МАТЕМАТИЧЕСКИЕ МОДЕЛИ ДЛЯ ОЦЕНКИ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Соловьев С.В.[1], Язов Ю.К.[2], Теплинских А.А.[3]

Цель *исследования состоит в разработке математических моделей для количественной оценки показателей полноты, достоверности, актуальности и защищенности информационного обеспечения деятельности по организации и ведению технической защиты информации в органах власти, организациях и предприятиях.*

В результате исследования *предложены показатели оценки качества информационного обеспечения деятельности по технической защите информации: полноты, достоверности, своевременности (актуальности) и защищенности информации, необходимой для такого обеспечения, раскрыта взаимосвязь указанных показателей качества с комплексным показателем оценки эффективности информационного обеспечения. С учетом содержания модели предметной области технической защиты информации показано, что полнота, достоверность и актуальность информационного обеспечения защиты информации определяется множествами: функций, предусмотренных в модели предметной области и действительно реализуемых в информационной системе; задач, решение которых обеспечивает реализацию функций; информационных объектов и их атрибутов, подлежащих использованию в соответствии с моделью предметной области и реально используемых при решении задач защиты информации. Для оценки показателя защищенности информации, необходимой при информационном обеспечении деятельности по защите информации, предложено использование аппарата нечетких оценок вероятностей реализации угроз относительно системной и пользовательской информации, нарушение конфиденциальности, целостности или доступности которой может сорвать информационное обеспечение.*

Практическая ценность. *Разработаны аналитические соотношения для расчета показателей качества информационного обеспечения, что позволяет количественно обосновывать требования к информационному обеспечению деятельности по защите информации и к создаваемым системам информационного обеспечения для органов власти, организаций и предприятий.*

Ключевые слова: *информационная система, эффективность, предметная область, полнота, достоверность, актуальность, защищенность информации.*

DOI: 10.21681/2311-3456-2023-6-81-95

Введение

Информационное обеспечение деятельности по организации и ведению технической защиты информации (ТЗИ) в органах власти, организациях и предприятиях связано сегодня с предоставлением им такой информации, как [1]:

— состав и содержание актуальных нормативных правовых, организационно-распорядительных и методических документов государственного регулятора в области ТЗИ;

1 Соловьёв Сергей Вениаминович, кандидат технических наук, доцент, заместитель начальника Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail:sersol@mail.ru

2 Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail:yazoff_1946@mail.ru

3 Теплинских Александр Андреевич, научный сотрудник Государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю России, г. Воронеж, Россия. E-mail:ma4karek48@yandex.ru

— сведения из реестра значимых объектов критической информационной инфраструктуры в части, касающейся информационной системы (ИС) субъекта деятельности по ТЗИ (органа власти, организации, предприятия) в случае, если ИС относится или может быть отнесена к таким объектам;
— акты, докладные, указания и сообщения, аналитические обзоры и иные информационные документы, присланные вышестоящими инстанциями или высланные им субъектом деятельности по ТЗИ;
— состав и характеристики ИС, функционирующей в субъекте деятельности по ТЗИ, требуемый класс (уровень) ее защищенности в соответствии с действующими документами;
— состав и характеристики мер и средств ТЗИ, применяемых в ИС, установленные для средств классы защиты и выданные на них сертификаты;
— состав и характеристики угроз безопасности информации, которые могут иметь место в данной ИС, а также уязвимостей системного и прикладного программного обеспечения функционирования ИС;
— результаты оценки рисков реализации угроз в данной ИС или в сходных с ней ИС;
— результаты контроля защищенности информации в ИС, выявления уязвимостей и нарушений безопасности информации и др.

Стремительно разрастающиеся объемы и сравнительно быстрые изменения содержания такой информации (например, связанные с разработкой и введением в действие новых нормативных и методических документов) приводят к значительным сложностям в ее подготовке, актуализации и предоставлении специалистам при организации и ведении ТЗИ, обусловливают необходимость автоматизации процессов информационного обеспечения (ИО) и создания в рамках организационно-технических систем защиты информации в органах власти, организациях и предприятиях специальных систем информационного обеспечения – СИО.

Однако для этого, как показано в [2], необходимо разработать соответствующее методическое обеспечение, то есть совокупность математических моделей и методик, которое сегодня только начинает развиваться применительно к предметной области ТЗИ. Важнейшей составляющей такого обеспечения является совокупность математических моделей количественной оценки эффективности информационного обеспечения деятельности по ТЗИ – эффективности функционирования СИО. При этом под эффективностью информационного обеспечения понимается [2-4] степень соответствия предоставляемых услуг в информационном обеспечении потребностям организации и ведения ТЗИ в субъекте деятельности по ТЗИ. В таком понимании эффективность информационного обеспечения является функцией частных показателей, характеризующих качество информационного обеспечения по его отдельным аспектам, таким как полнота, достоверность, своевременность (актуальность) и защищенность информации, требуемой при организации и ведении ТЗИ.

В [2] предложены аналитические соотношения, позволяющие с использованием линейной функции или мультипликативной функции Кобба-Дугласа [5, 6] свернуть указанные показатели в один комплексный показатель эффективности информационного обеспечения с учетом устанавливаемых для каждого частного показателя, например, с применением метода анализа иерархий[4] Т. Саати, коэффициентов важности. В частности, при использовании линейной функции соотношение для расчета комплексного показателя имеет вид:

$$\eta_1(t) = \alpha_{full} \cdot g_{full}(t) + \alpha_{rel} \cdot g_{rel}(t) + \\ + \alpha_{act} \cdot g_{act}(t) + \alpha_{prot} \cdot g_{prot}(t), \quad (1)$$

где $g_{full}(t)$, $g_{rel}(t)$, $g_{act}(t)$, $g_{prot}(t)$ – частные показатели полноты, достоверности, своевременности (актуальности) и защищенности информационного обеспечения при оценке в момент времени t;

α_{full}, α_{rel}, α_{act} и α_{prot} – коэффициенты важности частных показателей соответственно.

Вместе с тем в работе [2] не раскрывались методы и модели оценки самих частных показателей. В связи с изложенным цель данной статьи состоит в разработке математических моделей количественной оценки указанных частных показателей полноты, достоверности, актуальности и защищенности информационного обеспечения деятельности по организации и ведению ТЗИ в органах власти, организациях и предприятиях.

1. Математическая модель для оценки полноты информационного обеспечения деятельности по технической защите информации

Под полнотой информационного обеспечения понимается степень соответствия состава выполняемых услуг информационного обеспечения составу услуг, которые должны предоставляться в соответствии с мо-

4 Т. Саати. Метод анализа иерархий. М.: «Радио и связь». 1993 г.

делью предметной области ТЗИ и уровнем развития методического обеспечения организации и ведения ТЗИ [2, 7]. В связи с этим оценка полноты информационного обеспечения существенно зависит от содержания предметной области ТЗИ, в рамках которой осуществляется деятельность по ТЗИ. В соответствии с [7] модель предметной области ТЗИ формально описывается совокупностью множеств:

$$M(t)=\{F(t),Z(t),L(t),O(t),V(t),R(t)\} \quad (2)$$

где $F(t)=\{f_i(t)|i=\overline{1,I}\}$ – множество функций, реализуемых при организации и ведении ТЗИ. К таким функциям относятся, например, выявление актуальных угроз безопасности информации в ИС, формирование замысла защиты и т.д.;

$Z(t)=\{z_j(t)|j=\overline{1,J}\}$ – множество задач (процедур), решение (выполнение) которых обеспечивает реализацию функций множества F. К таким задачам (процедурам) относятся, например, выявление подлежащей защите информации, определение класса (уровня) защищенности ИС и др.;

$L(t)=\{l_k(t)|k=\overline{1,K}\}$ – множество пользователей защищаемой ИС;

$O(t)=\{o_m(t)|m=\overline{1,M}\}$ – множество информационных объектов, используемых при решении задач ТЗИ. К этому множеству относятся файлы с текстовой и иной информацией, файлы баз данных и т.д., содержащие совокупности сведений и данных, необходимых для организации и ведения ТЗИ, например, сведения о составе и характеристиках ИС, об угрозах безопасности информации и технических каналах утечки, о требованиях правовых нормативных документов, о методическом обеспечении решения задач ТЗИ и т.д.;

$V(t)=\{V_l(t)|l=\overline{1,L}\}$ – множество информационных элементов (атрибутов информационных объектов). Это множество содержит сведения об информационных объектах;

$R(t)=\{r_n(t)|n=1,N\}$ – множество отношений (взаимосвязей) между компонентами модели предметной области $F(t),Z(t),L(t),O(t),V(t)$.

