УДК 004.056

Б.И. Ефимов, Р.Т. Файзуллин

Вероятность принятия ложного решения под воздействием угроз информационной безопасности 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 изменение ответов экспертов. Получены оценки, показывающие целесообразность или нецелесообразность увеличения количества экспертов для уменьшения влияния действий злоумышленника на принимаемое решение.

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

В любой сфере деятельности человека постоянно возникает огромное количество проблем, требующих принятия решений. Во многих случаях, особенно когда по принимаемому вопросу не наработана необходимая база первичных данных, оптимальным вариантом может являться использование экспертов-аналитиков. Для принятия сложных управленческих решений разработаны и математически описаны различные модели и методы [1, 2].

При разработке систем принятия решений с привлечением экспертов обеспечение информационной безопасности является одной из важных задач. Вопросы информационной безопасности указанных систем подробно изложены в [3, 4].

В соответствии с [4] угрозы безопасности систем принятия решений с привлечением экспертов могут быть направлены на следующие объекты: 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 существующей альтернатив. В данной работе рассматривается вопросы устойчивости объективного решения экспертов при некоторой вероятности реализации угрозы, насколько оправдано увеличение числа экспертов.

Исходные положения. Для вычисления вероятности принятия ЛПР решения, отличного от решения, которое было бы принято по результатам опроса экспертов при отсутствии угроз информационной безопасности, определим следующие моменты:

– опрос экспертов проводится по выбору одной из двух альтернатив: «0» и «1»;

– действия злоумышленника направлены на изменение ответов экспертов в пользу альтернативы «0»;

– угрозы по блокированию ответа эксперта в процессе передачи до ЛПР являются случайными угрозами и могут быть реализованы в отношении любого эксперта.

Введем следующие обозначения:

m – общее количество экспертов, принимающих участие в голосовании;

n – количество экспертов, проголосовавших за альтернативу «1»;

$(m - n)$ – количество экспертов, проголосовавших за альтернативу «0»;

$P_{change\ i}$ – вероятность изменения злоумышленником ответа i-го эксперта;

$P_{bloc\ i}$ – вероятность блокирования ответа i-го эксперта в процессе передачи до ЛПР.

В данной статье рассматривается частный случай, когда угрозы по блокированию ответов экспертов отсутствуют ($P_{bloc\ i}$=0) и вероятности изменения ответов эксперта под действием угроз ИБ $P_{change\ i}$ одинаковы для всех экспертов.

Варианты голосования экспертов. Возможны следующие варианты голосования экспертов:

1) $n > m/2$.

Количество экспертов, проголосовавших за альтернативу «1», превышает количество экспертов, проголосовавших за альтернативу «0». В этих случаях из-за реализации угроз безопасности решение, принимаемое ЛПР по выбору одной из альтернатив, может быть изменено.

2) $n = m/2$.

Количество экспертов, проголосовавших за альтернативы «0» и «1», равны. В этом случае из-за реализации угроз безопасности ЛПР может быть выбрана альтернатива «0», а не назначено повторное голосование.

Указанный вариант возможен при четном количестве экспертов, принимающих участие в голосовании.

3) $n < m/2$.

Количество экспертов, проголосовавших за альтернативу «0», превышает количество экспертов, проголосовавших за альтернативу «1». ЛПР будет выбрана альтернатива «0», вне зависимости от того, существуют угрозы ИБ по изменению ответов экспертов в пользу альтернативы «0» либо подобных угроз не существует, т.е. действия злоумышленника в данном случае не приводят к изменению выбранной экспертами альтернативы, а могут приводить лишь к изменению процентного соотношения ответов, полученных за разные альтернативы.

Необходимо отметить, что данное утверждение верно в случае отсутствия угроз по блокированию ответов экспертов ($P_{bloc\ i} = 0$), т.к. существует вероятность блокирования ответов экспертов, поданных за альтернативу «0», учитывая, что угрозы по блокированию (отказы оборудования, разрывы линий связи, «зависание» программного обеспечения) носят случайный характер.

