– скоротити час виявлення диктофона за рахунок того, що скануванню та оцінці піддаються лише характерні ділянки спектру, а не весь спектр паразитного випромінювання ЦД;

– виявляти цифрові диктофони будь-яких моделей (пошук цифрових диктофонів з іншим спектром випромінювання здійснюється після доповнення банку характерних частот);

– динамічно формувати банк пам'яті характерних частот залежно від поставлених задач та умов роботи (надійність виявлення, час виявлення, наявність завад тощо);

– застосовувати пристрій у носимому або стаціонарному варіантах використання;

– значно підвищити відстань виявлення та надійність визначення ЦД за рахунок використання високочутливого вузькосмугового приймача.

Література: ***1.*** *Нестеренко М. П., Шорошев В. В. Соціальний та правовий аспекти масового застосування стільникових телефонів // Науковий вісник НАВСУ. Науково-теоретичний журнал. – Випуск № 2 . Частина 1. – К.: НАВС України, 2005 р. – С. 173 – 180.* ***2.*** *Шорошев В. В., Нестеренко М. П. Суспільно небезпечні дії з використанням стільникових терміналів // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. – Випуск 10. – К.: ПП "ЕКМО", 2005. – С. 181 – 185 .****3.*** *Нестеренко М. П., Бєгов Д. Д. Цифровий диктофон – сучасний засіб фіксації звуку // Сучасні технології у судовій акустиці: Матер. міжнар. наук.-практ. семін. – К.: НАВС України, 2003. – С. 117 – 120.* ***4.*** *Защита информации. Поисковая техника. Звукозапись. // Каталог DAS. – К.: ООО "D.A.S", 1999. – С. 211.* ***5.*** *В. В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС" , 2001. – С. 201.* ***6.*** *Защита информации. Звукозапись. Видеонаблюдение. Сигнализация // Каталог DAS. – К.: ООО "D.A.S", 2002. – С. 16.* ***7.*** *Патент України на винахід № 74218 С2, G 01 R 23/00 Детектор цифрових диктофонів / Жаріков Ю. Ф., Кондратьєв Я. Ю., Нестеренко М. П., Орлов Ю. Ю., Сущенко В. Д., Циганок О. Г. Національна академія внутрішніх справ України. - №2003054667; Заявл. 22. 05. 03. Опубл. 15. 11. 05. Бюл. № 11, 2005 р.*

УДК 681.3.06

ОРГАНИЗАЦИОННЫЕ И МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ЭКСПЕРТНОЙ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Сергей Гладыш

Харьковский национальный университет радиоэлектроники

Аннотация: **Рассмотрена суть метода и основные этапы процедуры экспертной оценки. Выявлены особенности экспертной оценки информационной безопасности телекоммуникационных систем. Разработаны организационно-методические рекомендации по проведению экспертизы при оценке информационной безопасности телекоммуникационных систем.**

Summary: **The essence of method and the basic stages of expert evaluation procedure is considered. The features of information security expert evaluation of telecommunication systems are exposed. Organizationally-methodical recommendations are developed on the procedure of information security expert evaluation of telecommunication systems.**

Ключевые слова: **Экспертная оценка, риск, управление, информационная безопасность, телекоммуникационные системы, комплексная система защиты информации.**

I Введение

Современные информационно-телекоммуникационные системы (ИТС) предъявляют новые, более высокие требования к информационной безопасности (ИБ) [1, 2]. Актуальным направлением повышения эффективности комплексных систем защиты информации (КСЗИ) является применение в процессе управления ИБ адекватных математических методов и моделей. Однако, полная математическая формализация задач ИБ часто неосуществима вследствие их качественной новизны и сложности [3 – 5]. В связи с этим все шире используются экспертные методы, под которыми понимают комплекс логических и математико-статистических методов и процедур, направленных на получение от специалистов

информации, необходимой для подготовки и выбора рациональных решений.

Проблема оптимизации КСЗИ в ИТС в наиболее общей ее постановке сводится к разработке методологии, которая позволяла бы формировать функцию выбора и выделения подмножества оптимальных стратегий по выбору варианта архитектуры КСЗИ. КСЗИ, с одной стороны, являются составной частью ИТС, с другой стороны сами по себе представляют сложную техническую систему. Как показывают результаты проведенных исследований [3 – 5], решение проблемы оптимизации КСЗИ ИТС усложняется рядом особенностей, основными из которых являются: сложная опосредствованная взаимосвязь показателей качества КСЗИ с показателями качества ИТС; необходимость учета большого числа показателей (требований) КСЗИ при оценке и выборе их рационального варианта; преимущественно качественный характер показателей (требований), учитываемых при анализе и синтезе КСЗИ; существенная взаимосвязь и взаимозависимость этих показателей (требований), имеющих противоречивый характер; трудность получения исходных данных, необходимых для решения задач анализа и синтеза КСЗИ, в особенности на ранних этапах их проектирования. Указанные особенности делают невозможным применение традиционных математических методов, в том числе методов математической статистики и теории вероятностей, а также классических методов оптимизации для решения прикладных задач анализа и синтеза КСЗИ.

Сложность процесса принятия решений, отсутствие математического аппарата приводят к тому, что при оценке и выборе альтернатив необходимо использовать и обрабатывать качественную экспертную информацию. Принятие решений в таком случае базируется на экспертных оценках. В условиях неопределенности исходных данных и некорректности постановки задач ИБ эти оценки могут внести дополнительную некорректность в принимаемое решение, увеличив тем самым исходную неопределенность.