Элементы указанных множеств, кроме множества отношений, представляют собой фреймы, содержащие определенные слоты описания результатов выполнения соответствующих функций.

С учетом содержания модели предметной области ТЗИ полнота информационного обеспечения деятельности по ТЗИ в рамках, например, одной ИС определяется: множеством функций, предусмотренных в модели предметной области $F(t)=\{f_i(t)|i=\overline{1,I}\}$ и действительно реализуемых при организации и ведении ТЗИ $F^{(ИС)}(t)=\{f_i^{(ИС)}(t)|i=\overline{1,I_{ИС}}\}$;;

множеством $Z(t)$ задач (процедур), решение (выполнение) которых обеспечивает реализацию функций множества F, то есть $Z_i(t)=\{z_{ij}(t)|i=\overline{1,I};\ j=\overline{1,J_i}\}$, при этом $J=\sum_{i=1}^{I}J_i$, и множества $Z_i^{(ИС)}(t)$ задач (процедур), решение которых обеспечивает реализацию функций множества $F_{ИС}$, то есть $Z_i^{(ИС)}(t)=\{z_{ij}^{(ИС)}(t)|i=\overline{1,I^{(ИС)}};\ j=\overline{1,J_i^{(ИС)}}\}$, при этом $J^{(ИС)}=\sum_{i=1}^{I}J_i^{(ИС)}$;

множеством $O_{ij}(t)=\{o_{ijn}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}}\}$ информационных объектов, подлежащих использованию в соответствии с моделью предметной области, при этом $N=\sum_{i=1}^{I}\sum_{j=1}^{J_i}N_{ij}$, и множеством $O_{ij}^{(ИС)}(t)=\{o_{ijn}^{(ИС)}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}^{(ИС)}}\}$ информационных объектов, используемых реально при решении задач ТЗИ, при этом $N^{(ИС)}=\sum_{i=1}^{I}\sum_{j=1}^{J_i}N_{ij}^{(ИС)}$;

множеством $V_{ijn}(t)=\{v_{ijnk}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}};k=\overline{1,K_{ijn}}\}$ информационных элементов, атрибутов информационных объектов, в соответствии с моделью предметной области, при этом $K=\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{n=1}^{N_{ij}}K_{ijn}$, и множеством $V_{ijn}^{(ИС)}(t)$ информационных элементов, реально используемых при организации и ведении ТЗИ, $V_{ijn}^{(ИС)}(t)=\{v_{ijnk}^{(ИС)}(t)|i=\overline{1,I};\ j=\overline{1,J_i};\ n=\overline{1,N_{ij}};k=\overline{1,K_{ijn}^{(ИС)}}\}$, при этом $K^{(ИС)}=\sum_{i=1}^{I^{(ИС)}}\sum_{j=1}^{J_i^{(ИС)}}\sum_{n=1}^{N_{ij}^{(ИС)}}K_{ijn}^{(ИС)}$.

Полнота информационного обеспечения характеризует, по сути, охват подлежащих реализации указанных множеств. С учетом изложенного данный показатель может быть рассчитан по следующей формуле:

$$g_{full}(t)=\frac{\sum_{i=1}^{I^{(ИС)}}\delta_{ИС}\left\{f_i^{(ИС)}(t)\right\}\cdot\sum_{j=1}^{J_i^{(ИС)}}\delta_{ИС}\left\{z_{ij}^{(ИС)}(t)\right\}\cdot\sum_{n=1}^{N_{ij}^{(ИС)}}\delta_{ИС}\left\{o_{ijn}^{(ИС)}(t)\right\}\cdot\sum_{k=1}^{K_{ijn}^{(ИС)}}\delta_{ИС}\left\{v_{ijnk}^{(ИС)}(t)\right\}}{\sum_{i=1}^{I}\delta\left\{f_i(t)\right\}\sum_{j=1}^{J_i}\delta\left\{z_{ij}(t)\right\}\sum_{n=1}^{N_{ij}}\delta\left\{o_{ijn}(t)\right\}\sum_{k=1}^{K_{ijn}}\delta\left\{v_{ijnk}(t)\right\}},\quad(3)$$

где

$\delta\{\bullet\}$ – единичная функция, равная единице, если функция (задача, информационный объект или его атрибут) предусмотрена в модели предметной области, и нулю – в противоположном случае;

$\delta_{ИС}\{\bullet\}$ – единичная функция, равная единице, если функция (задача, информационный объект или его атрибут) реально применяются (решаются) при организации и ведении ТЗИ, и нулю – в противоположном случае.

Таким образом, алгоритм оценки показателя полноты информационного обеспечения сводится к последовательному определению состава функций, задач, информационных объектов и информационных элементов, которые предусматриваются при организации и ведении ТЗИ в разработанной модели предметной области ТЗИ и которые реально решаются субъектом деятельности по ТЗИ.

2. Математическая модель для оценки достоверности информационного обеспечения деятельности по технической защите информации

Снижение достоверности информационного обеспечения организации и ведения ТЗИ обусловливается преимущественно ошибками прогноза характеристик предметной области ТЗИ, записываемых в соответствующие базы данных и, прежде всего, ошибками прогноза значений информационных элементов – атрибутов информационных объектов, не измененных к заданному моменту времени. Такие ошибки могут быть оценены следующим образом.

Пусть I – общее количество функций, которые должны выполняться при организации и ведении ТЗИ в соответствии с содержанием предметной области, из которых $I^{(err)}$ к данному моменту времени имеют ошибки в прогнозе значений атрибутов информационных объектов и, в зависимости от размеров ошибок, могут быть неадекватны обстановке, и аналогично J_i и $J_i^{(err)}$ – по решаемым задачам при реализации i-й функции, N_{ij} и $N_{ij}^{(err)}$ – по составу информационных объектов при решении j-й задачи и реализации i-й функции, K_{ijn} и $K_{ijn}^{(err)}$ – по информационным элементам в составе каждого n-го информационного объекта при решении j-й задачи и реализации i-й функции.

Тогда для оценки значения суммарной среднеквадратической ошибки прогноза численных значений[5] атрибутов информационных объектов в ИС имеет место соотношение:

$$\sigma_{\Sigma}^{(v)}(t)=\sqrt{\sum_{i=1}^{I^{(err)}}\delta\left\{f_i(t)\right\}\left[\sum_{j=1}^{J_i^{(err)}}\delta\left\{z_{ij}(t)\right\}\left[\sum_{n=1}^{N_{ij}^{(err)}}\delta\left\{o_{ijn}(t)\right\}\left[\sum_{k=1}^{K_{ijn}^{(num,err)}}\sigma_l^2(t)\,\delta\left\{v_{ijnk}^{(num)}(t)\right\}\right]\right]\right]},\quad(4)$$

где $\sigma_l(t)$ – средняя квадратическая ошибка прогноза значения l-й характеристики (атрибута информационного объекта);

$\delta(\bullet)$ – единичная функция, равная 1, если функция, задача, информационный объект используются при организации и ведении ТЗИ, а информационный элемент не приводит к срыву выполнения задачи или функции, и равна 0 в противоположном случае;

$K_{ijn}^{(num)}$, $K_{ijn}^{(num,err)}$ – общее количество числовых (количественных) атрибутов в составе каждого n-го информационного объекта при решении j-й задачи и реализации i-й функции и количество таких атрибутов, которые имеют ошибки в прогнозе значений, соответственно.