Возможные события по выбору альтернативы ЛПР. Далее будут рассматриваться только случаи голосования, когда количество экспертов, проголосовавших за альтернативу «1», равно или превышает количество экспертов, проголосовавших за альтернативу «0» ($n \geq m/2$), т.е. те случаи, когда действия злоумышленника могут привести к изменению выбранной альтернативы. При этом возможны следующие события:

*Answ*1 – 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;

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

Событие *AnswEq* возможно при четном количестве экспертов *m*, принимающих участие в опросе (в случае отсутствия угроз по блокированию ответов экспертов).

События *Answ*1, *AnswEq*, *Answ*0 образуют полную группу событий.

Условия возникновения событий AnswEq, Answ0. Событие *Answ*0 возникает только под действием угроз информационной безопасности, действия злоумышленника достигают своей цели полностью (при условии $n \geq m/2$).

Событие *AnswEq* может возникнуть как под действием угроз информационной безопасности (при $n > m/2$), так и в случае, когда эксперты проголосовали поровну за альтернативы «0» и «1» ($n = m/2$) и их ответы в процессе передачи не изменялись. При возникновении события *AnswEq* возможно назначение повторного голосования.

Количество экспертов (из *n* экспертов, проголосовавших за альтернативу «1»), ответы которых необходимо изменить в процессе передачи для того, чтобы произошло событие *AnswEq*:

$$n - m/2, \qquad m \text{ – четное.}$$

Количество экспертов (из *n* экспертов, проголосовавших за альтернативу «1»), ответы которых необходимо изменить в процессе передачи для того, чтобы произошло событие *Answ*0:

$$n - m/2 + 1,\ n - m/2 + 2,\ \ldots\ n, \qquad m \text{ – четное;}$$

$$n - (m+1)/2 + 1,\ n - (m+1)/2 + 2,\ \ldots\ n, \quad m \text{ – нечетное.}$$

Вероятности наступления событий

Вероятность наступления события AnswEq:

$$P(AnswEq) = (P_{change})^{(n-m/2)} \cdot (1 - P_{change})^{(n-(n-m/2))} \cdot C_n^{n-m/2}, \tag{1}$$

где $C_n^{n-m/2}$ – число сочетаний из *n* по *n*–*m*/2.

$$C_n^{n-m/2} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-(n-m/2+1)}{1 \cdot 2 \cdot \ldots \cdot (n-m/2)} = \frac{n!}{(n-m/2)! \cdot (n-(n-m/2))!} = \frac{n!}{(n-m/2)! \cdot (m/2)!}, \tag{2}$$

$$P(AnswEq)=(P_{change})^{(n-m/2)}\cdot(1-P_{change})^{(n-(n-m/2))}\cdot\frac{n!}{(n-m/2)!\cdot(n-(n-m/2)!}, \quad (3)$$

$$P(AnswEq)=(P_{change})^{(n-m/2)}\cdot(1-P_{change})^{(m/2)}\cdot\frac{n!}{(n-m/2)!\cdot(m/2)!}. \quad (4)$$

Вероятность наступления события Answ0:

$$P(Answ0)=\sum_i P(A_i), \quad (5)$$

где P_i – вероятность появления события A_i.

Событие A_i – изменение при передаче до ЛПР ровно i ответов экспертов из n экспертов, проголосовавших за альтернативу «1».

$i=\{n-m/2+1,\ n-m/2+2,\ \dots\ n\}$, если m – четное;

$i=\{n-(m+1)/2+1,\ n-(m+1)/2+2,\ \dots\ n\}$, если m – нечетное.

$$P(A_i)=(P_{change})^{i}\cdot(1-P_{change})^{(n-i)}\cdot C_n^i, \quad (6)$$

где C_n^i – число сочетаний из n по i

$$C_n^i=\frac{n\cdot(n-1)\cdot\ldots\cdot(n-i+1)}{i!}=\frac{n!}{i!\cdot(n-i)!}, \quad (7)$$

$$P(Answ0)=\sum_i((P_{change})^{i}\cdot(1-P_{change})^{(n-i)}\cdot C_n^i)=\sum_i((P_{change})^{i}\cdot(1-P_{change})^{(n-i)}\cdot\frac{n!}{i!\cdot(n-i)!}, \quad (8)$$

$i=\{n-m/2+1,\ n-m/2+2,\ \dots\ n\}$, если m – четное;

$i=\{n-(m+1)/2+1,\ n-(m+1)/2+2,\ \dots\ n\}$, если m – нечетное.

