DOI 10.37882/2223–2966.2021.02.24

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

IMPROVING THE METHODOLOGY QUANTITATIVE ASSESSMENT OF THREATS TO INFORMATION SECURITY OF TELECOMMUNICATIONS SYSTEMS AND NETWORKS

O. Nazarova
A. Sagdeev
I. Stakheev
O. Titova
A. Shilina

Summary. In order to improve the effectiveness of security systems for telecommunications systems and networks, the paper considers the issue of assessing threats to their information security. The technique of definition of quantity of threats taking into account the probabilistic nature of the process of realization of negative impacts on the objects of telecommunications, the factors that promote and (or) their initiator obtained according to formal definitions of the quantitative indicators of threats. Methods of quantitative threat assessment in order to justify and describe the method for determining the threat to telecommunications networks and systems and quantifying the degree of this threat are considered by example. Recommendations are formulated for obtaining expert assessments of negative impacts on the object of Informatization and countering them with information security systems, as well as qualitative classification of threat categories for making decisions on the protection of telecommunications facilities.

Keywords: telecommunication systems and networks, information security, information security threats, security systems, methods for assessing information security threats.

Назарова Ольга Юрьевна
К.т.н., доцент, Донской государственный технический университет, Ростов-на-Дону
olga2018rostov@yandex.ru
Сагдеев Александр Константинович
К.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
brother-aks@yandex.ru
Стахеев Иван Геннадиевич
К.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Титова Ольга Викторовна
К.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
Шилина Анна Николаевна
К.т.н., доцент, Южно-Российский государственный политехнический университет (НПИ) имени М. И. Платова, Новочеркасск

Аннотация. С целью повышения эффективности систем обеспечения безопасности телекоммуникационных систем и сетей, в работе рассматривается вопрос оценки угроз их информационной безопасности. Предложена методика определения количественного показателя угроз с учетом вероятностного характера процесса реализации негативных воздействий на объекты телекоммуникаций, определены факторы, способствующие и (или) их инициирующие, получены зависимости формального определения количественного показателя угроз. Методики количественной оценки угрозы с целью обоснования и описания способа определения угрозы на телекоммуникационные сети и системы и количественной оценки степени этой угрозы рассмотрены на примере. Сформулированы рекомендации по получению экспертных оценок негативных воздействий на объект информатизации и противодействия им систем обеспечения информации, а так же качественной классификации категорий угроз для принятия решений по защите объектов телекоммуникаций.

Ключевые слова: телекоммуникационные системы и сети, безопасность информации, угрозы информационной безопасности, системы обеспечения безопасности, методика оценки угроз информационной безопасности.

В современных условиях значение телекоммуникационных систем и сетей (ТКСС), их составляющая в жизни общества, а вместе с тем важность и сложность задачи обеспечения их информационной безопасности неизмеримо возросли. Безусловно, что согласно закрепленного Федеральным законом [1] интегрального понятия защищаемого объекта, телекоммуникации становятся важной составляющей, объектом безопасности в информационной сфере.

Значимость обеспечения защиты ТКСС определяется уязвимостью, некоторым свойством информационной сферы, которое делает возможным возникновение и реализацию угрозы, негативного воздействия вследствие множества факторов, основными среди которых являются:

- огромные масштабы информационной инфраструктуры страны,
- взаимодействие объектов информатизации с международными сетями передачи и хранения информации,
- возросшим числом компьютерных атак на критически важные объекты инфраструктуры,
- эксплуатация средств вычислительной техники и связи иностранного производства.

Основными объектами угрозы информационной безопасности являются объекты информатизации, информационные системы, ресурсы информационной системы, информационные технологии, программные средства и сети связи. Быстро развивающиеся технологии передачи данных требуют постоянного совершенствования методов обеспечения БИ, а значит анализа «аспектов, связанных с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки» [2].