При этом имеют место следующие равенства:

$$J=\sum_{i=1}^{I}J_i,\quad J^{(err)}=\sum_{i=1}^{I^{(err)}}J_i^{(err)},\quad N=\sum_{i=1}^{I}\sum_{j=1}^{J_i}N_{ij},$$
$$N^{(err)}=\sum_{i=1}^{I^{(err)}}\sum_{j=1}^{J_i^{(err)}}N_{ij}^{(err)},K^{(num)}=\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{n=1}^{N_{ij}}K_{ijn}^{(num)},\quad(5)$$

5 В их состав не входят атрибуты, имеющие вербальные описания.

$$K^{(num,err)} = \sum_{i=1}^{I^{(err)}} \sum_{j=1}^{J_i^{(err)}} \sum_{n=1}^{N_{ij}^{(err)}} K_{ijn}^{(num,err)}, \qquad (5)$$

$$K^{(num)} + K^{(num,err)} = K_{IIC}^{(num)} .$$

Следует отметить, что в качестве показателя достоверности ИО может быть использована суммарная среднеквадратическая ошибка прогноза значений атрибутов всех информационных объектов в ИС, однако более адекватным является вероятностная оценка, основанная на расчете вероятности превышения отклонения суммы числовых значений атрибутов информационных объектов, при это суть расчета сводится к следующему.

Суммарное математическое ожидание числовых значений атрибутов информационных объектов рассчитывается по формуле:

$$\overline{k_{\Sigma}^{(v)}(t)} = \frac{\sum_{i=1}^{I^{(err)}} \delta\{f_i(t)\} \left[\sum_{j=1}^{J_i^{(err)}} \delta\{z_{ij}(t)\} \left[\sum_{n=1}^{N_{ij}^{(err)}} \delta\{o_{ijn}(t)\} \left[\sum_{k=1}^{K_{ijn}^{(num,err)}} v_{ijnk}^{(num)}(t) \delta\{v_{ijnk}^{(num)}(t)\} \right] \right] \right]}{K^{(num,err)}}. \qquad (6)$$

Сумма большого количества в общем случае случайных значений количественных атрибутов информационных объектов $\xi(t)$, определяемая к моменту времени t, распределена по нормальному закону[6]:

$$w_{\xi}(x,t) = \frac{1}{\sigma_{\Sigma}^{(v)}\sqrt{2\pi}} \cdot \exp\left\{ -\frac{1}{2} \cdot \left[\frac{x - \overline{k_{\Sigma}^{(v)}(t)}}{\sigma_{\Sigma}^{(v)}(t)} \right]^2 \right\}. \qquad (7)$$

Тогда вероятность того, что ошибка в оценке суммы значений числовых атрибутов информационных объектов $\xi(t)$ не превысит заданного значения a_{lim}, используемая в качестве показателя оценки достоверности информационного обеспечения в ИС, рассчитывается по формуле:

$$g_{rel}^{(num)}(t) = \int_0^{a_{lim}} w_{\xi}(x,t)dx = \Phi_0\left[\frac{a_{lim} - \overline{k_{\Sigma}^{(v)}(t)}}{\sigma_{\Sigma}^{(v)}(t)} \right] - \frac{1}{2}, \qquad (8)$$

где $\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-z^2} dz$ – табулированная функция нормального распределения.

Если атрибуты информационных объектов имеют вербальные описания, то наличие ошибок в их прогнозе определяется путем сравнения слотов их описаний и экспертной оценки существенности таких ошибок. Пусть $K_{ijn}^{(w)}$ и $K_{ijn}^{(w,err)}$ – общее количество атрибутов с вербальным описанием в составе каждого n-го информационного объекта при решении j-й задачи и реализации i-й функции и количество таких атрибутов, для которых имеются ошибки в прогнозе значений, соответственно. Ориентировочно уровень недостоверности ИО по таким атрибутам может быть оценен как отношение количества вербально описанных атрибутов, по которым имеются существенные отклонения в результате ошибок прогнозирования, что может отрицательно повлиять на организацию и ведение ТЗИ, к общему количеству вербально описанных атрибутов. Тогда показатель достоверности ИО по вербально описанным атрибутам оценивается как величина, дополняющая показатель недостоверности до единицы, то есть следующим образом:

$$g_{rel}^{(w)}(t) = 1 - \frac{\sum_{i=1}^{I^{(err)}} \delta\{f_i(t)\} \left[\sum_{j=1}^{J_i^{(err)}} \delta\{z_{ij}(t)\} \left[\sum_{n=1}^{N_{ij}^{(err)}} \delta\{o_{ijn}(t)\} \left[\sum_{k=1}^{K_{ijn}^{(w,err)}} \delta\{v_{ijnk}^{w}(t)\} \right] \right] \right]}{\sum_{i=1}^{I} \delta\{f_i(t)\} \left[\sum_{j=1}^{J_i} \delta\{z_{ij}(t)\} \left[\sum_{n=1}^{N_{ij}} \delta\{o_{ijn}(t)\} \left[\sum_{k=1}^{K_{ijn}^{(w)}} \delta\{v_{ijnk}(t)\} \right] \right] \right]} \qquad (9)$$

При этом имеют место соотношения:

$$\sum_{i=1}^{I^{(w)}} \sum_{j=1}^{J_i^{(w)}} \sum_{n=1}^{N_{ij}^{(w)}} K_{ijn}^{(w)} = K^{(w)}; \sum_{i=1}^{I^{(w)}} \sum_{j=1}^{J_i^{(w)}} \sum_{n=1}^{N_{ij}^{(w)}} K_{ijn}^{(w,err)} = K^{(w,err)}; \; K^{(w)} + K^{(w,err)} = K_{IIC}^{(w)}. \qquad (10)$$

Для оценки достоверности ИО применительно к совокупности как вербальных, так и числовых атрибутов информационных объектов предлагается использовать следующее соотношение:

$$g_{rel}(t) = \frac{g_{rel}^{(w)}(t) \cdot K^{(w,err)} + g_{rel}^{(num)}(t) \cdot K^{(num,err)}}{K^{(w,err)} + K^{(num,err)}}. \qquad (11)$$

6 Справочник по теории вероятностей и математической статистике / В.С.Королюк, Н.И.Портенко, А.В.Скороход, А.Ф.Турбин – М.: «Наука». Главная редакция физико-математической литературы. 1985 г., 640 с.

Полученные соотношения впервые позволяют оценить достоверность информационного обеспечения организации ТЗИ на объектах информатизации.

3. Математическая модель для оценки актуальности информационного обеспечения деятельности по технической защите информации

Вероятность того, что информационное обеспечение станет неактуальным по всей совокупности информации, практически отсутствует. Однако некоторая информация, включенная в описание предметной области, может быть не предусмотрена в ходе прогнозирования или устарела к моменту решения задач организации или ведения ТЗИ и не будет соответствовать реалиям. В связи с этим актуальность информационного обеспечения рассматривается как соответствие информации, применяемой в субъекте деятельности по ТЗИ, реальному состоянию развития предметной области ТЗИ к заданному моменту времени.