Вероятность наступления события Answ1:

$$P(Answ1)=1-(P(AnswEq)+P(Answ0)), \quad (9)$$

так как события *Answ*1, *AnswEq*, *Answ*0 образуют полную группу событий.

При возникновении события *AnswEq* должно назначаться повторное голосование до тех пор, пока не возникнет событие *Answ*1 или *Answ*0. При этом условная вероятность событий *Answ*1 и Answ2 при условии, что произошло одно из этих событий, составляет:

$$P(Answ1\,|\,Answ1\cup Answ0)=\frac{P(Answ1)}{P(Answ1)+P(Answ0)}, \quad (10)$$

$$P(Answ0\,|\,Answ1\cup Answ0)=\frac{P(Answ0)}{P(Answ1)+P(Answ0)}. \quad (11)$$

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.

Вероятности выбора альтернатив «0» и «1». Учитывая повторные голосования, назначаемые при возникновении события *AnswEq*, вычислим полные вероятности выбора альтернативы «0» (событие А0) и альтернативы «1» (событие А1).

$$P(A0)=P(Answ0)+P(AnswEq)\cdot P(Answ0\,|\,Answ1\cup Answ0), \quad (12)$$

$$P(A1)=P(Answ1)+P(AnswEq)\cdot P(Answ1\,|\,Answ1\cup Answ0). \quad (13)$$

Вероятность события А0 – вероятность того, что действия злоумышленника приводят к изменению выбранной экспертами альтернативы.

Вероятность события А1 – вероятность того, что действия злоумышленника не приводят к изменению выбранной экспертами альтернативы.

События А0 и А1 образуют полную группу событий.

$$P(A0)+P(A1)=1. \quad (14)$$

Следовательно, для нахождения вероятностей их наступления достаточно найти вероятность наступления только одного события, например $P(A0)$. Из формулы (12), используя формулу (11), получаем:

$$P(A0)=P(Answ0)+P(AnswEq)\cdot\frac{P(Answ0)}{P(Answ1)+P(Answ0)}=P(Answ0)\cdot(1+\frac{P(AnswEq)}{P(Answ1)+P(Answ0)}). \quad (15)$$

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

$$P(A0) = P(Answ0)\cdot(1+\frac{P(AnswEq)}{1-P(AnswEq)}) = \frac{P(Answ0)}{1-P(AnswEq)}. \quad (16)$$

Вероятности $P(AnswEq)$, $P(Answ0)$ находятся по формулам (4), (8).

Программная реализация. Для вычисления вероятности события А0 (изменение выбранной экспертами альтернативы в процессе передачи) в зависимости от вероятности изменения ответов экспертов P_{change}, количества экспертов m и количества экспертов, проголосовавших за альтернативу «1», разработан модуль на языке программирования MATLAB.

Результаты вычислений. На рис. 1 представлена зависимость вероятности $P(A0)$ от вероятности изменения отдельного ответа эксперта P_{change} , но при постоянном соотношении количества ответов экспертов за альтернативы «0» и «1» (n/m = 0,6). На графике приведены зависимости при m = {10, 20, 30, 40, 50}.

Из рис. 1 видно, что существует определенное значение P'_{change}, при котором вероятности наступления события $A0$ для различных значений m (при n/m = const) одинаковы.