Экспертные методы непрерывно развиваются и совершенствуются. Об этом свидетельствуют многочисленные работы, в частности [6 – 8]. Основные направления этого развития определяются рядом факторов, в числе которых можно указать на стремление расширить области применения, повысить степень использования математических методов и электронно-вычислительной техники. Исследованию проблем, связанных с использованием экспертных методов в сфере ИБ ИТС, посвящены работы [9 – 11].

Однако, несмотря на наличие определенных результатов, достигнутых в последние годы в разработке и практическом использовании метода экспертных оценок в сфере ИБ ИТС, имеется ряд проблем и задач организационного и методологического характера, требующих дальнейших методологических исследований и практической проверки. Необходимо совершенствовать систему отбора экспертов, находить пути повышения надежности характеристик группового мнения, разрабатывать методы проверки обоснованности оценок, исследовать скрытые причины, которые снижают достоверность экспертных оценок.

Организационные и методологические аспекты проведения экспертной оценки – одна из наиболее актуальных проблем, связанных с использованием метода экспертных оценок в сфере ИБ ИТС. Недооценка актуальности этой проблемы ставит под сомнение ценность результатов экспертизы и может выражаться в поспешном, непродуманном опросе экспертов. Низкое качество собранных таким образом мнений не может быть скомпенсировано применением для обработки современных математических методов.

В отечественной нормативно-правовой базе отсутствует такой документ, который бы носил рекомендательный характер, и в котором достаточно подробно были бы прописаны все этапы организации и методологии проведения экспертной оценки ИБ ИТС. Это свидетельствует о новизне поставленной задачи проведения исследований, которые будут предшествовать созданию такого рекомендательного документа.

Целью данной статьи является разработка организационно-методологических рекомендаций путем анализа, синтеза и проработки соответствующих аспектов проведения экспертной оценки ИБ ИТС.

Постановка задачи: методом анализа и сравнения международных рекомендаций [12 – 25] с действующей в Украине нормативно-правовой базой оценки защищенности информации [26 – 28] разработать организационно-методологические рекомендации по проведению экспертной оценки ИБ ИТС.

II Метод экспертных оценок как научный инструмент

Метод экспертных оценок – это метод организации работы со специалистами-экспертами и обработки мнений экспертов, выраженных в количественной и/или качественной форме с целью подготовки информации для принятия решений лицами, принимающими решения (ЛПР). Согласно [6] сущность метода экспертных оценок заключается в проведении экспертами интуитивно-логического анализа проблемы с количественной оценкой суждений и формальной обработкой результатов. Характерными

особенностями метода экспертных оценок как научного инструмента решения сложных неформализуемых проблем являются, во-первых, научно-обоснованная организация проведения всех этапов экспертизы, обеспечивающая наибольшую эффективность работы на каждом из этапов, и, во-вторых, применение количественных методов как при организации экспертизы, так и при оценке суждений экспертов и формальной групповой обработке результатов.

Можно выделить два основных типа процедур экспертного опроса: 1) процедура с личными контактами между экспертами, 2) многотуровые (итеративные) процедуры без личных контактов с контролируемой обратной связью. В работах [6 – 8] рассмотрены различные разновидности метода экспертных оценок, которые применяются в настоящее время. К основным видам относятся: анкетирование и интервьюирование; мозговой штурм; дискуссия; совещание; оперативная игра; сценарий, методы суда, мозговой атаки, отнесенной оценки, процедуры номинальной группы. Каждый из этих видов экспертного оценивания обладает своими преимуществами и недостатками, определяющими рациональную область применения. Во многих случаях наибольший эффект дает комплексное применение нескольких видов экспертизы.

При выполнении своей роли в процессе управления эксперты производят две основные функции: формируют объекты (альтернативные ситуации, цели, решения и т. п.) и производят измерение их характеристик (вероятности свершения событий, коэффициенты значимости целей, предпочтения решений и т. п.). Формирование объектов осуществляется экспертами на основе логического мышления и интуиции. Измерение характеристик объектов требует от экспертов знания теории измерений.

Обобщая результаты работ [3 – 8], все множество плохо формализуемых проблем условно можно разделить на два класса. К первому классу относятся проблемы, в отношении которых имеется достаточный информационный потенциал, позволяющий успешно решать эти проблемы. При этом методы опроса и обработки основываются на использовании принципа «хорошего» измерителя. Данный принцип означает, что выполняются следующие гипотезы: 1) эксперт является хранилищем большого объема рационально обработанной информации, и поэтому он может рассматриваться как качественный источник информации; 2) групповое мнение экспертов близко к истинному решению проблемы.

Ко второму классу относятся проблемы, в отношении которых информационный потенциал знаний недостаточен для уверенности в справедливости указанных гипотез. В работах [3 – 5, 11] показано, что таковыми являются проблемы ИБ. При решении таких проблем экспертов уже нельзя рассматривать как «хороших измерителей». Поэтому необходимо осторожно проводить обработку результатов экспертизы. Применение методов осреднения, справедливых для «хороших измерителей», в данном случае может привести к большим ошибкам. Например, мнение одного эксперта, сильно отличающееся от мнений остальных экспертов, может оказаться правильным. В связи с этим для проблем ИБ должна применяться качественная обработка [11].

III Особенности применения метода экспертных оценок при решении задач ИБ

В современной практике существует несколько подходов к оценке ИБ: аудит безопасности [12], расчет метрик безопасности [13], оценка на основе использования модели зрелости [14, 15], подход на основе сравнения показателей защищенности исследуемой системы с соответствующими эталонными показателями, прописанными в нормативных документах, например [16], подход на основе оценки рисков [11].