Пусть, как и при расчете показателя достоверности, I – общее количество функций, которые должны выполняться при организации и ведении ТЗИ в соответствии с содержанием предметной области, из которых $I^{(act)}$ к данному моменту времени адекватны обстановке, то есть не устарели по сравнению с имеющимися в описании предметной области прогнозными значениями, и аналогично J_i и $J_i^{(act)}$ – то же, но по решаемым задачам при реализации i-й функции, N_{ij} и $N_{ij}^{(act)}$ – по информационным объектам при решении j-й задачи и реализации i-й функции, K_{ijn} и $K_{ijn}^{(act)}$ – по информационным элементам в составе каждого n-го информационного объекта, используемого при решении j-й задачи и реализации i-й функции. При этом имеют место соотношения:

$$K_{ИС}=\sum_{i=1}^{I}\sum_{j=1}^{J_i}\sum_{n=1}^{N_{ij}}K_{ijn},\quad K_{ИС}^{(act)}=\sum_{i=1}^{I^{(act)}}\sum_{j=1}^{J_i^{(act)}}\sum_{n=1}^{N_{ij}^{(act)}}K_{ijn}^{(act)}. \quad (12)$$

Кроме того, положим, что возможно появление новых функций $f_i^{(new)}(t), i=\overline{1,I^{(new)}}$, задач $z_{ij}^{(new)}(t), j=\overline{1,J_i^{new}}, i=\overline{1,I^{(new)}}$, и соответствующим им информационных объектов $o_{ijn}^{(new)}(t), n=\overline{1,N_{ij}^{(new)}}, j=\overline{1,J_i^{new}}, i=\overline{1,I^{(new)}}$ и информационных элементов $v_{ijnk}^{(new)}(t), k=\overline{1,K_{ijnk}^{(new)}}, n=\overline{1,N_{ij}^{(new)}}, j=\overline{1,J_i^{new}}, i=\overline{1,I^{(new)}}$. Пусть известны (заданы экспертным путем или получены на основе обработки статистических данных за предыдущие годы) вероятности появления к моменту времени t новых функций $P_{fi}^{(new)}$ и задач $P_{zij}^{(new)}$. Пример шкалы оценок этих вероятностей приведен в табл. 1. Тогда общее количество новых атрибутов информационных элементов может быть оценено следующим образом:

$$K_{ИС}^{(new)}=\sum_{i=1}^{I^{new}}P_{fi}^{(new)}\delta\left\{f_i^{(new)}(t)\right\}\left[\sum_{j=1}^{J_i^{new}}P_{zij}^{(new)}\delta\left\{z_{ij}^{(new)}(t)\right\}\times\left[\sum_{n=1}^{N_j^{new}}\delta\left\{o_{ijn}^{(new)}(t)\right\}\left[\sum_{k=1}^{K_{ijn}^{new}}\delta\left\{v_{nijk}^{(new)}(t)\right\}\right]\right]\right]. \quad (13)$$

При этом степень актуальности информационного обеспечения деятельности по ТЗИ может быть оценена по формуле:

$$g_{акт}(t)=1-\frac{K_{ИС}-K_{ИС}^{(act)}+K_{ИС}^{(new)}}{K_{ИС}+K_{ИС}^{(new)}}=\frac{K_{ИС}^{(act)}}{K_{ИС}+K_{ИС}^{(new)}}. \quad (14)$$

Полученное соотношение впервые позволяет рассчитать показатель актуальности информационного ТЗИ и количественно оценить, насколько в действующей модели предметной области учтены возможные инновации.

4. Математическая модель для оценки защищенности информационного обеспечения деятельности по технической защите информации

Защищенность информационного обеспечения деятельности по ТЗИ достигается парированием (нейтрализацией) возможных угроз функционированию ИС, используемой в органе, организации, на предприятии для автоматизации этой деятельности, угроз нарушения конфиденциальности, целостности и доступности прикладных программ и данных, необходимых для организации и ведения ТЗИ.

Указанные угрозы могут реализовываться на сетевом (при передаче защищаемой информации по сети), системном (на уровне операционной системы) и прикладном (на уровне прикладных программ и данных) системно-технических уровнях[7] [8]. При этом угрозы на сетевом уровне реализуются путем перехвата трафика, а на системном и прикладном – путем проникновения в операционную среду ИС. Состав актуальных угроз определяется в частной модели угроз, которая должна составляться для каждой ИС.

Состав мер и средств защиты, которые должны

7 Угрозы на микропрограммном уровне в данной работе не рассматриваются.

Таблица 1

Экспертная шкала оценок возможности возникновения новых функций и задач, подлежащих учету при организации и ведении ТЗИ

Критерий возникновения новой функции	Вербальная оценка возможности возникновения новой функции	Вероятность возникновения новой функции	Критерий возникновения новой задачи	Вербальная оценка возможности возникновения новой задачи	Вероятность возникновения новой задачи
Имеются публикации, подтверждающие возможность появления инноваций: новых технологий обработки информации, новых угроз безопасности, новых нормативных и методических документов, новых мер и средств защиты информации и т.д.	Высокая	$P_{fi}^{(new)} > 0.8$	Путем решения известных задач невозможно выполнить новую функцию, необходимо решать для ее выполнения новые задачи	Высокая	$P_{zij}^{(new)} > 0.8$
			Решением известных задач частично можно выполнить новую функцию, однако для решения некоторых из задач, возможно, потребуется новое методическое обеспечение или новые исходные данные	Средняя	$0.4 < P_{zij}^{(new)} \le 0.8$
			Предположительно возможно обеспечить выполнение новой функции путем решения известных задач	Низкая	$P_{zij}^{(new)} \le 0.4$
Имеются сведения, свидетельствующие лишь о возможности разработки инноваций	Средняя	$0.4 < P_{fi}^{(new)} \le 0.8$	Путем решения известных задач невозможно выполнить новую функцию, необходимо решать для ее выполнения новые задачи	Высокая	$P_{zij}^{(new)} > 0.8$
			Решением известных задач частично можно выполнить новую функцию, однако для решения некоторых из задач, возможно, потребуется новое методическое обеспечение или новые исходные данные	Средняя	$0.4 < P_{zij}^{(new)} \le 0.8$
			Предположительно возможно обеспечить выполнение новой функции путем решения известных задач	Низкая	$P_{zij}^{(new)} \le 0.4$
Сведения, свидетельствующие о сроках появления инноваций весьма неопределенные или отсутствуют	Низкая	$P_{fi}^{(new)} \le 0.4$	Путем решения известных задач невозможно выполнить новую функцию, необходимо решать для ее выполнения новые задачи	Высокая	$P_{zij}^{(new)} > 0.8$
			Решением известных задач частично можно выполнить новую функцию, однако для решения некоторых из задач, возможно, потребуется новое методическое обеспечение или новые исходные данные	Средняя	$0.4 < P_{zij}^{(new)} \le 0.8$
			Предположительно возможно обеспечить выполнение новой функции путем решения известных задач	Низкая	$P_{zij}^{(new)} \le 0.4$

применяться в интересах парирования угроз, определяется классом защищенности ИС и соответствующим этому классу составом мер защиты, регламентированным нормативными документами ФСТЭК России. Чем выше класс защищенности, тем меньше вероятность того, что принятая мера может быть преодолена в ходе реализации той или иной угрозы.

Для парирования возможности перехвата трафика, поступающего в ИС органа власти, организации, предприятия или передаваемого с защищаемой ИС в вышестоящие инстанции или другим органам власти, организациям и предприятиям, как правило, применяются частные виртуальные сети с криптографической защитой, реализуемой с применением сертифицированных ФСБ России криптографических средств, при этом считается, что такая защита является достаточной.

В связи с этим оценку защищенности целесообразно проводить только относительно угроз на системном и прикладном уровнях, то есть относительно угроз, реализация которых связана с проникновением в операционную среду ИС, в том числе с внедрением вредоносных программ. Особенности такой оценки заключаются в следующем.

1. Оценка защищенности от угроз нарушения конфиденциальности, целостности и доступности защищаемой информации должна быть привязана к самой информации, то есть к пользовательским программам и данным, и охватывать всю защищаемую информацию, циркулирующую в ИС. До сих пор оценка защищенности не проводилась относительно всего объема подлежащей защите информации, а выбирались лишь отдельные файлы и применительно к каждому из них оценивалась возможность реализации угрозы без мер защиты и в условиях применения мер защиты. Поскольку объемы защищаемой информации даже в одном компьютере весьма велики, крайне сложной оказывается и оценка защищенности информационного обеспечения деятельности по ТЗИ, то есть защищенности всей информации, необходимой для организации и ведения ТЗИ. Более того, даже подход к такой оценке фактически не разрабатывался.