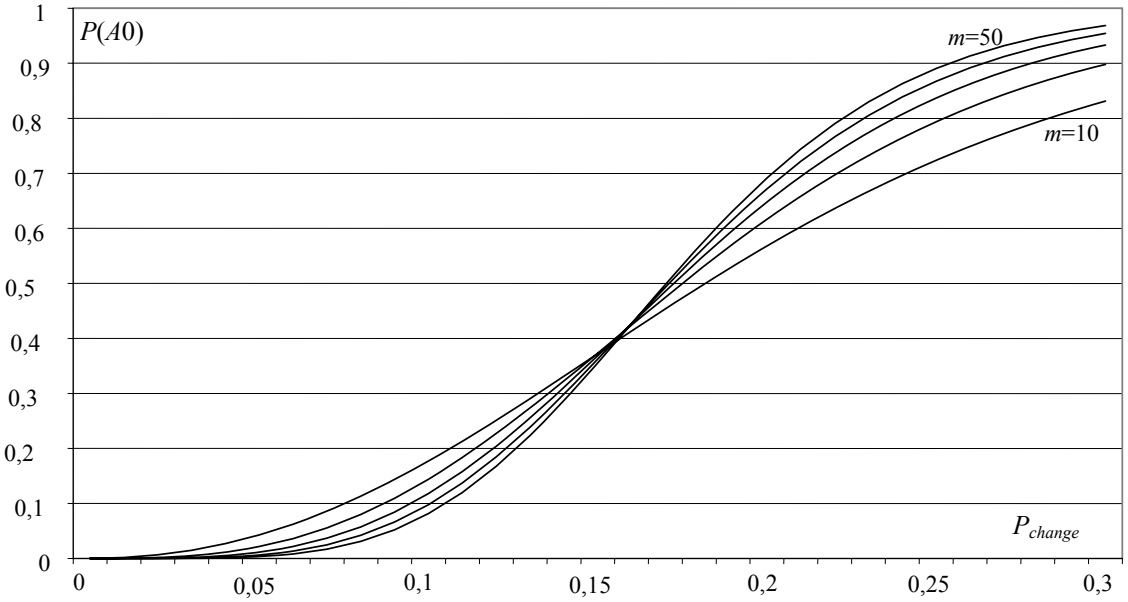

Рис. 1. Вероятность события $A0$ в зависимости от P_{change} при разных значениях m (n/m = 0,6 = const)

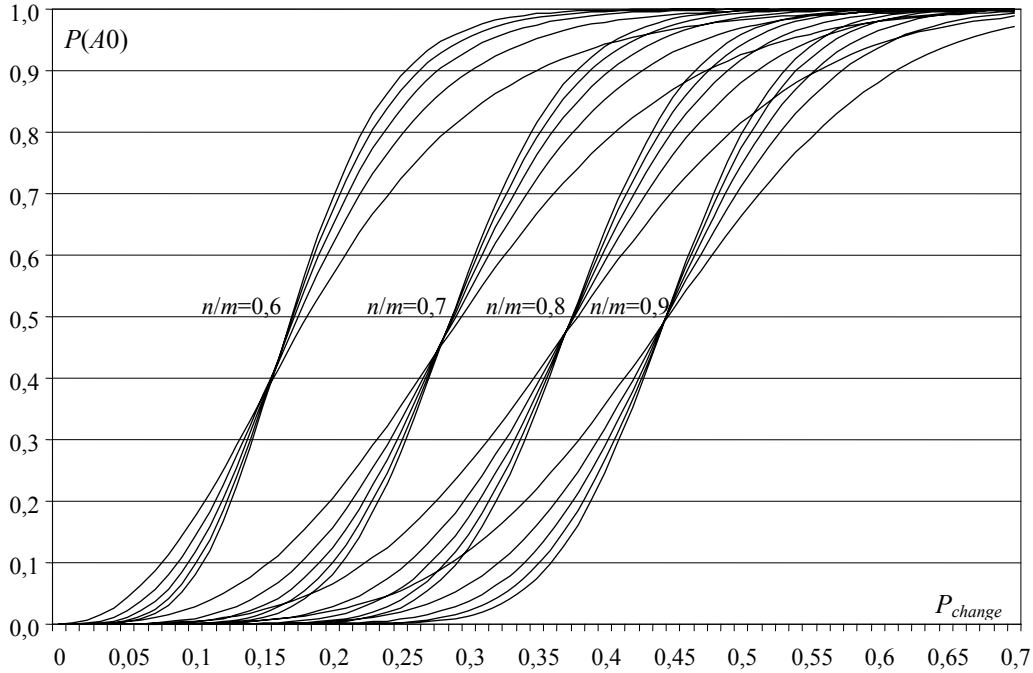

Рис. 2. Группы диаграмм зависимости P(A0) от P_{change}

При $P_{change} < P'_{change}$ увеличение количества экспертов m приводит к уменьшению вероятности изменения выбранной экспертами альтернативы.

При $P_{change} > P'_{change}$ увеличение количества экспертов m приводит к увеличению вероятности изменения выбранной экспертами альтернативы.

На рис. 2 построены группы диаграмм, отображающих зависимость вероятности $P(A0)$ от вероятности изменения отдельного ответа эксперта P_{change}. Каждая группа графиков построена для различных значений n/m, т.е. для различных распределений ответов экспертов.

