {0; 100}, считая, что значение 100 соответствует ситуации, когда для данного ребра предшествующий фактор (начало ребра) всегда порождает последующий фактор (конец ребра). Полученные оценки были разделены на 100, переведены в шкалу {0; 1} изменения вероятностей. После обработки результатов, в том числе и на основе формулы (3), получены результаты, суммированные в табл. 1. Первые четыре ребра с номерами 1, 2, 3, 4 соответствуют условным событиям: вероятности нарушения систем отопления, горячего водоснабжения, целостности крыши и верхних перекрытий, соответственно, при условии, что какое-то из перечисленных событий произошло.

Таблица 1. Экспертные оценки вероятностей взаимовлияния сопутствующих факторов в процессе формирования угроз (%)

№	Ребро графа	Ожидаемые типы угроз									
		1. Хищение данных		2. Уничтожение данных		3. Модификация данных		4. Внедрение злоумышленных программ		5. Хищение носителей	
		$P_{усп}$	$P_{г}$	$P_{усп}$	$P_{г}$	$P_{усп}$	$P_{г}$	$P_{усп}$	$P_{г}$	$P_{усп}$	$P_{г}$
1	2	3	4	5	6	7	8	9	10	11	12
1	(Зл;ОТ)	35.4	38.9	42.4	47.5	35.4	38.9	35.4	38.9	34.8	37.7
2	(Зл;ГВ)	32.1	33.4	20.7	21.4	32.1	33.4	32.1	33.4	29.3	32.1
3	(Зл;ХВ)	33.2	34.8	31.5	34.3	33.2	34.8	33.2	34.8	30.7	34.3
4	(Зл;ОС)	11.6	14.2	3.40	3.90	11.6	14.2	11.6	14.2	3.60	4.10
5	(ОТ;ЗТ)	84.7	86.0	84.7	86.0	84.7	86.0	84.7	86.0	84.7	86.0
6	(ГВ;ЗТ)	43.1	46.2	43.1	46.2	43.1	46.2	43.1	46.2	43.1	46.2
7	(ХВ;ЗТ)	41.9	44.5	41.9	44.5	41.9	44.5	41.9	44.5	41.9	44.5
8	(ОС;ЗТ)	2,.0	3.00	2.60	3.00	2.60	3.00	2.60	3.00	2.60	3.00
9	(ОТ;КЗ)	77.4	78.2	77.4	78.2	77.4	78.2	77.4	78.2	77.4	78.2
10	(ГВ;КЗ)	35.0	38.2	35.0	38.2	35.0	38.2	35.0	38.2	35.0	38.2
11	(ХВ;КЗ)	36.1	37.4	36.1	37.4	36.1	37.4	36.1	37.4	36.1	37.4
12	(ОС;КЗ)	2.10	2.40	2.10	2.40	2.10	2.40	2.10	2.40	2.10	2.40
13	(КЗ;ПЖ)	28.6	30.1	28.6	30.1	28.6	30.1	28.6	30.1	28.6	30.1
14	(ЗТ;ЭВ)	56.8	58.0	56.8	58.0	56.8	58.0	56.8	58.0	56.8	58.0
15	(ПЖ;ЭВ)	92.4	95.8	92.4	95.8	92.4	95.8	92.4	95.8	92.4	95.8
16	(ЗВ;ЗИС)	53.6	63.1	53.6	63.1	53.6	63.1	53.6	63.1	53.6	63.1
17	(ЗВ;ЗХН)	32.2	33.7	32.2	33.7	32.2	33.7	32.2	33.7	32.2	33.7
18	(ЗИС;УД)	45.3	47.4								
19	(ЗИС;ХД)			69.3	72.3						
20	(ЗИС;МД)					51.8	53.4				
21	(ЗИС;ВЗП)							32.6	33.9		
22	(ЗХН;ХНД)									88.6	91.0

При заполнении строк с 5-ой по 17-ую, т.е. при оценке вероятностей по внутренним ребрам диаграммы, эксперты исходили из того, что если все данные хранятся на сервере, тогда, с точки зрения совершения любых злоумышленных действий, вероятности внутренних переходов равноопасны, а, значит, равны. Поэтому значения в ячейках на пересечении строк с 5-ой по 17-ую и столбцов (5, 6), (7, 8), (9, 10), (11, 12) повторяют соответствующие значения в столбцах (3, 4). В последних пяти строках имеются незаполненные ячейки: по всей видимости, злоумышленник, который намеревался совершить, например, хищение данных или любое другое действие, в момент непосредственного совершения действия не будет менять тип действия (например, хищение – на другое действие).