2. При оценке защищенности информационного обеспечения от угроз, связанных с проникновением в операционную среду, необходимо учитывать то, что для разных угроз несанкционированные (деструктивные) действия, определяющие содержание угрозы, различны. Так, угрозы нарушения конфиденциальности информации реализуются путем несанкционированного копирования соответствующих файлов с записью в выбранные области постоянной памяти с последующей их передачей (возможно скрытной) по нужному сетевому адресу или на отчуждаемый носитель. Угрозы нарушения целостности информации реализуются путем полного или частичного уничтожения (стирания) информации, полной или частичной ее подмены. Угрозы нарушения доступности пользовательской информации реализуются путем изменения пути к файлам с такой информацией (несанкционированной перезаписи файлов в иные каталоги и директории), нарушения таблиц дескрипторов файлов и др. [8 – 11]. При этом, во-первых, имеется существенная неопределенность, относительно какой защищаемой информации и какое конкретно будет выполняться несанкционированное действие с защищаемой информацией. Во-вторых, при реализации всех таких угроз сначала осуществляется проникновение в операционную среду. Таким образом, при оценке защищенности необходимо в первую очередь оценить возможность проникновения в операционную среду в условиях применения мер защиты, а затем – возможность выполнения какого-либо из несанкционированных действий или совокупности таких действий, направленных на нарушение конфиденциальности, целостности или доступности информации.

3. Для количественной оценки защищенности информационного обеспечения необходимо иметь математические модели процессов реализации угроз безопасности информации, используемой для организации и ведения ТЗИ. Некоторые из таких моделей разработаны, например, в [8, 11 – 13]. Однако применительно к оценке защищенности информационного обеспечения в условиях огромного разнообразия угроз безопасности информации и мер защиты от них таких моделей сегодня явно не хватает, поэтому применительно к рассматриваемой проблеме в данной работе был предложен метод, основанный на использовании нечетких оценок вероятностей реализации угроз безопасности информации[8]. Однако применительно к проблеме ИО деятельности по ТЗИ до сих пор не рассматривался. Суть этого метода сводится к следующему.

Пусть в условиях отсутствия мер защиты вероятности реализации угроз безопасности как системной,

8 Например, в статье Язова Ю.К., Середы О.А. «Комплексная оценка эффективности защиты от угроз безопасности с использованием аппарата теории нечетких множеств» // Региональный научный вестник «Информация и безопасность» / ВГТУ Воронеж, 2001 г. Вып.2., в монографии Корченко А.Г. «Построение систем защиты информации на нечетких множествах. Теория и практическое решение»/ Киев: «МК-Пресс», 2006. – 216 с. и др.

так и прикладной информации близки к единице. Тогда ее защищенность может быть оценена нечетким значением показателя g_{prot}, соответствующего нечеткой вероятности того, что угрозы не могут быть реализованы в ИС, рассчитываемым по формуле:

$$g_{prot} = 1 - P_{imp} \cdot \left\{ \gamma_1 \cdot P_{syst} + \gamma_2 \cdot P_{app} \right\}, \quad (15)$$

где P_{imp} – нечеткая оценка вероятности проникновения в операционную среду ИС в условиях применения адекватных мер защиты;

$$P_{imp} = \pi_1 P_{imp.1} + \pi_2 P_{imp.2}, \quad (16)$$

π_1 и π_2 – априорные вероятности реализации первого и второго варианта проникновения соответственно, $\pi_1 + \pi_2 = 1$;

P_{imp1} и P_{imp2} – нечеткие оценки вероятности проникновения при действиях внешнего и внутреннего нарушителя соответственно;

P_{syst} – нечеткая оценка условной вероятности выполнения несанкционированных (деструктивных) действий файлов операционной системы, то есть относительно системной информации, приводящих к отказу в обслуживании пользователей, при условии проникновения в операционную среду и при наличии мер защиты;

P_{app} – нечеткая оценка условной вероятности выполнения несанкционированных действий относительно текстовых, графических, видео- и аудиофайлов, а также исполняемых файлов прикладных программ пользователей[9], то есть относительно пользовательской информации, при условии проникновения в операционную среду и при наличии мер защиты;

γ_1 и γ_2 – априорные вероятности того, что после проникновения будут выполняться действия, направленные на нарушение безопасности системной информации с отказом функционирования ИС (угрозы отказа ИС в обслуживании), или действия, направленные на нарушения целостности, конфиденциальности или доступности пользовательской информации, при этом имеет место условие $\gamma_1 + \gamma_2 = 1$.

Для определения вероятности проникновения учитываются первоочередные меры разграничения доступа такие как:

- межсетевое экранирование;
- идентификация и аутентификация;
- антивирусная защита;
- обнаружение вторжений, в том числе незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);
- выявление нарушений целостности, доступности и работоспособности программного обеспечения и средств защиты информации, отклонения параметров его настройки от номинальных;
- контроль состава технических средств, в том числе средств защиты информации и сигнализация о выявленных нарушениях;
- прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения.

Полагается, что у нарушителя имеется достаточно времени для реализации любой угрозы и, таким образом, оценивается потенциальная возможность такой реализации без учета ее динамики [8, 12].

Если применяются адекватные меры защиты, то угроза проникновения в операционную среду возможна в случае эксплуатации неизвестной ранее уязвимости системного программного обеспечения и внедрения вредоносной программы, обеспечивающей такое проникновение. В настоящее время большинство угроз проникновения реализуются с применением вредоносных программ, при этом имеется два варианта проникновения: первый – из внешней сети, второй – путем проведения сетевой атаки с одного из компьютеров ИС этого органа, организации, предприятия, при этом возможна реализация несанкционированных действий и относительно информации, находящейся на этом компьютере.

При использовании аппарата нечетких множеств [14] наиболее удобным является использование треугольных нечетких чисел. Пример представления нечеткого треугольного числа, например, для вероятности проникновения в операционную среду приведен на рис.1.

На рисунке $\mu_{P_{imp}}(x)$ – функция принадлежности нечеткого числа P_{imp} заданному множеству значений (в данном случае интервалу значений от 0.25 до 0.7). В аналитическом виде функция принадлежности, показанная на рис.1, записывается следующим образом: $\mu_{P_{imp}}(x) = \left\{ \frac{0}{0.25}; \frac{1}{0.4}; \frac{0}{0.7} \right\}$, где в числителях указываются значения функции принадлежности, а в знаменателях значения нечеткого числа.

9 Здесь не рассматриваются маловероятные случаи, когда угрозы одновременно направлены как на нарушение безопасности прикладной информации, так и на отказ в обслуживании пользователей операционной системы.

