УДК 004.056

Б.И. Ефимов, Р.Т. Файзуллин

Устойчивость объективного решения экспертов при воздействии угроз по блокированию информации в системах принятия решений с привлечением экспертов

Предложено решение задачи вычисления вероятности принятия ложного решения в системах принятия решения с привлечением экспертов под воздействием угроз информационной безопасности, направленных на блокирование ответов экспертов.

Ключевые слова: информационная безопасность, системы принятия решений, эксперты, угрозы, теория вероятностей.

В настоящее время одними из наиболее динамично развивающихся информационных систем являются системы принятия управленческих решений. Одним из видов указанных систем являются системы, построенные на использовании знаний экспертов-аналитиков.

Данные системы могут использоваться во многих сферах жизнедеятельности. В ряде источников описано применение систем принятия управленческих решений в том числе и для эффективного регулирования уровня информационной безопасности. Так, в [1] приводится общая методология проведения так называемого SWOT-анализа, который может применяться в практике организаций по усилению безопасности; описаны сильные и слабые стороны данного вида анализа.

В настоящей статье рассмотрены некоторые частные вопросы обеспечения информационной безопасности самих систем принятия решений. Как показано в [2], обеспечение безопасности указанных систем является одной из важных задач при их разработке.

Для информационных систем в целом в [3] приводится классификация объектов угроз, позволяющая определить ресурсы, подлежащие защите. В перечень объектов включены: информация; элементы информационной системы (программные и аппаратные) и их настройки; элементы системы защиты (программные и аппаратные) и их настройки.

Угрозы безопасности систем принятия решений с привлечением экспертов в основном могут быть направлены на следующие объекты [4]: экспертов, принимающих участие в опросе, узлы коммутации, линии связи, лицо, принимающее решение.

Виды воздействий на объекты сети могут быть как преднамеренными, т.е. осуществляемыми злоумышленником, так и случайными, обусловленными отказами оборудования, программ и каналов связи. Преднамеренные угрозы направлены, в конечном итоге, на принятие «нужного» для злоумышленника решения. Отказы оборудования носят случайный, непредсказуемый характер и могут повлиять на принятие решения в пользу любой из существующих альтернатив.

В общем случае основной целью применения средств защиты информации является предотвращение ущерба, т.е. предотвращение реализации угроз информационной безопасности [5]. Однако в системах принятия решения для лица, принимающего решение, значимым является лишь конечный результат – выбор экспертами одной из предложенных альтернатив. Как показано в [2], система защиты информации должна быть построена таким образом, чтобы выполнялась единственная задача – решение, принимаемое экспертами при условии реализации возможных угроз, должно быть таким же, что и решение, которое было бы принято системой при полном отсутствии угроз информационной безопасности. Значение «перевеса», с которым побеждает одна альтернатива над другой, а также процентное распределение голосов экспертов между альтернативами не имеют никакого значения.

В [6] подробно рассмотрено поведение систем принятия решений с привлечением экспертов под воздействием угроз информационной безопасности по изменению ответов экспертов в пользу одной из альтернатив.

В данной статье рассмотрим частный случай, когда угрозы по изменению ответов экспертов отсутствуют, но существуют угрозы по блокированию ответов экспертов.

Исходные положения. Пусть опрос экспертов проводится по выбору одной из двух альтернатив: «0» и «1», общее количество экспертов, принимающих участие в голосовании, – m, количество экспертов, проголосовавших за альтернативу «1», – n.

Из всех возможных вариантов голосования экспертов рассмотрим только случаи голосования, когда количество экспертов, проголосовавших за альтернативу «1», равно или превышает количество экспертов, проголосовавших за альтернативу «0» ($n \geq m/2$), и определим, как угрозы информационной безопасности по блокированию ответов экспертов могут привести к выбору лицом, принимающим решение (ЛПР), другой альтернативы (альтернативы «0»).

Будем считать также, что вероятности блокирования ответов экспертов $P_{bloc\,i}$ одинаковы для всех экспертов.

Возможные варианты по выбору альтернативы ЛПР

Answ1 – количество дошедших до ЛПР ответов за альтернативу «1» больше, чем за альтернативу «0»; лицом, принимающим решение, выбирается альтернатива «1»;

AnswEq – количество дошедших до ЛПР ответов за альтернативы «1» и «0» равно, назначается повторное голосование;

Answ0 – количество дошедших до ЛПР ответов за альтернативу «1» меньше, чем за альтернативу «0»; лицом, принимающим решение, выбирается альтернатива «0».