Обоснованию критериев и созданию методологии оценки ИБ уделено значительное внимание. Можно выделить следующие нормативные документы [17 – 22], которые внесли серьезный теоретический и практический вклад в формирование единой международной научно-методологической базы решения проблемы оценки ИБ в различных ИТС. Анализ этих документов подтверждает, что для решения задач обеспечения ИБ, наряду с формальными методами моделирования процессов функционирования КСЗИ необходимо использовать методы декомпозиции и структуризации компонентов систем и процессов, неформальные методы оценки эффективности функционирования и принятия решений. Это означает, что метод экспертных оценок необходимо использовать на всех этапах жизненного цикла КСЗИ. В Украине нормативными документами, посвященными методике оценки ИБ являются [23 – 25]. Проблемы нормативно-правового обеспечения оценки ИБ в Украине рассмотрены в [26].

В самых общих чертах порядок проведения государственной экспертизы КСЗИ в АС определен в [25].

Комплект документов, который предоставляется в ДСТСЗИ СБУ вместе с заявкой на проведение экспертизы, включает: техническое задание на КСЗИ; формуляр на автоматизированную систему; акт категорирования комплекса технических средств АС; акт принятия строительных работ; акт по результатам обследования АС; акт аттестации комплекса ТЗИ; комплект организационно-технических документов по вопросам ТЗИ и обеспечения режима секретности (Положение о службе защиты

информации в АС, План защиты информации в АС, инструкции администратору безопасности и пользователям АС и другие документы, определяющие порядок выполнения работ и ответственность персонала и пользователей АС); программа и методики предварительных испытаний АС и КСЗИ, протоколы проведенных испытаний; акт завершения опытной эксплуатации АС. Ведомственный порядок создания КСЗИ в АС класса 1 и проведения государственной экспертизы распространяется на государственные органы, которые имеют разрешение на право проведения работ по ТЗИ для собственных нужд и включены в Реестр организаторов экспертизы. Кроме того ДСТСЗИ СБУ установлен упрощенный порядок проведения государственной экспертизы КСЗИ в АС класса 1, созданных с использованием средств ТЗИ, которые отвечают следующим требованиям: имеют соответствующие сертификаты и экспертные заключения; включены в Перечень средств общего назначения, разрешенных для обеспечения ТЗИ, необходимость охраны которой определено законодательством Украины.

Первым этапом организации работ по проведению экспертной оценки ИБ ИТС является подготовка и издание руководящего документа, в котором должны формулироваться основные положения по выполнению экспертизы (постановка задачи; цели экспертизы; обоснование необходимости экспертизы; сроки выполнения работ; задачи и состав группы управления; обязанности и права группы; финансовое и материальное обеспечение работ).

Далее группа управления должна осуществлять работу примерно в такой последовательности: уяснение решаемой проблемы; определение круга областей деятельности, связанных с проблемой; определение долевого состава экспертов по каждой области деятельности; определение количества экспертов в группе; составление предварительного списка экспертов с учетом их местонахождения; анализ качеств экспертов и уточнение списка экспертов в группе; получение согласия экспертов на участие в работе; составление окончательного списка экспертной группы. Параллельно с процессом формирования группы экспертов группа управления должна проводить организацию и разработку методики проведения опроса экспертов. При этом должны решаться следующие вопросы: место и время проведения опроса; количество и задачи туров опроса; форма проведения опроса; порядок фиксации и сбора результатов опроса; состав необходимых документов. Следующим этапом работы группы управления должно являться определение организации и методики обработки данных опроса. На данном этапе необходимо определить задачи и сроки обработки, процедуры и алгоритмы обработки, силы и средства для проведения обработки. В процессе непосредственного проведения опроса экспертов и обработки его результатов группа управления должна осуществлять выполнение комплекса работ в соответствии с разработанным планом, корректируя его по мере необходимости по содержанию, срокам и обеспечению ресурсами. Последним этапом работ для группы управления должно являться оформление результатов работы. На этом этапе необходимо производить анализ результатов экспертного оценивания; составление отчета; обсуждение и одобрение результатов; представление итогов работы на утверждение; ознакомление с результатами экспертизы организаций и лиц.

IV Подбор экспертов

Общим требованием при формировании группы экспертов является эффективное решение проблемы экспертизы. Эффективность решения определяется характеристиками достоверности экспертизы и затрат. Достоверность экспертной оценки ИБ может быть определена только на основе практического решения проблемы управления рисками, построения КСЗИ и анализа ее эффективности. Если экспертиза проводится систематически с примерно одним и тем же составам экспертов, то появляется возможность накопления статистических данных по достоверности работы группы экспертов и получения устойчивой числовой оценки достоверности. Эту оценку можно использовать в качестве априорных данных о достоверности группы экспертов для последующих экспертиз. Достоверность группового экспертного оценивания зависит от общего числа экспертов в группе, долевого состава различных специалистов в группе, от характеристик экспертов. Определение характера зависимости достоверности от перечисленных факторов является еще одной проблемой процедуры подбора экспертов.

Сложной проблемой процедуры подбора является формирование системы характеристик эксперта, существенно влияющих на ход и результаты экспертизы. Эти характеристики должны описывать специфические свойства специалиста и возможные отношения между людьми, влияющие на экспертизу. Важным требованием к характеристикам эксперта является измеримость этих характеристик.