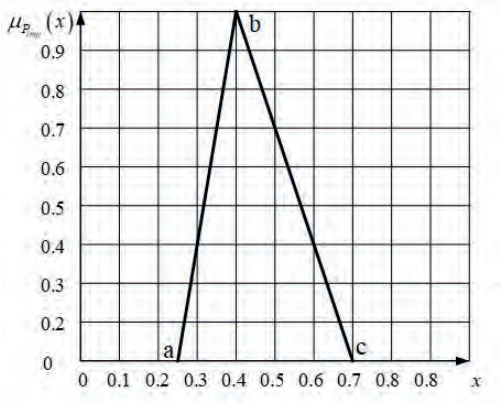

Рис.1. Пример представления треугольного нечеткого числа при оценке вероятности проникновения в операционную среду

Аналогичным образом описывается само нечеткое число, равное примерно 0.4:

$$P_{imp} = \left\{ \begin{array}{c|c|c|c} \mu_{P_{imp}}(x) & 0 & 1 & 0 \\ \hline x & 0.25 & 0.4 & 0.7 \end{array} \right\} \equiv \left\{ \frac{0}{0.25}, \frac{1}{0.4}, \frac{0}{0.7} \right\}$$

Сумма и произведение K треугольных нечетких чисел вида $A_k = \left\{ \frac{0}{a_k}; \frac{1}{b_k}; \frac{0}{c_k} \right\}, k = \overline{1,K}$, представляют собой нечеткие числа следующего вида:

$$\sum_{k=1}^{K} A_k = \left\{ \frac{0}{\sum_{k=1}^{K} a_k}; \frac{1}{\sum_{k=1}^{K} b_k}; \frac{0}{\sum_{k=1}^{K} c_k} \right\},$$

$$\prod_{k=1}^{K} A_k = \left\{ \frac{0}{\prod_{k=1}^{K} a_k}; \frac{1}{\prod_{k=1}^{K} b_k}; \frac{0}{\prod_{k=1}^{K} c_k} \right\}. \quad (17)$$

Последовательно можно рассчитать функции принадлежности для любого числа перемножаемых нечетких чисел. Если необходимо возвести в степень нечеткое число $A = \left\{ \frac{0}{a}; \frac{1}{b}; \frac{0}{c} \right\}$, то из (17) следует:

$$A^K = \left\{ \frac{0}{a^K}; \frac{1}{b^K}; \frac{0}{c^K} \right\}. \quad (18)$$

Наконец, важным моментом арифметики нечетких чисел в случае, когда рассматриваются нечеткие вероятности, является определение дополнения нечеткой вероятности до 1, то есть, если задана вероятность в виде нечеткого треугольного числа $P = \left\{ \frac{0}{a}, \frac{1}{b}, \frac{0}{c} \right\}$, то нечеткое треугольное число $1 - P$ определяется следующим образом:

$$1 - P = \left\{ \frac{0}{1-c}; \frac{1}{1-b}; \frac{0}{1-a} \right\}. \quad (19)$$

Использование аппарата нечетких множеств позволяет учесть неопределенности, которые возникают у специалистов при проведении анализа защищенности ИО деятельности по ТЗИ от угроз безопасности информации.

Вероятность P_{syst} выполнения несанкционированного (деструктивного) действия относительно системной информации, то есть относительно любого из файлов (исполняемых, файлов дескрипторных таблиц и др.), нарушение целостности, уничтожение или модификация которых приводит к нарушению функционирования ИС в условиях применения мер защиты, определяется возможностью запуска и выполнения соответствующих команд операционной системы. Пусть в операционной системе имеется K_{sys} таких файлов, нечеткая оценка вероятности уничтожения, модификации, подмены каждого k-го файла составляет величину $P^{(F)}_{syst.k}$, тогда нечеткая оценка условной вероятности выполнения несанкционированных (деструктивных) действий относительно файлов операционной системы, приводящих к отказу в обслуживании пользователей, при условии проникновения в операционную среду и при наличии мер защиты находится из соотношения:

$$P_{syst} = 1 - \prod_{k=1}^{K_{sys}} \left[1 - P^{(F)}_{syst.k} \right]. \quad (20)$$

Если вместо $P^{(F)}_{syst.i}$ использовать усредненное нечеткое значение вероятности

$$\overline{P^{(F)}_{syst.}} = \frac{1}{K_{sys}} \cdot \sum_{k=1}^{K_{sys}} P^{(F)}_{syst.k}, \quad (21)$$

то

$$P_{syst} = 1 - \left[1 - \overline{P^{(F)}_{syst}} \right]^{K_{sys}}. \quad (22)$$

Далее проводится дефаззификация, то есть получение четкого значения этой вероятности. При этом может быть использованы разные методы, такие как методы среднего максимума, «центра тяжести», центра сумм и т.д. [13].

Наиболее корректным из них является метод центра тяжести, при этом, если получено треугольное число в виде: $P_{syst} = \left\{ \frac{0}{a_{syst}}; \frac{1}{b_{syst}}; \frac{0}{c_{syst}} \right\}$, то четкое значение этой вероятности рассчитывается следующим образом:

$$P_{syst} = \frac{\int_{a_{syst}}^{b_{syst}} x \cdot \mu_{P_{syst}}(x)\,dx + \int_{b_{syst}}^{c_{syst}} x \cdot \mu_{P_{syst}}(x)\,dx}{\int_{a_{syst}}^{b_{syst}} \mu_{P_{syst}}(x)\,dx + \int_{b_{syst}}^{c_{syst}} \mu_{P_{syst}}(x)\,dx}, \quad (23)$$

откуда

$$P_{syst} = \frac{b_{syst}^2 - a_{syst}b_{syst} - a_{syst}^2 - b_{syst}c_{syst} + 2c_{syst}^2}{3\left(c_{syst} - a_{syst}\right)} \quad (24)$$

Например, если $P_{syst} = \left\{ \frac{0}{0.6}; \frac{1}{0.8}; \frac{0}{0.9} \right\}$, то после дефаззификации $P_{syst} = 0.77$.

Нечеткая оценка условной вероятности P_{app} выполнения несанкционированных действий относительно пользовательской информации находится следующим образом.

Пусть в ИС имеются K_{conf} файлов, содержащих защищаемую информацию конфиденциального характера, K_{int} файлов, содержащих информацию, целостность которой не должна быть нарушена, и K_{acc} файлов, доступность к которым должна быть обеспечена. Тогда нечеткая оценка вероятности выполнения несанкционированных действий относительно указанных файлов определяется из соотношения:

$$P_{app} = \theta_{conf} \cdot P_{conf} + \theta_{int} \cdot P_{int} + \theta_{acc} \cdot P_{acc}, \quad (25)$$

где $P_{conf}, P_{int}, P_{acc}$ – нечеткие оценки вероятностей выполнения действий, направленных на нарушение конфиденциальности, целостности и доступности хотя бы одного из соответствующих файлов с пользовательской информацией;

θ_{conf}, θ_{int}, θ_{acc} – априорные вероятности того, что будет выбрано действие, направленное на нарушение конфиденциальности, целостности или доступности пользовательской информации соответственно;

K_j – количество файлов, защищаемых от j-го несанкционированного действия, $j = \overline{1,3}$, при этом $K_1 \equiv K_{conf}, K_2 \equiv K_{\text{int}}, K_3 \equiv K_{acc}$;

θ_j – априорная вероятность того, что будет выбрано для выполнения j-е несанкционированное действие, направленное на нарушение или конфиденциальности, или целостности или доступности информации, $\sum_{j=1}^{3} \theta_j = 1$.

Если рассматривается наиболее жесткая оценка защищенности, когда считается, что недопустимо нарушение конфиденциальности, целостности или доступности ни одного из файлов с пользовательской информацией в системе, то

$$P_{conf} = 1 - \prod_{k=1}^{K_{conf}} \left[1 - P_{conf.k} \right];$$
$$P_{int} = 1 - \prod_{k=1}^{K_{int}} \left[1 - P_{int.k} \right]; P_{acc} = 1 - \prod_{k=1}^{K_{acc}} \left[1 - P_{acc.k} \right], \quad (26)$$

где $P_{conf.k}, P_{int.k}, P_{acc.k}$ – нечеткие оценки вероятностей выполнения действий, направленных на нарушение конфиденциальности, целостности или доступности k-го файла соответственно.