На основе построенной табл. 1 формируются две матрицы $A_{Усп}$ и $A_{г}$, состоящие из 22 строк (по количеству ребер в графе когнитивной модели) и 5 столбцов (по количеству показателей угроз). На пересечении *i*-ой строки и *j*-ого столбца матрицы $A_{Усп}$ и $A_{г}$ записываются, соответственно, полученные экспертные оценки $P_{Усп}$ и $P_{г}$ степени влияния *i*-го по порядку сопутствующего фактора на *j*-ый тип угроз.

С целью получения единой интегральной оценки вероятности проявления хотя бы одной из угроз в течение регламентируемого промежутка времени необходимо вначале провести оценку степени актуальности отдельных типов угроз для рассматриваемого объекта защиты. Так, например, если на объекте защиты хранится особо важная закрытая информация, то угроза ее хищения опаснее угрозы уничтожения. Если же объект защиты связан с опасным технологическим процессом, то, наоборот, опасность уничтожения текущей информации, связанной с технологическим процессом, может оказаться важнее угрозы ее хищения. Проведем оценку указанной вероятности применительно к рассматриваемому в качестве примера объекту на основе использования экспертного оценивания без предварительного обсуждения с привлечением тех же экспертов, поскольку специфические особенности объекта защиты уже были ранее рассмотрены экспертами. Оценки, как и в случае табл. 1, предлагается проводить по стобалльной шкале, а затем полученные оценки нормировать так, чтобы сумма всех вероятностей равнялась единице, значит, необходимо разделить каждую из пяти оценок на их сумму. В качестве результатов оценивания взяты средние значения полученных оценок. Полученные данные приведены в табл. 2.

Таблица 2. Оценки важности отдельных типов угроз по шкале [0; 1]

Наименование угроз	Хищение данных	Уничтожение данных	Модификация данных	Внедрение злоумышленных программ	Хищение носителей
Результирующие оценки, %	55	35	45	25	10
Результирующие оценки, нормированные	0.32	0.21	0.26	0.15	0.06

На основе оценок, приведенных в табл. 1 и 2, можно вычислить ряд важных характеристик безопасности. В частности, оценить влияние каждого из сопутствующих факторов на показатели угроз каждого типа, либо на показатели угроз в целом. Для примера опишем на основе рассмотренного ранее объекта (серверное помещение вуза) процедуру влияния исходного факторов ОТ («нарушение целостности системы отопления») на вероятность хищения или модификации данных.

На основе когнитивной модели опишем вначале возможные маршруты от фактора ОТ до угроз ХД и МД: 1) ОТ → 5 → 14 →16 → 19 → ХД; 2) ОТ → 9 → 13 → 15 → 16 → 19 → ХД; 3) ОТ → 5 → 14 →16 →20 → МД; 4) ОТ →9 → 13 → 15 → 16 →20 → МД.