Еще одной проблемой является организация процедуры подбора экспертов, т. е. определение четкой последовательности работ, выполняемых в процессе подбора экспертов и необходимых ресурсов. Определить необходимый численный состав экспертной группы очень важно. При недостаточном числе экспертов результаты экспертизы не будут надежными. Многочисленную группу квалифицированных экспертов трудно сформировать и трудно организовать ее работу.

Согласно [3, 6], численный состав экспертной группы, вычисляется по формуле:

$$k=[\beta\, t_{p,k-1} / \alpha\,]^2 \qquad (1)$$

где k – число экспертов; β – вариация (мера надежности проведенной экспертизы); $t_{p,k-1}$ – коэффициент Стьюдента; α – относительная ширина доверительного интервала.

Вариация определяется как:

$$\beta = \sigma / x_{cp} \qquad (2)$$

где σ – среднеквадратический разброс экспертных оценок; x_{cp} - среднее значение оценки.

Относительная ширина доверительного интервала вычисляется из соотношения:

$$\alpha = \Delta x / x_{cp} \qquad (3)$$

где Δx – доверительный интервал оценок.

Как видно из (2), величина вариации определяется по результатам экспертизы, но для этого в свою очередь необходимо знать требуемый состав экспертной группы. Для преодоления этой трудности предлагается следующий подход.

Пусть для статистической обработки допускается лишь такие экспертные оценки, относительное отличие которых от среднего значения по абсолютной величине не превышает $|\Delta x / x_{cp}|$. В пределах интервала $\pm |\Delta x$ около x_{cp} отдельные оценки могут располагаться различным образом, от чего будет зависеть величина вариации β. Однако при типичном характере рассеяния отдельных оценок и строгом соблюдении правила о привлечении к экспертизе только квалифицированных специалистов изменение вариации при изменении числа оценок будет не очень значительным. В работе [3] в качестве иллюстрации исследованы зависимости β в долях $\Delta x / x_{cp}$ от числа k. С увеличением *k* величина β изменяется не очень существенно; с возрастанием *k* величина β монотонно уменьшается. Если на основании предыдущих экспертиз зададимся некоторой величиной β, соответствующей небольшому *k,* а затем с помощью (1) вычислим *k,* то при найденном значении *k* доверительный интервал не превысит выбранной величины [6].

На основании опыта применения метода экспертных оценок для решения различных не формализуемых задач установлено, что результаты экспертизы можно считать удовлетворительными при $\beta \le 0{,}3$ и хорошими, если $\beta \le 0{,}2$ [3, 6]. Исходя из этого, при определении численного состава экспертной группы априорное значение вариации следует выбирать в пределах 0,2÷0,3.

Коэффициент Стьюдента $t_{p,k-1}$ определяется по таблицам. Выбрав доверительную вероятность p, для различных *k* находим соответствующие значения $t_{p,k-1}$. Затем для каждой пары *k* и $t_{p,k-1}$ из уравнения (1) находим β / α и для выбранной p будет получена зависимость f(k) = β / α, которую можно трактовать как k = F (β / α).

Таким образом, вычислив соотношение β / α и задав доверительную вероятность p находим численный состав экспертной группы *k.*

Распределение Стьюдента, использованное в формуле (1), при увеличении *k* сходится к нормальному распределению. Поэтому число экспертов приближенно можно определить с помощью выражения:

$$\beta / \alpha = k^{0,5} / z(k) \qquad (4)$$

где *z(k)* – значение интеграла вероятности, которое определяется по таблицам.

Численность группы экспертов проверяется на ограничение по финансовым ресурсам. Определив зависимость между достоверностью, количеством экспертов и расходами на оплату, группа управления должна представлять руководству эту информацию и формулировать возможные альтернативы решений: либо снижение достоверности результатов экспертного оценивания до уровня, обеспечивающего выполнение ограничения по расходам на оплату экспертов, либо сохранение исходного требования на достоверность экспертизы и увеличение расходов на оплату экспертов.

Обращения к экспертам сопряжены с определенными финансовыми издержками. Учитывая это обстоятельство, при формировании экспертной группы можно использовать следующую методику [3].

Для заданной доверительной вероятности *p* находится численный состав возможных кандидатов экспертной группы ($э_1$, $э_2$, ..., $э_n$) и вычисляются их весовые коэффициенты (μ_1, ..., μ_n). Пусть h_1 – условная стоимость обращения к *i*-му эксперту, а h_0 – граничная суммарная условная стоимость обращения ко всем экспертам.

Введем переменные:

$x_i = 1$, если *i*-й эксперт включен в состав экспертной группы;

$x_i = 0$, – в противном случае.

Тогда задачу формирования экспертной группы, обладающей максимальной компетентностью, можно записать как задачу линейного программирования следующим образом:

$$\sum_{i=1}^{n} \mu_i \cdot x_i \rightarrow \max \qquad (5)$$

при ограничениях

$$\sum_{i=1}^{n} h_i \cdot x_i \le h_0,\ x_i = \begin{cases} 1 \\ 0 \end{cases},\ i \in \{1, ..., n\}. \qquad (6)$$

Следующим этапом работы по подбору экспертов является составление предварительного списка экспертов. При составлении этого списка необходимо проводить анализ качеств экспертов. Кроме учета качеств экспертов, следует определять их местонахождение и возможность участия выбранных специалистов в экспертизе.

V Опрос экспертов, формализация информации и обработка экспертных оценок

Основным содержанием опроса является: постановка задачи и предъявление вопросов экспертам; информационное обеспечение работы экспертов; выработка экспертами суждений, оценок, предложений; сбор результатов работы. Главным в организации опроса является обеспечение максимума информации и максимума творческой активности, самостоятельности эксперта.