Если рассматривается менее жесткая оценка защищенности, когда считается, что недопустимо нарушение сразу всех рассматриваемых файлов пользовательской информации, то

$$P_{conf} = \prod_{k=1}^{K_{conf}} P_{conf.k}; P_{int} = \prod_{k=1}^{K_{int}} P_{int.k}; P_{acc} = \prod_{k=1}^{K_{acc}} P_{acc.k}. \quad (27)$$

Если использовать усредненную оценку нечетких значений вероятностей по каждому из возможных несанкционированных действий, то формула (25) преобразуется к виду:

$$P_{app} = \theta_{conf} \cdot \left[1 - (1 - \overline{P_{conf}})^{K_{conf}} \right] + \\ + \theta_{int} \cdot \left[1 - (1 - \overline{P_{int}})^{K_{int}} \right] + \theta_{acc} \cdot \left[1 - (1 - \overline{P_{acc}})^{K_{acc}} \right], \quad (28)$$

где $\overline{P_{conf}}, \overline{P_{\text{int}}}, \overline{P_{acc}}$ – средние вероятности выполнения несанкционированных действий, направленных соответственно на нарушение конфиденциальности, целостности и доступности информации,

$$\overline{P_{conf}} = \frac{1}{K_{conf}} \cdot \sum_{k=1}^{K_{conf}} P_{conf.k};$$
$$\overline{P_{int}} = \frac{1}{K_{int}} \cdot \sum_{k=1}^{K_{int}} P_{int.k}; \overline{P_{acc}} = \frac{1}{K_{acc}} \cdot \sum_{k=1}^{K_{acc}} P_{acc.k}; \quad (29)$$

$\theta_{conf}, \theta_{int}, \theta_{acc}$ – априорные вероятности вы-

Таблица 2

Шкала перевода количественных значений показателя защищенности информационного обеспечения в качественные суждения

Количественные значения показателя защищенности g_{prot}	$g_{prot} > 0.99$	$0.99 \geq g_{prot} > 0.8$	$g_{prot} < 0.8$
Качественные суждения об уровне защищенности	Высокий	Средний	Низкий

бора несанкционированных действий, $\theta_{conf} \equiv \theta_1, \theta_{int} \equiv \theta_2, \theta_{acc} \equiv \theta_3$;

$P_{conf.k}, P_{int.k}, P_{acc.k}$ – вероятности выполнения несанкционированного действия относительно k-го файла, направленного на нарушение соответственно конфиденциальности, целостности или доступности содержащейся в нем информации.

Рассчитанный по формуле (15) показатель защищенности информационного обеспечения может быть переведен в качественные суждения по шкале, указанной в табл. 2.

Пример. Пусть количество системных файлов, реализация угрозы нарушения целостности или доступности которых приводит к отказу в обслуживании (например, к «зависанию» операционной системы) составляет $K_{syst} = 50$. Угрозы могут реализованы как по сети, так и с одного из компьютеров ИС, при этом возможности проникновения в операционную среду ИС в условиях мер защиты как по первому, так и по второму варианту проникновения равны, то есть вероятности $P_{imp}^{(1)} = P_{imp}^{(2)} = \left(\frac{0}{7\cdot10^{-3}}, \frac{1}{10^{-2}}, \frac{0}{3\cdot10^{-2}}\right)$ и $\pi_1 = \pi_2 = 0.5\cdot10^{-2}$. Априорные вероятности того, что угроза будет реализована относительно системной или пользовательской информации равны соответственно $\gamma_{syst} = 0.6$ и $\gamma_{app} = 0.4$, а нечеткая оценка вероятности того, что относительно одного системного файла будет выполнено несанкционированное действие, составляет величину $P_{syst.k}^{(F)} = \left(\frac{0}{0.01}, \frac{1}{0.02}, \frac{0}{0.03}\right)$, одинаковую для всех системных файлов.

Пусть количество файлов пользовательской информации, относительно которых могут быть реализованы угрозы нарушения конфиденциальности, целостности и доступности, равны соответственно $K_{conf} = 10, K_{int} = 20, K_{acc} = 7$, а априорные вероятности выбора действий $\theta_{conf} = 0.6, \theta_{int} = 0.3, \theta_{acc} = 0.1$. Нечеткие значения вероятностей выполнения несанкционированных действий относительно файлов с пользовательской информацией в случае нарушения конфиденциальности, целостности и доступности одинаковы для соответствующих файлов

$$P_{conf.k} = \left(\frac{0}{0.2}, \frac{1}{0.3}, \frac{0}{0.4}\right),$$

$$P_{int.k} = \left(\frac{0}{0.88}, \frac{1}{0.96}, \frac{0}{0.99}\right),$$

$$P_{acc.k} = \left(\frac{0}{10^{-3}}, \frac{1}{10^{-2}}, \frac{0}{10^{-1}}\right).$$

Необходимо оценить защищенность информации, используемой в деятельности по ТЗИ.

Усредненное нечеткое значение вероятности реализации угроз относительно системных файлов рассчитывается по формуле (20): $\overline{P_{syst.}^{(F)}} = P_{syst}^{(F)} = \left(\frac{0}{0.01}, \frac{1}{0.02}, \frac{0}{0.03}\right)$, при этом дополнение до 1 этой вероятности представляет собой нечеткое число: $1 - P_{syst}^{(F)} = \left(\frac{0}{0.97}, \frac{1}{0.98}, \frac{0}{0.99}\right)$.

Отсюда в соответствии с формулами (17), (18) и (21) получаем $P_{syst} = \left(\frac{0}{0.4}, \frac{1}{0.64}, \frac{0}{0.78}\right)$.

Применительно к пользовательской информации находим аналогично:

$$P_{conf} = \left(\frac{0}{0.89}, \frac{1}{0.97}, \frac{0}{0.994}\right);$$

$$P_{\text{int}} = \left(\frac{0}{0.12}, \frac{1}{0.15}, \frac{0}{0.2}\right);$$

$$P_{acc} = \left(\frac{0}{0.007}, \frac{1}{0.07}, \frac{0}{0.52}\right).$$

По формуле (27) находим нечеткую оценку вероятности выполнения несанкционированных действий относительно указанных файлов: $P_{app} = \left(\frac{0}{0.57}, \frac{1}{0.63}, \frac{0}{0.7}\right)$. Далее по формуле (15) оценивается нечеткое значение показателя защищенности $g_{prot} = \left(\frac{0}{0.98}, \frac{1}{0.993}, \frac{0}{0.997}\right)$.

В результате дефаззификации по формуле, аналогичной формуле (24), получаем $g_{prot} = 0.98$. В соответствии с табл. 2 уровень защищенности информационного обеспечения – средний.

Выводы

1. Разработаны математические модели для количественной оценки показателей полноты, достоверности, актуальности и защищенности информационного обеспечения деятельности по организации и ведению ТЗИ в органах власти, организациях и предприятиях и показана их связь с комплексным показателем эффективности такого обеспечения. Модели необходимы при построении систем информационного обеспечения деятельности по ТЗИ и позволяют перейти от качественных к количественным оценкам его эффективности и тем самым, во-первых, существенно повысить обоснованность требований к СИО, во-вторых, автоматизировать процессы информационного обеспечения деятельности по ТЗИ в органах власти, организациях и предприятиях.

2. Предложенные показатели качества информационного обеспечения и аналитические соотношения для их расчета использованы при построении и сопровождении функционирования информационно-аналитической системы ФСТЭК России, а также в ходе аудита при проверке информационного обеспечения деятельности по ТЗИ в органах власти, организациях и предприятиях.