Условия возникновения событий AnswEq, Answ0

Событие AnswEq возникает в случае, если ответов экспертов, отданных за альтернативу «1», блокируется ровно на $(2n - m)$ больше, чем ответов экспертов, отданных за альтернативу «0».

Событие Answ0 возникает в случае, если разница между количеством блокируемых ответов экспертов, проголосовавших за альтернативу «1», и количеством блокируемых ответов экспертов, проголосовавших за альтернативу «0», больше чем $(2n - m)$.

Вероятности наступления событий

Вероятность наступления события AnswEq:

$$P(AnswEq) = \sum_{k=0}^{m-n-1} P(B_k) \cdot P(D_{2n-m+k}), \tag{1}$$

где $P(B_k)$ – вероятность блокирования ровно k ответов экспертов из $(m–n)$ экспертов, проголосовавших за альтернативу «0»; $P(D_{2n-m+k})$ – вероятность блокирования ровно $(2\ m–n\ +k)$ ответов экспертов из n экспертов, проголосовавших за альтернативу «1».

$$P(B_k) = (P_{bloc})^k \cdot (1 - P_{bloc})^{(m-n-k)} \cdot C_{m-n}^k, \tag{2}$$

где C_{m-n}^k – число сочетаний из $m–n$ по k;

$$C_{m-n}^k = \frac{(m-n)!}{k! \cdot (m-n-k)!},$$

$$P(D_{2n-m+k}) = (P_{bloc})^{(2n-m+k)} \cdot (1 - P_{bloc})^{(n-(2n-m+k))} \cdot C_n^{2n-m+k}, \tag{3}$$

где C_n^{2n-m+k} – число сочетаний из n по $(2n - m + k)$;

$$C_n^{2n-m+k} = \frac{n!}{(2n-m+k)! \cdot (m-n-k)!}.$$

Подставляем в (1) формулы (2), (3):

$$P(AnswEq) = \sum_{k=0}^{m-n-1} \left((P_{bloc})^{(2n-m+2k)} (1 - P_{bloc})^{2(m-n-k)} \frac{n! \cdot (m-n)!}{k! \cdot (2n-m+k)! \cdot ((m-n-k)!)^2} \right). \tag{4}$$

Вероятность наступления события Answ0:

$$P(Answ0) = \sum_{k=0}^{m-n-1} P(E_k), \tag{5}$$

где $P(E_k)$ – вероятность появления события E_k.

Событие E_k – для конкретного значения k (количества заблокированных ответов экспертов, проголосовавших за альтернативу «0» ($k = \{0, 1, \ldots m - n - 1\}$), было заблокировано ответов экспертов, проголосовавших за альтернативу «1», более чем на $(2n - m)$ превышающее k ($l = \{2n - m+k+1, 2n–m+k+2, \ldots n\}$).

$$P(E_k) = P(B_k) \cdot P(F_{2n-m+k+1}), \quad (6)$$

где $P(B_k)$ – вероятность блокирования ровно k ответов экспертов из (m–n) экспертов, проголосовавших за альтернативу «0»; $P(F_{2n-m+k+1})$ – вероятность блокирования от ($2n$–m+k+1) до n ответов экспертов, проголосовавших за альтернативу «1».

$$P(F_{2n-m+k+1}) = \sum_{l=2n-m+k+1}^{n} P(D_l), \quad (7)$$

где $P(D_l)$ – вероятность блокирования ровно l ответов экспертов из n экспертов, проголосовавших за альтернативу «1».

$$P(B_k) = (P_{bloc})^k \cdot (1-P_{bloc})^{(m-n-k)} \cdot C_{m-n}^k, \quad (8)$$

где C_{m-n}^k – число сочетаний из m–n по k;

$$C_{m-n}^k = \frac{(m-n)!}{k! \cdot (m-n-k)!},$$

$$P(D_l) = (P_{bloc})^l \cdot (1-P_{bloc})^{(n-l)} \cdot C_n^l, \quad (9)$$

где C_n^l – число сочетаний из n по l;

$$C_n^l = \frac{n!}{l! \cdot (n-l)!}.$$

Подставляем в (6) формулу (7), полученную формулу подставляем в формулу (5):

$$P(Answ0) = \sum_{k=0}^{m-n-1} (P(B_k) \cdot \sum_{l=2n-m+k+1}^{n} P(D_l)). \quad (10)$$

В формулу (10) подставляем формулы (8), (9):

$$P(Answ0) = \sum_{k=0}^{m-n-1} \left((P_{bloc})^k \cdot (1-P_{bloc})^{(m-n-k)} \cdot \frac{(m-n)!}{k! \cdot (m-n-k)!} \cdot \sum_{l=2n-m+k+1}^{n} \left((P_{bloc})^l \cdot (1-P_{bloc})^{(n-l)} \cdot \frac{n!}{l! \cdot (n-l)!} \right) \right). \quad (11)$$