Информационной безопасностью (ИБ) ТКСС является ее способность противостоять множеству угроз, основными видами которых можно считать информационные нарушения сбора и обработки информации, аппаратно-программные угрозы и радиоэлектронные помехи, перехват информации, нормативно-правовые коллизии, а так же физические поломки, хищение и аварии в технических системах коммуникации. Применительно к основным свойствам информации возможны угрозы связанные с разглашением информации, с несанкционированным доступом, искажением (модификацией) информации, блокированием доступа к защищаемой информации, уничтожением носителей информации, непреднамеренным воздействием или сбоем оборудования и др. Виды угроз однозначно определяются видами НВ на ТКСС.

Появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации и указывающих на свершившуюся, преднамеренную или вероятную реализацию угрозы ИБ, является инцидентом (И) безопасности [3].

Противодействие угрозам — цель защиты систем обеспечения БИ, эффективность которых адекватно зависит от применения современных методик определения показателей угроз.

В качестве вида количественного показателя угрозы безопасности выберем *степень угрозы* И на объекте безопасности на некотором временном интервале $\Delta \boldsymbol{T}=[\boldsymbol{t}_1, \boldsymbol{t}_2]$.

Учитывая вероятный характер процесса реализации И на ТКСС, степень угрозы $в_j$И (j= 1,2,…, J_i) на i-й объект (i = 1,2,…, I) количественно может характеризоваться вероятностью $W_{i(в_j)T^{угр}}$ начала исполнения этой угрозы (начала реализации И) на временном интервале $\Delta \boldsymbol{T}$.

Здесь и в дальнейшем под *вероятностью* некоторого события, которая согласно положению теории вероятностей является неслучайной величиной, будем понимать полученную тем или иным способом ее *оценку*, которая представляет собой случайное число и характеризует вероятность с некоторой точностью в зависимости от способа ее определения [4, 5, 6].

Величина $W_{i(в_j)T^{угр}}$ определяется наличием на интервале $\Delta \boldsymbol{T}$ ряда факторов угрозы $f_{ij\Phi} \in \boldsymbol{F}ij$, $ф$=1,2,…, Φ_{ij}, способствующих и/или инициирующих $в_j$ И на i-й объект ТКСС (1).

При этом в зависимости от своего физического содержания указанные факторы могут вызывать И как самостоятельно, так и в определенных сочетаниях.

Факторы способствующие И (и/или их инициирующие) применительно к информационной сфере:

- наличие связей объектов ТКСС с сетью Интернет;
- наличие заинтересованности определенных лиц и организаций в получении конфиденциальной информации, циркулирующей в конкретной информационной системе;
- социальная значимость ТКСС;
- уязвимостью объектов информатизации и реализуемых ими технологических процессов;
- уязвимостью систем обеспечения БИ;
- надлежащее выполнение собственниками объектов информатизации эксплуатационных требований (режим эксплуатации, техническое обслуживание, регламентные работы, ремонт и т.п.);

$$W_{i(в_j)T^{угр}}=W_{T^{угр}}f_{ijФ} \in F_{ij}. \quad (1)$$

$$W(f_{ijФ})^{угр}{}_{Ф}=W(f_{ijФ})^{нал}{}_{Ф}W(f_{ijФ})^{вл}{}_{Ф}. \quad (2)$$

$$W_{i(в_j)Ф^{угр}} = \sum_{Ц=1}^{Ф_{ij}} W(f_{ijФ})_{T^{угр}} - \sum_{б,в} W(f_{ijб} \cap f_{ijв})_{Ф^{угр}} + \sum_{бвг} W(f_{ijб} \cap f_{ijв} \cap f_{ijг})_{Ф^{угр}} - \ldots + (-1)^{Ф_{ij}-1} W(f_{ij1} \cap f_{ij2} \cap \ldots f_{ij\,Ф_{ij}})_{Ф^{угр}}. \quad (3)$$