Как видно из рис. 2, для разных групп графиков (т.е. для разных соотношений n/m) значения P'_{change} будут различны.

На рис. 3 представлена зависимость P'_{change} от отношения n/m. То есть для предполагаемого соотношения n/m (доля экспертов, проголосовавших за альтернативу «1») и ожидаемой вероятности P_{change} изменения злоумышленником ответа эксперта в пользу альтернативы «0» можно дать рекомендацию о необходимости увеличения или уменьшения количества экспертов для уменьшения влияния действий злоумышленника на решение, принимаемое ЛПР.

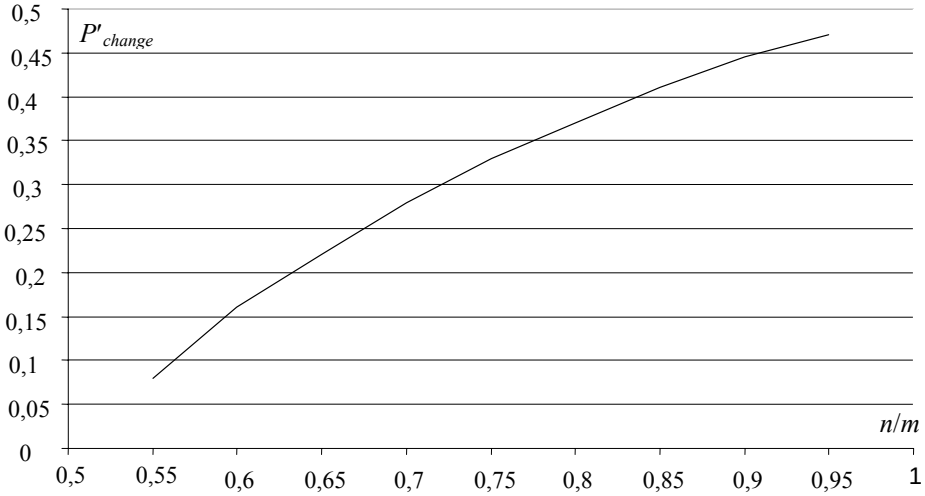

Рис. 3. Вероятность P'_{change} в зависимости от отношения n/m

Заключение. В статье показано, что для любого значения относительного количества экспертов, проголосовавших за альтернативу «1» (n/m), существует критическая вероятность изменения ответа эксперта под действием угроз информационной безопасности P'_{change}, при которой увеличение абсолютного значения количества экспертов приводит к увеличению вероятности принятия ложного решения (при $0{,}5 \le n/m \le 1$).

Так, при $n/m \to 0{,}5$ значение $P'_{change} \to 0$. Необходимо отметить, что при $n/m \to 0{,}5$ достаточно небольшой вероятности реализации угроз по изменению ответов экспертов P_{change}, чтобы было принято ложное решение. В данном случае возможным вариантом действий по проверке устойчивости результата может являться проведение ряда случайных выборок размером $m_1 < m$. При этом пространственная (сетевая) локализация экспертов, от которых лицом принимающим решение, получены результаты голосования за альтернативу «0», может служить основанием для подозрения об изменении их результатов (всех или части экспертов) вследствие реализации угроз информационной безопасности.

Литература

1. Ларичев О.И. Теория и методы принятия решений / О.И. Ларичев. – М.: Университетская книга, Логос, 2006. – 296 с.

2. Орлов А.И. Теория принятия решений / А.И. Орлов. – М.: Экзамен, 2005. – 656 с.

3. 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. – Кн. 1. – Омск: Изд-во ОмГТУ, 2009. – С. 280–284.

4. 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.

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

Файзуллин Рашит Тагирович
Д-р техн. наук, профессор, проректор по информатизации ОмГТУ
Тел.: (381-2) 62-87-07
Эл. почта: r.t.faizullin@mail.ru

Efimov B.I., Faizullin R.T.

The probability of making a false solutions under the influence of information security threats in decision-making systems with experts

Proposed solution to the problem of calculating the probability of a false solution in decision-making systems with experts under the influence of information security threats, aimed at changing the experts' responses. The graphs showing the feasibility of increasing the number of experts to reduce the influence of the attacker on the decision are obtained.
Keywords: information security, decision-making systems, experts, threats, probability theory.