Выбор того или иного вида опроса определяется многими факторами, из которых основными являются: цель и задачи экспертизы; сложность анализируемой ИТС; полнота и достоверность исходной информации; требуемые объем и достоверность информации, получаемой в результате опроса; время, отведенное на опрос и экспертизу в целом; допустимая стоимость опроса, и экспертизы в целом; количество экспертов и группы управления, их характеристики.

Рациональное использование информации, полученной от экспертов, возможно при условии преобразования ее в форму, удобную для дальнейшего анализа, направленного на подготовку и принятие решений по ИБ. Возможности формализации информации зависят от специфических особенностей исследуемой ИТС, надежности и полноты имеющихся данных, уровня принятия решения. Форма представления экспертных данных зависит и от принятых критериев, на выбор которых, в свою очередь, существенное влияние оказывает специфика ИБ. Формализация информации, полученной от экспертов, должна быть направлена на подготовку решения задач ИБ, которые не могут быть в полной мере описаны математически, т. к. являются «слабоструктуризованными», т. е. содержат неопределенности, связанные не только с измерением, но и характером исследуемых целей, средств их достижения и внешних условий.

Задача построения обобщенной оценки объектов по индивидуальным оценкам возникает при групповом экспертном оценивании. Решение этой задачи зависит от использованного экспертами метода измерения.

Пусть *m* экспертов произвели оценку *n* объектов по *l* показателям. Результаты оценки представлены в виде величин x_{ij}^h, где *j* – номер эксперта, *i* – номер объекта, *h* – номер показателя (признака) сравнения. Если оценка объектов произведена методом ранжирования, то величины x_{ij}^h представляют собой ранги. Если оценка объектов выполнена методом непосредственной оценки или методом последовательного сравнения, то величины x_{ij}^h представляют собой числа из некоторого отрезка числовой оси, или баллы. Обработка результатов оценки существенно зависит от рассмотренных методов измерения.

Рассмотрим случай, когда величины $x_{ij}^h\ (i = 1, ..., n;\ j = 1, 2, ..., m;\ h = 1, 2, ..., l)$ получены методами непосредственной оценки или последовательного сравнения, т. е. x_{ij}^h являются числами, или баллами. Для получения групповой оценки объектов в этом случае можно воспользоваться средним значением оценки для каждого объекта:

$$x_i = \sum_{h=1}^{l} \sum_{j=1}^{m} q_h x_{ij}^h k_j\ (i = 1, 2, ..., n), \qquad (7)$$

где q_h – коэффициенты весов показателей сравнения объектов, k_j – коэффициенты компетентности экспертов. Коэффициенты весов показателей и компетентности объектов являются нормированными величинами:

$$\sum_{h=1}^{l} q_h = 1; \quad \sum_{j=1}^{m} k_j = 1. \qquad (8)$$

Коэффициенты весов показателей могут быть определены экспертным путем. Если q_{hj} – коэффициент веса *h*-го показателя, даваемый *j*-м экспертом, то средний коэффициент веса *h*-го показателя по всем

экспертам равен:

$$q_h = \sum_{j=1}^{m} q_{hj} k_j (h = 1, 2, ..., l). \tag{9}$$

Коэффициенты компетентности экспертов можно вычислить по апостериорным данным, т. е. по результатам оценки объектов. Идеей этого вычисления является предположение о том, что компетентность экспертов должна оцениваться по степени согласованности их оценок с групповой оценкой объектов.

Алгоритм вычисления коэффициентов компетентности экспертов имеет вид рекуррентной процедуры :

$$x_i^t = \sum_{j=1}^{m} x_{ij} k_j^{t-1} (i = 1, 2, ..., n); \tag{10}$$

$$\lambda^t = \sum_{i=1}^{n} \sum_{j=1}^{m} x_{ij} x_i^t (t = 1, 2, ...); \tag{11}$$

$$k_j^t = \frac{1}{\lambda^t} \sum_{i=1}^{n} x_{ij} x_i^t ; \sum_{j=1}^{m} k_j^t = 1 (j = 1, 2, ..., m). \tag{12}$$

Рассмотрим теперь случай, когда эксперты производят оценку множества объектов методом ранжирования так, что величины x_{ij} есть ранги. Обработка результатов ранжирования заключается в построении обобщенной ранжировки. Для построения такой ранжировки введем конечномерное дискретное пространство ранжировок и метрику в этом пространстве. Каждая ранжировка множества объектов *j*-м экспертом есть точка R_j в пространстве ранжировок.

Ранжировку R_j можно представить в виде матрицы парных сравнений, элементы которой определим следующим образом:

$$a_{kl} = \begin{cases} 1, \text{ если } O_k \ \phi \ O_t , \\ -1, \text{ если } O_l \ \pi \ O_k , \\ 0, \text{ если } O_k \propto O_t . \end{cases} \tag{13}$$

Очевидно, что $a_{kk} = 0$, поскольку каждый объект эквивалентен самому себе. Элементы матрицы $\|a_{kl}\|$ антисимметричны $a_{kl} = -a_{lk}$.

Если все ранжируемые объекты эквивалентны, то все элементы матрицы парных сравнений равны нулю. Такую матрицу будем обозначать R_0 и считать, что точка в пространстве ранжировок, соответствующая матрице R_0, является началом отсчета.

Обращение порядка ранжируемых объектов приводит к транспонированию матрицы парных сравнений.