$$W_i\left(в_j\right)_{Ф^{угр}} = \sum_{Ц=1}^{Ф_{ij}} W(f_{ijФ})_{Ф^{угр}} - \sum_{б,в} W(f_{ijб})_{Ф^{угр}} W(f_{ijв})_{Ф^{угр}} + \sum_{б,в,г} W(f_{ijб})_{Ф^{угр}} W(f_{ijв})_{Ф^{угр}} W((-1)^{Ф_{ij}-1} W(f_{ij1})_{Ф^{угр}} W(f_{ij2})_{Ф^{угр}} \ldots W(f_{ijФij})_{Ф^{угр}}. \quad (4)$$

$$W(f_{ijб})_{Ф^{угр}} W(f_{ijв})_{Ф^{угр}}, \ldots, W(f_{ijб})_{Ф^{угр}} W(f_{ijв})_{Ф^{угр}} W(f_{ijг})T, \ldots) \quad (5)$$

$$W_{i(в_j)Ф^{угр}} = \prod_{ф=1}^{Ф_{ij}} (1 - W(f_{ijФ})_{Ф^{угр}}). \quad (6)$$

- возможность физического НД к технике и операционным системам;
- низкий уровень квалификации, состояния производственной дисциплины, морального и психологического состояния персонала объектов информатизации.

Определение перечня факторов угрозы $\boldsymbol{F}_{ij}$, их наличия на интервале $\Delta\boldsymbol{T}$ и влияния на началоИ на этом интервале является не формализуемой задачей и может осуществляться исключительно экспертными методами с участием специалистов.

В интересах формального определения степени угрозы введем в рассмотрение величину $W(f_{ijФ})^{нал}{}_{T}$, характеризующую наличие на интервале $\Delta\boldsymbol{T}$ фактора угрозы $f_{ijФ}$, способствующего реализации j-го И на i-й объект безопасности, и величину $W(f_{ijФ})^{вл}{}_{Ф}$, характеризующую влияние этого фактора (при его наличии) на начало указанного воздействия. При введении шкалы [0,1] в качестве области значений величин они могут быть интерпретированы как соответствующие вероятности.

Степень угрозы $W(f_{ijФ})^{угр}{}_{Ф}$ (со стороны фактора $f_{ijФ}$) начала реализации j-го И на ТКСС на интервале $\Delta\boldsymbol{T}$ определяется совпадением двух событий: наличием фактора $f_{ijФ}$ на этом интервале и его влиянием на начало воздействия (2).

Второй сомножитель $W(f_{ijФ})^{вл}{}_{Ф}$ при этом имеет смысл условной вероятности (при условия наличия фактора $f_{ijФ}$ на интервале $\Delta\boldsymbol{T}$).

В случае совместного присутствия на интервале $\Delta\boldsymbol{T}$ всей (в общем случае взаимосвязанной) совокупности факторов $f_{ijФ} \in \boldsymbol{F}_{ij}$ ($ф$ = 1,2,…, $Фij$) *степень угрозы* начала реализации $вj$ И на i-й объект ТКСС определяется следующим образом (3), где $W(f_{ijб} \cap f_{ijв})_{Ф^{угр}}$ — степень угрозы, обусловленная совместным влиянием на начало $вj$ НВ взаимосвязанных факторов $f_{ij\alpha}uf_{ij\beta}$; суммы распространяются на различные значения индексов $ф; \alpha, \beta; \alpha, \beta, \gamma$ и т.д.

Если события, характеризующие присутствие на интервале $\Delta\boldsymbol{T}$ факторов $\boldsymbol{f}_{ijф}$ и их влияние на начало $в_j$ И, являются независимыми, выражение (3) преобразуется в вид (4).

В случае, когда факторы $fijф$ не являются независимыми, ряд соответствующих сомножителей в слагаемых зависимости (4), представляющих собой произведение вероятностей (5), будут иметь смысл условных вероятностей [7].

При использовании понятия противоположного события [8] (1-W($fijф$)Тугр) зависимость (4) представляется в более компактной форме (6).