При возникновении события *AnswEq* должно назначаться повторное голосование до тех пор, пока не возникнет событие *Answ*1 или *Answ*0. При этом условная вероятность события *Answ*0 при условии, что произошло одно из этих событий, составляет:

$$P(Answ0 \mid Answ1 \cup Answ0) = \frac{P(Answ0)}{P(Answ1) + P(Answ0)}. \quad (12)$$

Необходимо отметить, что исключением является случай возникновения события *AnswEq*, когда угрозы ИБ отсутствуют и эксперты голосуют поровну за альтернативы «0» и «1». При дальнейшем описании указанный случай (n=m/2, m – четное) рассматриваться не будет.

Вероятность выбора альтернативы «0». Учитывая повторные голосования, назначаемые при возникновении события *AnswEq*, вычислим полные вероятности выбора альтернативы «0» (событие A0):

$$P(A0) = P(Answ0) + P(AnswEq) \cdot P(Answ0 \mid Answ1 \cup Answ0). \quad (13)$$

Вероятность события A0 – вероятность того, что действия злоумышленника приводят к изменению выбранной экспертами альтернативы.

Из формулы (13), используя формулу (12), получаем:

$$P(A0) = P(Answ0) + P(AnswEq) \cdot \frac{P(Answ0)}{P(Answ1) + P(Answ0)} = P(Answ0) \cdot (1 + \frac{P(AnswEq)}{P(Answ1) + P(Answ0)}). \quad (14)$$

Так как события *Answ*1, *AnswEq*, *Answ*0 образуют полную группу событий, получаем:

$$P(A0) = P(Answ0) \cdot (1 + \frac{P(AnswEq)}{1 - P(AnswEq)}) = \frac{P(Answ0)}{1 - P(AnswEq)}. \quad (15)$$

Вероятности $P(AnswEq)$, $P(Answ0)$ находятся по формулам (4), (11).

Программная реализация. Для вычисления вероятности события A0 в зависимости от вероятности блокирования ответов экспертов P_{bloc}, количества экспертов m и количества экспертов, проголосовавших за альтернативу «1», разработан модуль на языке программирования MATLAB.

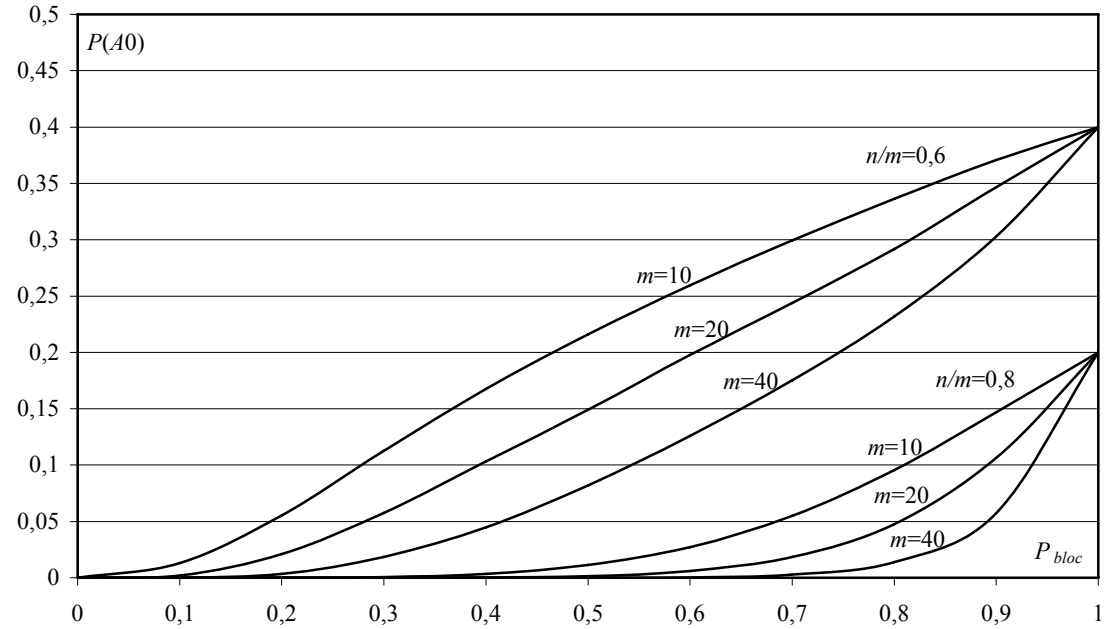

Рис. 1. Вероятность события $A0$ в зависимости от P_{blok} при разных значениях m и n/m

Результаты вычислений. На рис. 1 представлена зависимость вероятности $P(A0)$ от вероятности блокирования отдельного ответа эксперта P_{bloc} , при различных значениях количества экспертов m (m = {10, 20, 40}) и различных соотношениях ответов экспертов, поданных за альтернативы «0» и «1» (n/m = {0,6; 0,8}).