Метрика $d(R_i, R_j)$ как расстояние между *i*-й и *j*-й ранжировками определяется формулой

$$d(R_i, R_j) = \frac{1}{2} \sum_{k,l=1}^{n} \left| a_{kl}^i - a_{kl}^j \right|, \tag{14}$$

если выполнены следующие 6 аксиом.

1. $d(R_i, R_j) \geq 0,$ причем равенство достигается, если ранжировки R_i и R_j тождественны;

2. $d(R_i, R_j) = d(R_j, R_i);$

3. $d(R_i, R_h) + d(R_h, R_j) \geq d(R_i, R_j),$ причем равенство достигается, если ранжировка «лежит между» ранжировками R_i и R_j. Понятие «лежит между» означает, что суждение о некоторой паре $O_k O_l$ объектов в ранжировке совпадает с суждением об этой паре либо в R_i, либо в R_j или же в R_i $O_k \ \phi \ O_l$, в R_j $O_l \ \phi \ O_k$, а в R_h $O_k \propto O_l$;

4. $d(R_i^{'}, R_j^{'}) = d(R_i, R_j),$ где $R_i^{'}$ получается из R_i некоторой перестановкой объектов, а $R_j^{'}$ из R_j той же самой перестановкой. Эта аксиома утверждает независимость расстояния от перенумерации объектов.

5. Если две ранжировки R_i, R_j одинаковы всюду, за исключением *n*-элементного множества элементов, являющегося одновременно сегментом обеих ранжировок, то $d(R_i, R_j)$ можно вычислить, как если бы рассматривалась ранжировка только этих *n*-объектов. Сегментом ранжировки называется множество, дополнение которого непусто и все элементы этого дополнения находятся либо впереди, либо позади каждою элемента сегмента. Смысл этой аксиомы состоит в том, что если две ранжировки полностью согласуются в начале и конце сегмента, а отличие состоит в упорядочении средних *n*-объектов, то естественно принять, что расстояние между ранжировками должно равняться расстоянию, соответствующему ранжировкам средних *n*-объектов.

6. Минимальное расстояние равно единице.

Пространство ранжировок при двух объектах можно изобразить в виде трех точек, лежащих на одной прямой. Расстояния между точками равны $d(R_1, O) = d(R_2, O) = 1,\ d(R_1, R_2) = 2.$ *При трех объектах пространство всех возможных ранжировок состоит из 13 точек.*

Используя введенную метрику, определим обобщенную ранжировку как такую точку, которая наилучшим образом согласуется с точками, представляющими собой ранжировки экспертов. Понятие наилучшего согласования на практике чаще всего определяют как медиану и среднюю ранжировку.

Медиана есть такая точка в пространстве ранжировок, сумма расстояний от которой до всех точек – ранжировок экспертов является минимальной. В соответствии с определением медиана вычисляется из условия

$$R_M \Leftarrow \min_R \sum_{j=1}^{m} d(R_j, R). \tag{15}$$

Средняя ранжировка есть такая точка, сумма квадратов расстояний от которой до всех точек – ранжировок экспертов является минимальной. Средняя ранжировка определяется из условия

$$R_C \Leftarrow \min_R \sum_{j=1}^{m} d^2(R_j, R). \tag{16}$$

Пространство ранжировок конечно и дискретно, поэтому медиана и средняя ранжировка могут быть только какими-либо точками этого пространства. В общем случае медиана и средняя ранжировка могут не совпадать ни с одной из ранжировок экспертов.

Если учитывается компетентность экспертов, то медиана и средняя ранжировка определяются из условий:

$$R_M \Leftarrow \min_R \sum_{j=1}^{m} k_j d(R_j, R);\quad R_C \Leftarrow \min_R \sum_{j=1}^{m} k_j d^2(R_j, R), \tag{17}$$

где k_j – коэффициенты компетентности экспертов.

Если ранжировка объектов производится по нескольким показателям, то определение медианы вначале производится для каждого эксперта по всем показателям, а затем вычисляется медиана по множеству экспертов:

$$R_{M_j} \Leftarrow \min_R \sum_{h=1}^{l} q_h d(R_j^h, R) \quad (j=1, 2, \ldots, m), \tag{18}$$

$$R_M \Leftarrow \min_R \sum_{j=1}^{m} k_j d(R_{M_j}, R), \tag{19}$$

где q_h – коэффициенты весов показателей.

Недостатком определения обобщенной ранжировки в виде медианы или средней ранжировки является трудоемкость расчетов. Сложность вычисления медианы или средней ранжировки привела к необходимости применения более простых способов построения обобщенной ранжировки. К числу таких способов относится способ сумм рангов, который заключается в ранжировании объектов по величинам сумм рангов, полученных каждым объектом от всех экспертов. Для матрицы ранжировок $\|r_{ij}\|$ составляются суммы

$$r_i = \sum_{j=1}^{m} r_{ij} \quad (i=1, 2, \ldots, n). \tag{20}$$

Далее объекты упорядочиваются по цепочке неравенств $r_1 < r_2 < \ldots < r_n$.

Для учета компетентности экспертов достаточно умножить каждую *i*-ю ранжировку на коэффициент компетентности *j*-го эксперта $0 \le k_j \le 1$. В этом случае вычисление суммы рангов для *i*-го объекта производится по следующей формуле:

$$r_i = \sum_{j=1}^{m} r_{ij} k_j \quad (i=1, 2,\ldots, n.). \tag{21}$$

Обобщенная ранжировка с учетом компетентности экспертов строится на основе упорядочения сумм рангов для всех объектов.