Таблица 1

Фактор $f_{ij\phi}$	Инцидент на j=1,2,…, J					
	1		j		J	
	Наличие	Влияние	Наличие	Влияние	Наличие	Влияние
1	$W_k(f_{i11})^{\text{нал}}{}_{\Phi}$	$W_k(f_{i11})^{\text{вл}}{}_{\Phi}$	$W_k(f_{ij1})^{\text{нал}}{}_{\Phi}$	$W_k(f_{ij1})^{\text{вл}}{}_{\Phi}$	$W_k(f_{iJ1})^{\text{нал}}{}_{\Phi}$	$W_k(f_{iJ1})^{\text{вл}}{}_{\Phi}$
ϕ	$W_k(f_{i1\Phi})^{\text{нал}}{}_{\Phi}$	$W_k(f_{i1\Phi})^{\text{вл}}{}_{\Phi}$	$W_k(f_{ij\Phi})^{\text{нал}}{}_{\Phi}$	$W_k(f_{ij\Phi})^{\text{вл}}{}_{\Phi}$	$W_k(f_{iJ\Phi})^{\text{нал}}{}_{\Phi}$	$W_k(f_{iJ\Phi})^{\text{вл}}{}_{\Phi}$
Φ_{ij}	$W_k(f_{i1\Phi})^{\text{нал}}{}_{\Phi}$	$W_k(f_{i1\Phi})^{\text{вл}}{}_{\Phi}$	$W_k(f_{ij\Phi})^{\text{нал}}{}_{\Phi}$	$W_k(f_{ij\Phi})^{\text{вл}}{}_{\Phi}$	$W_k(f_{iJ\Phi})^{\text{нал}}{}_{\Phi}$	$W_k(f_{iJ\Phi})^{\text{вл}}{}_{\Phi}$

Таблица 2

Фактор $f_{ij\phi}$	Инцидент на j=1,2,…, J		
	1	j	J
1	$W_k(f_{i11})_{\Phi^{\text{угр}}}$	$W_k(f_{ij1})_{\Phi^{\text{угр}}}$	$W_k(f_{iJ1})_{\Phi^{\text{угр}}}$
ϕ	$W_k(f_{i1\Phi})_{\Phi^{\text{угр}}}$	$W_k(f_{ij\Phi})_{\Phi^{\text{угр}}}$	$W_k(f_{iJ\Phi})_{\Phi^{\text{угр}}}$
Φ_{ij}	$W_k(f_{i1\Phi})_{\Phi^{\text{угр}}}$	$W_k(f_{ij\Phi})_{\Phi^{\text{угр}}}$	$W_k(f_{iJ\Phi})_{\Phi^{\text{угр}}}$

Таблица 3

Эксперт, k = 1,2,…, k	инцидент на j=1,2,…, J		
	1	j	J
1	$W_{i(6_1)\Phi}{}^{\text{угр}}{}_{1}$	$W_{i(6_j)\Phi}{}^{\text{угр}}{}_{1}$	$W_{i(6_J)\Phi}{}^{\text{угр}}{}_{1}$
k	$W_{i(6_1)\Phi}{}^{\text{угр}}{}_{k}$	$W_{i(6_j)\Phi}{}^{\text{угр}}{}_{k}$	$W_{i(6_J)\Phi}{}^{\text{угр}}{}_{k}$
K	$W_{i(6_1)\Phi}{}^{\text{угр}}{}_{\text{К}}$	$W_{i(6_j)\Phi}{}^{\text{угр}}{}_{\text{К}}$	$W_{i(6_J)\Phi}{}^{\text{угр}}{}_{\text{К}}$

Рассмотрение методики количественной оценки угрозы с целью обоснования и описания способа определения угрозы на ТКСС и количественной оценки степени этой угрозы рассмотрим при следующих исходных данных:

- временной интервал, на котором оцениваются угрозы реализациинегативных воздействий на ТКСС.
- перечень и содержание характерных для этого объекта И.
- перечень и содержание факторов угрозы, которые могут способствовать началу И на ТКСС.

Для конкретных ТКСС содержание исходных данных уточняются специалистами по обеспечению безопасности на основании:

- анализа специфических особенностей этого объекта, характерных для него И, а также факторов, способствующих их реализации;
- накопление опыта борьбы с И;
- имеющейся статистики по происшествиям безопасности применительно к данному объекту и подобным ему объектам безопасности;
- прогнозирования возможных изменений И (например, совершенствование нарушителями способов осуществления актов незаконного вмешательства в работу ТКСС) и факторов, способствующих их реализации.