Из данного графика видно, что при $P_{bloc}\rightarrow 1$ значение вероятности $P(A0)$ стремится к значению доли экспертов, проголосовавших за альтернативу «0» ($1–n/m$), при любом значении m.

$$P_{bloc}\rightarrow 1;\ P(A0)\rightarrow 1–n/m.$$

То есть если доля экспертов, проголосовавших за альтернативу «0», равна ($1 – n/m$) и практически все ответы блокируются (кроме одного, так как нахождение $P(A0)$ при блокировании ответов всех экспертов не имеет смысла), то вероятность, что единственный незаблокированный ответ эксперта будет подан за альтернативу «0», также будет равна ($1 – n/m$).

Заключение. В статье показано, что так же, как и в случае воздействия угроз информационной безопасности, направленных на изменение ответов экспертов (подробно описано в [6]), при наличии угроз по блокированию ответов экспертов вероятность принятия ложного решения увеличивается при уменьшении относительного количества экспертов n/m, проголосовавших за альтернативу «1» (m – const, P_{bloc} – const).

При увеличении количества экспертов m, вероятность принятия ложного решения $P(A0)$ уменьшается при любых значениях вероятности блокирования ответов экспертов P_{bloc}, в отличие от случаев воздействия угроз по изменению ответов экспертов, при которых увеличение m приводит к уменьшению $P(A0)$ не при всех значениях P_{bloc}.

Таким образом, одним из способов повышения устойчивости объективного решения в системах принятия решений с привлечением экспертов при воздействии угроз по блокированию информации является увеличение числа экспертов.

Литература

1. Мицель А.А. Модель стратегического анализа информационной безопасности / А.А. Мицель, А.А. Шелупанов, С.С. Ерохин // Доклады ТУСУРа. – 2007. – № 2 (16). – С. 34–41.

2. Ефимов Б.И. Обеспечение информационной безопасности систем принятия решений с использованием теории графов / Б.И. Ефимов, Р.Т. Файзуллин // Динамика систем, механизмов и машин: матер. VII Междунар. науч.-техн. конф. – Омск: Изд-во ОмГТУ, 2009. – Кн. 1. – С. 280–284.

3. Ефимов Б.И. Применение алгоритмов теории графов для решения задач, связанных с обеспечением информационной безопасности в системах принятия решений // Системы управления и информационные технологии. – 2009. – № 1.3 (35). – С. 342–346.

4. Филькин К.Н. Информационно-управляющая система поддержки принятия решений при управлении информационной безопасностью территориально распределенной организацией / К.Н. Филькин, С.Н. Филькин, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 83–86.

5. Авсентьев О.С. Принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности / О.С. Авсентьев, В.В. Александров, Г.И. Рябинин, С.В. Скрыль, Р.В. Мещеряков // Доклады ТУСУРа. – 2008. – Т. 2. – № 1. – С. 135–136.

6. Ефимов Б.И. Вероятность принятия ложного решения под воздействием угроз информационной безопасности в системах принятия решений с привлечением экспертов / Б.И. Ефимов, Р.Т. Файзуллин // Доклады ТУСУРа. – 2013. – № 1 (27). – С. 69–74.

Ефимов Борис Игоревич
Аспирант каф. комплексной защиты информации
Омского государственного технического университета (ОмГТУ)
Тел.: 8 (381-2) 79-94-22
Эл. почта: b_efimov@mail.ru

Файзуллин Рашит Тагирович
Д-р техн. наук, профессор, зав. каф. комплексной защиты информации ОмГТУ
Тел.: 8 (381-2) 21-77-02
Эл. почта: r.t.faizullin@mail.ru

Efimov B.I., Faizullin R.T.

Stability of the objective decision of experts at influence of threats on blocking of information in decision-making systems with experts

The solution of a problem of calculation of probability of adoption of the false decision in decision-making systems with involvement of experts as a result of the threats of information security directed on blocking of answers of experts is proposed.

Keywords: information security, decision-making systems, experts, threats, probability theory.