Следует отметить, что построение обобщенной ранжировки по суммам рангов является корректной процедурой, если ранги назначаются как места объектов в виде натуральных чисел 1, 2, ..., *n*.

Еще одним более обоснованным в теоретическом отношении подходом к построению обобщенной ранжировки является переход от матрицы ранжировок к матрице парных сравнений и вычисление собственного вектора, соответствующего максимальному собственному числу этой матрицы. Упорядочение объектов производится по величине компонент собственного вектора.

Определение согласованности мнений экспертов производится путем вычисления числовой меры (энтропийного коэффициента конкордации), характеризующей степень близости индивидуальных мнений.

Энтропийный коэффициент конкордации определяется формулой (коэффициент согласия):

$$W = 1 - \frac{H}{H_{\max}}, \tag{22}$$

где *H* – энтропия, вычисляемая по формуле

$$H = -\sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij} \log p_{ij}, \tag{23}$$

а $H_{\max}$ – максимальное значение энтропии. В формуле для энтропии p_{ij} – оценки вероятностей *j*-го ранга, присваиваемого *i*-му объекту. Эти оценки вероятностей вычисляются в виде отношения количества экспертов m_{ij}, приписавших объекту O_i ранг *j* к общему числу экспертов:

$$p_{ij} = \frac{m_{ij}}{m}. \tag{24}$$

Максимальное значение энтропии достигается при равновероятном распределении рангов, т. е. когда $m_{ij} = m / n$. Тогда

$$p_{ij} = \frac{m}{mn} = \frac{1}{n}. \tag{25}$$

Подставляя это соотношение в формулу (23), получаем

$$H_{\max} = -\frac{1}{n} \log \frac{1}{n} \sum_{i,j=1}^{n} = n \log n. \tag{26}$$

Анализ значения меры согласованности способствует выработке правильного суждения об общем уровне знаний по информационной безопасности и выявлению группировок мнений экспертов. Качественный анализ причин группировки мнений позволяет установить существование различных взглядов, концепций, выявить научные школы, определить характер профессиональной деятельности и т. п. Все эти факторы дают возможность более глубоко осмыслить результаты опроса экспертов.

Обработкой результатов экспертного оценивания можно определять зависимости между ранжировками различных экспертов и тем самым устанавливать единство и различие в мнениях экспертов. Важную роль играет также установление зависимости между ранжировками, построенными по различным показателям сравнения объектов. Выявление таких зависимостей позволяет вскрыть связанные показатели сравнения и, может быть, осуществить их группировку по степени связи. Важность задачи определения зависимостей для практики очевидна. Например, если показателями сравнения являются различные цели (показатели

защищенности информации), а объектами – средства достижения целей (механизмы безопасности), то установление взаимосвязи между ранжировками, упорядочивающими средства с точки зрения достижения целей, позволяет обоснованно ответить на вопрос, в какой степени достижение одной цели при данных средствах способствует достижению других целей.

Оценки, получаемые на основе обработки, представляют собой случайные объекты, поэтому одной из важных задач процедуры обработки является определение их надежности.

Повышение качества и скорости проведения экспертной оценки, повышение качества информационного обеспечения, создание благоприятных условий для работы эксперта могут быть достигнуты путем автоматизации на основе использования компьютерной техники, современного алгоритмического и программного обеспечения. Автоматизированная система должна удовлетворять определенному перечню требований, которые предъявляются к подобным системам.

Априорная невозможность охвата всех нюансов ИБ, быстротечность процессов защиты информации вызывают определенную степень неопределенности или неуверенности в оценках эксперта. Поэтому математический аппарат, который будет использоваться в качестве основы оценки должен обеспечивать возможность получения оценок, которые учитывают эту неопределенность, и корректность их обработки. В качестве такого аппарата можно рассматривать методы нечетких множеств и нечеткой логики [11] и аппарат субъективной логики [10].

Выводы

При использовании метода экспертных оценок для оценки ИБ возникают организационно-методологические проблемы. Основными из них являются: подготовка и подбор экспертов, проведение опроса экспертов, обработка результатов опроса, организация процедур экспертизы, повышение надежности характеристик группового мнения, разработка методов проверки обоснованности оценок, исследование скрытых причин, снижающих достоверность экспертных оценок.

Для повышения обоснованности решений по созданию КСЗИ с учетом многочисленных факторов, оказывающих влияние на ИБ ИТС, необходим разносторонний анализ, основанный как на расчетах, так и на аргументированных суждениях специалистов, знакомых с состоянием дел и перспективами развития ИБ.

Следует заметить, что метод экспертных оценок лишь позволяет пополнить информацию, необходимую для подготовки и принятия таких решений. Широкое использование экспертных оценок правомерно только там, где для оценки информационной безопасности невозможно применить более точные методы. В ряде случаев повышение объективности исходных данных можно предложить как рациональную альтернативу методу нечеткой логики при оценке ИБ ИТС [27].

Обработка результатов экспертизы представляет собой трудоемкий процесс. Выполнение операций вычисления оценок и показателей их надежности вручную связано с большими трудовыми затратами даже в случае решения простых задач упорядочения. В связи с этим целесообразно использовать вычислительную технику. Применение компьютера выдвигает проблему разработки программного обеспечения, реализующего алгоритмы обработки результатов экспертного оценивания.