Ввиду невозможности формализации получения исходных данных количественная оценка угрозы безопасности осуществляется экспертным методом. Выбранной

группе в составе K экспертов представляется перечень характерных для данной ТКСС И (которые представляют интерес с точки зрения обеспечения безопасности), предлагается определит перечень факторов угрозы воздействия на временном интервале $\Delta \boldsymbol{T}$ и ответить на следующие вопросы:

1. Какие факторы, по вашему мнению, на временном интервале $\Delta \boldsymbol{T}$ могут способствовать угрозе реализации представленных И на данную ТКСС?
2. Какова, по вашему мнению, степень влияния (по шкале [0, 1]) наличия на интервале $\Delta \boldsymbol{T}$ выбранных вами факторов?
3. Какова, по вашему мнению, степень влияния (по шкале [0, 1]) каждого из выбранных вами факторов на начало представленных И?

Ответы каждого эксперта фиксируются в форме табл. 1.

По результатам экспертного опроса величины $W_k(в_j)_{\text{Ф}^{\text{угр}}}$оцениваются с использованием зависимости (2) и представляются в форме табл. 2.

В соответствии с данными табл. 2 с использованием зависимостей (5) или (4) проводятся количественные оценки степени угрозы $Wi(вj)Tугрk$ начала реализации инцидента на i-й ОБ (по мнению каждого из участвовавших в опросе экспертов). Результаты этих оценок оформляются в виде табл. 3.

Экспертному методу оценки характеристик СОБ защищаемых объектов принадлежит важная роль в процессе этой оценки вследствие большой сложности структур «ОБ — СОБ», широкого участия в них человека и невозможности исчерпывающего формального описания процессов негативных воздействий на ОБ и противодействия им СОБ.

Экспертный метод, базирующийся на *эвристической* деятельности человека, является исторически наиболее известным. Эвристическая деятельность представляет собой познавательный процесс, направленный на изучение качественных и количественных сторон исследуемого процесса или явления, протекающий в голове человека с использованием сформированных в мозгу образов этого процесса или явления [9]. Причем зачастую человек не в состоянии четко сформулировать, каким образом он сделал ту или иную оценку.

Совершенно очевидно, что не всякий человек, ежедневно пользующийся своими эвристическими оценками в повседневной жизни, несмотря на прирожденные способности и даже талант, способен количественно оценить характеристики сложных процессов (явлений), когда требуется большой объем знаний в специальных областях и соответствующий опыт работы. Опыт формируется в процессе оценки результатов схожих процессов (явлений), наблюдения за их протеканием, сравнения результатов собственных оценок с практическими результатами и корректировки, исходя из этого, «собственной методики» оценки.

Экспертный метод не потерял своего значения в тех случаях, когда бывает сложно, а иногда на данном уровне знаний просто невозможно построить математическую модель исследуемого процесса, провести оценки формальными методами с требуемой точностью. Между тем человек в подобных ситуациях решает задачи оценки зачастую достаточно успешно и в условиях неполной информации. Здесь проявляется подмеченная Н. Винером замечательная способность человеческого мозга «оперировать с нечетко очерченными понятиями» [10].

В связи с этим, т.к. в основе экспертных оценок, как отмечалось выше, лежит познавательный процесс, протекающий в мозгу человека, они подвержены целому ряду объективных и субъективных факторов, определяемых характером, особенностями мышления и чертами конкретного человека.

Факторами, без которых получение точных оценок просто невозможно, являются уже упомянутые профессиональные знания, опыт, а также интуиция, способность к выделению главного, умение вовремя признать свою ошибку.

К факторам, которые могут отрицательно сказаться на качестве оценки, относятся [10]: профессиональная ограниченность, психологическая инерция, консерватизм мышления, трудность восприятия отрицательных выводов, склонность к преувеличению плохого, боязнь ответственности.