Тогда на основе графа влияния (рис. 1) выписывается следующее выражение для вероятности хищения или модификации данных по причине фактора ОТ:

$$q_{OT}^{ХД,МД} = (v_{ХД} p_{19} + v_{МД} p_{20}) \cdot (p_{16}^{ХД} \cdot p_{14}^{ХД} \cdot p_{5}^{ХД} + p_{16}^{МД} p_{15}^{МД} \cdot p_{13}^{МД} \cdot p_{9}^{МД}) \cdot p_{OT} \quad (4)$$

Значения всех используемых в (4) вероятностей p_{19}, p_{20}, $p_i^{ХД}$ и $p_i^{МД}$ приведены в табл. 1 (после деления их на 100); предлагается использовать оценки гарантированного уровня $P_г$. Значения коэффициентов важности $v_{ХД}$ и $v_{МД}$ приведены в табл. 2. Значение вероятности P_{OT} получается из табл. 1 после нормировки по формуле:

$$p_{OT} = \frac{p_1}{p_1 + p_2 + p_3 + p_4} = \frac{38{,}9}{38{,}9 + 33{,}4 + 34{,}8 + 14{,}2} = 0{,}32$$

Тогда на основе (4) выводим:

$$q_{OT}^{ХД,МД} = (0{,}32 \cdot 0{,}723 + 0{,}26 \cdot 0{,}534) \cdot (0{,}631 \cdot 0{,}58 \cdot 0{,}86 + 0{,}631 \cdot 0{,}958 \cdot 0{,}301 \cdot 0{,}782) \cdot 0{,}32 = 0{,}0496$$

Аналогичные оценки можно получить и для других исходных и других сопутствующих факторов. Сравнение полученных вероятностей для различных факторов позволит упорядочить их по степени важности для каждого типа угроз и для безопасности в целом, что явится основой для распределения ресурсов на повышение безопасности объекта защиты.

Задачу анализа показателей безопасности на основе построения когнитивной модели сопутствующих факторов автор предполагает рассмотреть в последующих своих работах.

Заключение

В работе рассмотрена задача повышения достоверности оценок показателей информационной безопасности на основе построения когнитивных моделей сопутствующих факторов при формировании и развитии различных типов угроз. Введены новые типы оценок показателей безопасности, обеспечивающие определенный гарантированный уровень интервала возможных значений показателя. Сформирована процедура построения когнитивных моделей сопутствующих факторов, а также оценки показателей безопасности на основе этих моделей. Указанная процедура продемонстрирована на конкретном примере.

Литература:

1. Ермольев Ю.М. Методы стохастического программирования. М.: Главная редакция физ.-мат. лит-ры изд-ва «Наука», 1976. 340 с.

2. Гмурман В.Е. Теория вероятностей и математическая статистика. М.: Высшая школа, 2003. 474 с.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн. Кн.1. М.: Энергоатомиздат, 1994 . 400 с.

4. Гайдамакин Н.А Теоретические основы компьютерной безопасности. Учебно-методический комплекс. Екатеринбург, Уральский гос. ун-т, 2008. 212 с.

5. Васильев А. Е., Третьяков О. П. Графовая модель контроля и анализа состояния защиты информации // Известия Южного федерального университета. Технические науки.

2013. № 7 (144). С. 156–160.

6. Кальнов М.И., Лаптев В.В., Попов Г.А. Защита сетевых коммуникаций в распределенной образовательной системе на основе интенсивной смены ключей шифрования // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2012. № 2. С. 94–98.

7 Магомедов Ш.Г. Математическое моделирование охранных действий на объекте защиты // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2016. № 1. С. 70–80.

8. Магомедов Ш.Г., Морозова Т.Ю., Акимов Д.А. Обеспечение безопасности передачи данных в вычислительных сетях на основе использования систем остаточных классов // Проблемы информационной безопасности. Компьютерные системы. 2016. Т. 3. С.43–47.

9. Зайцев А.С., Малюк А.А. Выявление потенциального инсайдера с использованием моделей классификации // Проблемы информационной безопасности. Компьютерные системы. 2016. Т. 3. С. 34–42.

10. Попов Г.А., Попова Е.А., Мельников А.В. Анализ параметров информационной безопасности автоматизированных систем на основе использования уточненных экспертных оценок // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2015. № 1. С. 33–39.

11. Макаров М.И., Медведев А.А., Савельев Ю.М., Макаров В.М. Автоматизированная система обеспечения эксплуатации ракетно-космической техники космодрома. Решаемые задачи и перспективы развития // Российский технологический журнал. 2016. Т. 4. № 5. С. 46–55.