Литература:

1. Ю.К.Язов. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К.Язов, С.В.Соловьев. Воронеж: Кварта, 2018. – 588 с.
2. Соловьев С. В. Информационное обеспечение деятельности по технической защите информации / С.В. Соловьев, Ю.К. Язов / Вопросы кибербезопасности. 2021, №1 (41), с. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79
3. Сюнтюренко О.В. Информационное обеспечение: факторы развития, управление, эффективность. Научно-техническая информация. Серия 2: Информационные процессы и системы. 2016. №6. С 7–15.
4. Трояновская М. А. Информационное обеспечение деятельности органов государственного управления: понятие и значение. Международный научно-исследовательский журнал. 2020. №5-2(95). С.100-103.
5. Чернов В. А. Теория экономического анализа. Изд-во ООО «Проспект». – М.: 2017.
6. Сазанова Л. А. Анализ особенностей производственной функции Кобба-Дугласа. В сборнике: Актуальные тенденции и инновации в развитии российской науки / сборник научных статей. Москва. 2020. С. 120–123.
7. Колесникова, Е. В. Моделирование развития информационного обеспечения организационно-технических систем технической защиты информации с учетом прогноза изменений предметной области / Е. В. Колесникова // Сборник докладов международной конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2016», Российское научно-техническое общество радиотехники, электроники и связи им. А. С. Попова. – 2016. – том 2 – С. 564–569.
8. Язов Ю. К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с.
9. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.
10. Бутрик Е.Е. Подход к определению актуальных угроз безопасности информации в автоматизированных системах управления технологическими процессами с применением банка данных угроз безопасности информации ФСТЭК России / Е.Е.Бутрик, С.В.Соловьев // Информация и безопасность. – Воронеж,2018. – Выпуск 19 (2). – с.203 – 210.
11. Олифер, В.Г. Безопасность компьютерных систем / В.Г.Олифер, Н.А.Олифер – М.: Горячая линия – Телеком, 2017.– 644 с.: илл.
12. Язов, Ю.К. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография / Ю. К. Язов, А. В. Анищенко. – Воронеж: Кварта,2020. 173 с.
13. Рубцова, И.О. Об оценке эффективности защиты электронного документооборота с применением аппарата сетей Петри-Маркова [Текст] / И. О. Рубцова, Ю. К. Язов, О.С. Авсентьев, А.О. Авсентьев // Труды СПИИРАН, №5(25) – 2019.
14. Пегат, А. Нечеткое моделирование и управление / А.Пегат; пер. с англ.– 2-е изд. – М.: БИНОМ. Лаборатория знаний, 2015. – 798 с.: ил. – (Адаптивные интеллектуальные системы).

MATHEMATICAL MODELS FOR ASSESSING QUALITY INDICATORS OF INFORMATION SUPPORT OF TECHNICAL INFORMATION PROTECTION ACTIVITIES

Soloviev S.V.[10], Yazov Yu.K.[11], Teplinskikh A.A.[12]

The purpose of the research *is to develop mathematical models for quantitative assessment of indicators of completeness, reliability, relevance and security of information support for organizing and maintaining technical information protection in government agencies, organizations and enterprises*

The methods of research are: *mathematical apparatus of factor analysis, methods of set theory, fuzzy number theory and probability theory.*

The result of the research: *indicators for assessing the quality of information support for technical information protection activities are proposed: completeness, reliability, relevance and security of information necessary for such support; the correlation of these quality indicators with a comprehensive indicator for assessing the effectiveness of information support is revealed. Taking into account the content of the subject area model of technical information protection, it is shown that the completeness, reliability and relevance of security information support is determined by the sets of: functions provided for in the subject area model and actually implemented in the information system; tasks, the solution of which ensures the implementation of functions; information objects and their attributes to be used in accordance with the domain model and actually used in solving information security problems. To assess the indicator of information security required for information support of information protection activities, it is proposed to use a device for fuzzy estimates of the probabilities of the implementation of threats regarding system and user information, violation of the confidentiality, integrity or availability of which can disrupt the information support.*

Analytical relations have been developed to calculate the quality indicators of in-formation support, makes it possible to quantify the requirements for information support of information protection activities and for the created information support systems for government agencies, organizations and enterprises.

Keywords: *information system, effectiveness, subject area, completeness, reliability, relevance, information protection.*

References

1. Ju.K.Jazov. Organizacija zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju.K.Jazov, S.V.Solov'ev. Voronezh: Kvarta, 2018. – 588 s.
2. Solov'ev S. V. Informacionnoe obespechenie dejatel'nosti po tehnicheskoj zashhite informacii / S.V. Solov'ev, Ju.K. Jazov / Voprosy kiberbezopasnosti. 2021, №1 (41), s. 69–79. DOI: 10.21681/2311-3456-2021-1-69-79
3. Sjuntjurenko O.V. Informacionnoe obespechenie: faktory razvitija, upravlenie, jeffektivnost'. Nauchno-tehnicheskaja informacija. Serija 2: Informacionnye processy i sistemy. 2016. №6. S 7–15.
4. Trojanovskaja M. A. Informacionnoe obespechenie dejatel'nosti organov gosudarstvennogo upravlenija: ponjatie i znachenie. Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. 2020. №5-2(95). S.100-103.
5. Chernov V. A. Teorija jekonomicheskogo analiza. Izd-vo 000 «Prospekt». – M.: 2017.
6. Sazanova L. A. Analiz osobennostej proizvodstvennoj funkcii Kobba-Duglasa. V sbornike: Aktual'nye tendencii i innovacii v razvitii rossijskoj nauki / sbornik nauchnyh statej. Moskva. 2020. S. 120–123.
7. Kolesnikova, E. V. Modelirovanie razvitija informacionnogo obespechenija organizacionno-tehnicheskih sistem tehnicheskoj zashhity informacii s uchetom prognoza izmenenij predmetnoj oblasti / E. V. Kolesnikova // Sbornik dokladov mezhdunarodnoj konferencii

10 Sergey V. Soloviev, Ph.D. (Technology), Associate Professor, Deputy Head ofof the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russian Federation. E-mail:sersol@mail.ru

11 Yuri K. Yazov, Dr.Sc. (Technology), Professor, Principal Researcher at the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russian Federation. E-mail:yazoff_1946@mail.ru

12 Alexander A. Teplinskikh, Researcher of the State Scientific and Research Testing Institute for the Problems of Technical Protection of Information of the Federal Service for Technical and Export Control of Russia, Voronezh, Russian Federation. E-mail:ma4karek48@yandex.ru

«Radiojelektronnye ustrojstva i sistemy dlja infokommunikacionnyh tehnologij – RJeUS-2016», Rossijskoe nauchno-tehnicheskoe obshhestvo radiotehniki, jelektroniki i svjazi im. A. S. Popova. – 2016. – tom 2 – S. 564–569.
8. Jazov Ju. K. Metodologija ocenki jeffektivnosti zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju.K. Jazov, S.V. Solov'ev. – Sankt-Peterburg: Naukoemkie tehnologii, 2023. – 258 s.
9. Vasil'ev V. I., Vul'fin A. M., Kirillova A. D., Kuchkarova N. V. Metodika ocenki aktual'nyh ugroz i ujazvimostej na osnove tehnologij kognitivnogo modelirovanija i Text Mining // Sistemy upravlenija, svjazi i bezopasnosti. 2021. № 3. S. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.
10. Butrik E.E. Podhod k opredeleniju aktual'nyh ugroz bezopasnosti informacii v avtomatizirovannyh sistemah upravlenija tehnologicheskimi processami s primeneniem banka dannyh ugroz bezopasnosti informacii FSTJeK Rossii / E.E.Butrik, S.V.Solov'ev // Informacija i bezopasnost'. – Voronezh,2018. – Vypusk 19 (2). – s.203 – 210.
11. Olifer, V.G. Bezopasnost' komp'juternyh sistem / V.G.Olifer, N.A.Olifer – M.: Gorjachaja linija – Telekom, 2017.– 644 s.: ill.
12. Jazov, Ju.K. Seti Petri-Markova i ih primenenie dlja modelirovanija processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah: monografija / Ju. K. Jazov, A. V. Anishhenko. – Voronezh: Kvarta,2020. 173 s.
13. Rubcova, I.O. Ob ocenke jeffektivnosti zashhity jelektronnogo dokumentooborota s primeneniem apparata setej Petri-Markova [Tekst] / I. O. Rubcova, Ju. K. Jazov, O.C. Avsent'ev, A.O. Avsent'ev // Trudy SPIIRAN, №5(25) – 2019.
14. Pegat, A. Nechetkoe modelirovanie i upravlenie / A.Pegat; per. s angl.– 2-e izd. – M.: BINOM. Laboratorija znanij, 2015. – 798 s.: il. – (Adaptivnye intellektual'nye sistemy).