Влияние на результаты экспертных оценок факторов, обусловленных субъективизмом конкретного человека, может быть умышленно при проведении опроса группы экспертов при правильно организованной процедуре самого опроса и обработке полученных результатов, например, с использованием уже упомянутого метода ДЕЛЬФИ [11].

Метод ДЕЛЬФИ представляет собой многоэтапный экспертный метод, предусматривающий первоначальное изолированное вынесение экспертами своих суждений и дальнейшую многократную их корректировку на базе ознакомления каждого эксперта с суждениями других экспертов до тех пор, пока величина разброса оценок не будет находиться в рамках заранее устанавливаемого желаемого интервала варьирования оценок.

Таблица 4

Вид инцидента	Степень угрозы начала инцидента на интервале ΔT
$в_1$	$\overline{W}_i(в_1)_{\Phi^{угр}}$
$в_j$	$\overline{W}_i(в_j)_{\Phi^{угр}}$
$в_J$	$\overline{W}_i(в_J)_{\Phi^{угр}}$

$$\tilde{y} = \sum_{k=1}^{K} y_k / K \quad (7)$$

$$e = \frac{\left\{\frac{\left[\sum_{k=1}^{K}(y_k - \tilde{y})^2\right]}{K-1}\right\}^{\frac{1}{2}}}{\tilde{y}} \quad (8)$$

$$\overline{W}_i(в_i)_{\Phi^{угр}} = \sum_{k=1}^{K} W_{i(в_j)\Phi}{}^{угр}{}_{k} - K. \quad (10)$$

$$\varepsilon = \{[\sum_{k=1}^{K}(W_{i(в_j)\Phi}{}^{угр}{}_{k} - \overline{W}_i(в_i)_{\Phi^{угр}})^2]/(K - \frac{1)\}^{\frac{1}{2}}}{\overline{W}_i(в_i)_{\Phi^{угр}}} \quad (11)$$

В результате экспертного опроса относительно величины некоторой характеристики СОБ защищаемого объекта обобщенного мнение группы из K экспертов представляется в виде:

- среднего значения величины y (7)
- коэффициента вариации мнений группы экспертов (8)

Результаты опроса подвергаются анализу, целью которого является оценка с помощью коэффициента вариации ε согласованности мнений экспертов. Если коэффициент вариации не превосходит некоторого заранее оговоренного допустимого значения $\varepsilon^{доп}$, $\varepsilon \leq \varepsilon^{доп}$, (9) окончательные результаты принимаются соответствующими оценке (7).

Значение коэффициента $\varepsilon^{доп}$ с учетом случайного характера величины y и возможных ошибок экспертов выбирается в виде некоторого диапазона (для практических задач, например, диапазон 0,15—0,20).

В случае невыполнения условия (9) проводится обсуждение мнений экспертов, находятся причины разброса экспертных оценок и проводится повторный опрос экспертов. Данная процедура проводится до тех пор, пока не будет выполнено условие (9).

С использованием данных табл. 3, находится обобщенное мнение группы экспертов (7) в виде среднего значения степени угрозы начала реализации на интервале ΔT каждого j-го инцидента на i-й ОБ (10) и оценивается согласованность мнений группы экспертов (8) по величине коэффициента вариации (11).

В случае наличия согласованного (9) мнения группы экспертов результаты количественной оценки степени угрозы начала реализации на интервале ΔT инцидента оформляются в виде таблицы 4.