Перспективными направлениями для дальнейших исследований являются методологические разработки по совершенствованию систем подготовки и отбора экспертов, повышение надежности характеристик группового мнения, разработка методов проверки обоснованности оценок, исследование скрытых причин, снижающих достоверность экспертных оценок, разработка усовершенствованного программного обеспечения, реализующего опрос и обработку результатов экспертного оценивания.

*Литература: **1.** Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". **2.** Степанов В. Д. Система технічного захисту інформації України: стан та напрямки розвитку// Матеріали доповідей на семінарі "Захист інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності", К., 2005. **3.** Домарев В. В. Математические модели систем и процессов защиты информации. http://www.domarev.kiev.ua/nauka/ 4. Хамула С., Ковбаса С., Кулинич Ю. Формализация процессов защиты информации в информационно-вычислительных системах //«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 7, К., 2003. С. 113-118. 5. Ухлинов Л. М., Мирошниченко Г. К. О формализации процессов защиты информации в вычислительных сетях // Автоматика и вычислительная техника. – 1992. - №1. – с. 6 – 12. **6.** Панкова Л. А., Петровский А. М., Шнейдерман Н. В. Организация экспертизы и анализ экспертной информации – М; Наука, 1984 – 214 с. **7.** Обработка нечеткой информации в системах принятия решений/ А. Н. Борисов, А. В. Алексеев, Г. В. Меркурьева и др. – М.: Радио и связь, 1989. – 304 с. 8. Маренко В. А. Модели и алгоритмы экспертных систем поддержки принятия решений по электромагнитной совместимости. Автореферат диссертации.*

Тюмень, 2004. ***9.*** *Потий А., Леншин А. Методика формирования вербальных оценок защищенности ИТС на основе требований нормативных документов //«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 10, К., 2005. С. 8 – 18.* ***10.*** *Потий А., Леншин А. Методика определения мыслей экспертов относительно зрелости безопасности информации с применением математического аппарата субъективной логики //«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 9, К., 2004. С. 38 – 47.* ***11.*** *Гладыш С. В. Использование теории нечетких множеств при экспертной оценке и многокритериальной оптимизации систем защиты информации// Материалы IX Международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», Харьков, 2005 г.* ***12.*** *GAO/AIMD-12.19.6. Federal Information Systems Control Audit Mnual. 1999.* ***13.*** *NIST SP 800-53. Marianne Swanson. Security Metrics Guide for Information Technology Systems. 2003.* ***14.*** *NIST SP 800-26. Marianne Swanson. Security Self-Assessment Guide for Information Technology Systems.* ***15.*** *ISO/IEC 21827:2002 – Systems Security Engineering – Capability Maturity Model.* ***16.*** *ISO/IEC 17799:2000E – Information Technology – Practice for Information Security Management.* ***17.*** *Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985.* ***18.*** *Information Tecnhology Security Evaluation Criteria, v. 1. 2. - Office for Official publications of the European Communities, 1991.* ***19.*** *Canadian Tusted Computer Product Evaluation Criteria, v. 3. 0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.* ***20.*** *Federal Criteria for Information Technology security. - NIST, NSA, US Government, 1993.* ***21.*** *ISO/IEC 15408-1:2000 - Information technology - Security techniques - Evaluation criteria for IT security.* ***22.*** *CEM-97/017. Common Evaluation Methodology for Information Technology Security - Part 1.* ***23.*** *НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в КС від НСД.* ***24.*** *НД ТЗІ 3.7-002-99. ТЗІ на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).* ***25.*** *Положення про державну експертизу в галузі ТЗІ (приказ ДСТСЗІ СБ України від 29. 12. 99 № 62).* ***26.*** *Воробиенко П., Нечипорук О., Щербина Ю. Проблемы нормативно-правового обеспечения оценки защищенности автоматизированных систем//«Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні», вип. 9, К., 2004. – с. 17 – 20.* ***27.*** *С. М. Доценко, А. А. Зайчиков, В. Н. Малыш. Повышение объективности исходных данных как альтернатива методу нечеткой логики при оценке риска информационной безопасности//«Защита информации. Конфидент» № 5 '2004 г., С-Пб., 2004.*

УДК 004.049.2

ПРАКТИКА ПРИМЕНЕНИЯ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Михаил Дивизинюк, Владимир Шахайда

Севастопольский национальный университет ядерной энергетики и промышленности

Анотація: **Дана оцінка сучасних вимог стосовно ТЗІ, доведени недолікі та шляхи їх усунення.**

Summary: **The estimation of modern requirements concerning a technical privacy is given, existing problems and ways of their decision are resulted.**

Ключевые слова: **Техническая защита информации, поисковые средства, ТЗИ, закладные устройства.**

Введение

Говоря об информационной безопасности, в настоящее время чаще всего имеют в виду компьютерную безопасность. Действительно, информация, находящаяся на электронных носителях, играет все большую роль в жизни современного общества. Уязвимость такой информации обусловлена целым рядом факторов: огромные объемы, большое количество пользователей, возможность анонимного доступа к информации, простота переноса информации. Все это создает возможность проведения "информационных диверсий", делает задачу обеспечения защиты информации, размещенной в компьютерной среде, гораздо более сложной проблемой, чем, скажем, сохранение тайны традиционной почтовой переписки. Тем не менее, понятие ТЗИ подразумевает защиту всех видов информации.

I Применяемые в настоящее время средства ТЗИ

В настоящее время при лицензировании помещений для получения разрешения на обработку документов с ограниченной формой доступа, оговорен ряд мероприятий организационно-технического характера, направленных на ограничение доступа посторонних лиц в помещения. Также оговорен