Введение количественного показателя степени угрозы И на ОБ позволяет количественно описать содержа-

Таблица 5

Инцидент, $в_j$ (j=1,2,…, j)	**Категория угроз i-муОБ**		
	I категория угрозы	IIкатегория угрозы	III категория угрозы
1	$0 < W_{i(в_1)Ф}^{угр} \le A_{i1}$	$A_{i1} < W_{i(в_1)Ф}^{угр} \le B_{i1}$	$B_{i1} < W_{i(в_1)Ф}^{угр} \le 1$
j	$0 < W_{i(в_j)Ф}^{угр} \le A_{i1}$	$A_{ij} < W_{i(в_j)Ф}^{угр} \le B_{ij}$	$B_{ij} < W_{i(в_j)Ф}^{угр} \le 1$
J	$0 < W_{i(в_J)Ф}^{угр} \le A_{i1}$	$A_{iJ} < W_{i(в_J)Ф}^{угр} \le B_{iJ}$	$B_{iJ} < W_{i(в_J)Ф}^{угр} \le 1$

Таблица 6

НВ	**Категория угроз i-муОБ**		
	Потенциальная	Непосредственная	Прямая
$в_j$	$0 < W_{i(в_J)Ф}^{угр} \le 0{,}30$	$0{,}30 < W_{i(в_J)Ф}^{угр} \le 0{,}80$	$0{,}80 < W_{i(в_J)Ф}^{угр} \le 1$

ние различных существующих качественных категорий угроз («красной», «оранжевой», «желтой», «прямой», «непосредственной» и т.п.).

Указанные категории угроз могут быть заданы табл. 5, в которой интервалы значений (Aij, Bij) вероятности $Wi(вj)Тугр$ для каждого i-го ОБ применительно к j-му инциденту задаются экспертами.

В частности, границы диапазона значений вероятностей $Wi(вj)Тугр$ могут быть такими:

A_{ij} = 0,20–0,30; B_{ij} = 0,80–0,85 (12)

Так введение показателя степени угрозы И на ОТИ и ТС позволяет, количественно определить понятие степени угрозы совершения незаконного вмешательства в деятельность объектов ТКСС.

Принимая во внимание уровни безопасности объектов ТКСС и порядок их объявления (установления) получим качественную классификацию угроз (I– потенциальная угроза, II–непосредственная угроза, III — прямая угроза) и количественные значения диапазона вероятностей (12), табл. 5 для И-a в рассматриваемом случае может представляться в виде табл. 6.

В этом случае оцененную угрозу начала реализации И-a, характеризуемую вероятностью $\overline{W}_i(в_1)_{Ф^{угр}}$= 0,86, можно отнести к категории «прямая угроза».

Предложенная методика количественной оценки угрозы начала реализации И на ОБ, может быть использована для принятия научно-обоснованных решений по их защите и повышении эффективности системы управления в информационно-телекоммуникационных системах [12].

ЛИТЕРАТУРА

1. Федеральный закон от 5 марта1992 г. № 2446–1 «О безопасности».
2. ГОСТ Р ИСО/МЭК 13335–1–206 // Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
3. Пелешенко В. С., Говорова С. В., Лапина М. А. //Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: Ставрополь: СКФУ, 2017.
4. Михайлов Ю. Б. // Математические основы повышения точности прогнозирования количественных характеристик процессов. М.: Научтехлитиздат, 2000;
5. Смирнов Н. В., Дунин-Барковский И.В. // Курс теории вероятностей и математической статистики. М.: Наука, 1965;
6. Бусленко Н. П. и др. // Метод статистических испытаний. М.: Сов. Радио, 1972.

7. Вентцель Е. С. Исследование операций. М.: Сов. Радио, 1972.
8. Семенов В. А. // Теория вероятностей и математическая статистика: Учебное пособие. Стандарт третьего поколения. СПб.: Питер, 2013.
9. Орлов А. И. // Экспертные оценки. Учебное пособие. М., 2002.
10. Чуев Ю. В., Михайлов Ю. Б., Кузьмин В. И. // Прогнозирование количественных характеристик процессов. М.: Сов. Радио, 1971.
11. А. Г. Гранберг // Статистическое моделирование и прогнозирование. М.: Финансы и статистика, 1990.
12. Шилина А. Н., Кузнецова В. В., Гайдаревский А. А. // Предложения по оптимизации показателей эффективности системы управления в информационно-телекоммуникационных систем // Материалы III международной научно-практической конференции «Фундаментально-прикладные проблемы безопасности, живучести, надежности, устойчивости и эффективности систем» Часть I, Елец-2019.

Донской государственный технический университет