Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования

Владимирский государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

КНИГА 16

Д.А. ПОЛЯНСКИЙ, О.И. ФАЙМАН

ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Владимир 2009

УДК 519.6 (075)
ББК 22.186
П54

Редактор серии – доктор технических наук, профессор
М.Ю. Монахов

Рецензенты:
Кандидат технических наук, доцент
зав. кафедрой оперативно-технической деятельности
Владимирского юридического института
Федеральной службы исполнения наказаний
К.Н. Курысев

Кандидат физико-математических наук, доцент
кафедры информатики и защиты информации
Владимирского государственного университета
А.В. Александров

Печатается по решению редакционного совета
Владимирского государственного университета

Полянский, Д. А.

П54 Экономика защиты информации : учеб. пособие / Д. А. Полянский, О. И. Файман ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2009. – 96 с. (Комплексная защита объектов информатизации. Кн. 16 / под ред. М. Ю. Монахова).

ISBN 978-5-89368-975-4

Это шестнадцатая книга из серии «Комплексная защита объектов информатизации». В ней представлена методика оценки экономических показателей системы защиты информации коммерческого предприятия.

Учебное пособие предназначено для студентов 5-го курса специальности 090104 – комплексная защита объектов информатизации очной формы обучения. Может быть полезно широкому кругу читателей, самостоятельно осваивающих вопросы защиты информации.

Табл. 8. Ил. 7. Библиогр.: 21 назв.

УДК 519.6 (075)
ББК 22.186

ISBN 978-5-89368-975-4

ОГЛАВЛЕНИЕ

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место
АС – автоматизированная система
БД – базы данных
ВС – вычислительная система
ЗИ – защита информации
ИБ – информационная безопасность
ИС – информационная система
ИТ – информационные технологии
КИБ – концепция информационной безопасности
КС – компьютерная система
КСИБ – комплексная система информационной безопасности
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПИБ – политика информационной безопасности
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
РД – руководящий документ
СВТ – средства вычислительной техники
СЗИ – система защиты информации
СКУД – система контроля и управления доступом
СИБ – система информационной безопасности
ССВ – совокупная стоимость владения
СУБД – система управления базами данных
ТКУИ – технический канал утечки информации
ТО – техническое обслуживание
ТСО – технические средства охраны
ТСР – техническое средство разведки
ЧС – чрезвычайная ситуация

ВВЕДЕНИЕ

Настоящее учебное пособие – шестнадцатая книга из серии «Комплексная защита объектов информатизации», подготовленная кафедрой «Информатика и защита информации» Владимирского государственного университета.

Учебное пособие предназначено в первую очередь для студентов специальности «Комплексная защита объектов информатизации» в качестве основного источника информации при изучении дисциплины «Экономика защиты информации», в том числе для выполнения курсовой работы.

Современные предприятия и организации сталкиваются с проблемой оценки качества СИБ. Постоянно растет доля расходов на обеспечение защиты конфиденциальной информации. Однако выделение средств на построение или совершенствование СИБ для коммерческого предприятия должно быть обоснованным с экономической точки зрения.

Оценка экономической эффективности СЗИ, качества механизмов и средств защиты, защищенности всей информационной системы в целом является неотъемлемой частью оценки качества работы предприятия. Это позволяет выбрать наиболее эффективную систему защиты для определенного предприятия как с функциональной, так и с экономической точки зрения.

В настоящем учебном пособии рассмотрена методика оценки экономической эффективности и коэффициента защищенности СЗИ, реализуемая с использованием как количественных, так и качественных показателей на основе экспертизы ИС и аудита СЗИ на соответствие требованиям российских и международных стандартов ИБ.

Данное учебное пособие состоит из четырех глав. В нем раскрываются следующие вопросы:

- параметры ИС предприятия и показатели качества СЗИ, методика организации и проведения экспертизы ИС предприятия и обработки первичной экспертной информации (гл. 1, Д.А. Полянский);

- основы теории нечетких множеств в части представления математического описания лингвистических экспертных оценок параметров ИС (гл. 2, Д.А. Полянский);
- методика проведения аудита ИБ предприятия и ее применение для оценки степени соответствия параметров СЗИ требованиям стандартов безопасности (гл. 3, О.И. Файман);
- экономическая модель СЗИ, методика оценки параметров ИС и экономических показателей СЗИ, получение интегральных оценок экспертной группы и расчет достоверности проведения экспертизы (гл. 4, Д.А. Полянский).

В учебном пособии также приведен пример расчета показателей качества СЗИ типового коммерческого предприятия (приложение).

В конце каждой главы даны краткие выводы и приведен список вопросов для самоконтроля, а также несколько заданий для самостоятельной работы.

Глава 1. ЭКСПЕРТИЗА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

1.1. Параметры ИС и показатели качества СЗИ предприятия

Защита информации представляет собой комплекс мероприятий по поддержанию конфиденциальности, целостности, доступности и других свойств информации. В определении этого термина не заложены никакие ограничения затрат ресурсов на проведение этих мероприятий.

Коммерческие предприятия существуют в системе товарно-денежных отношений, в основе которой лежит понятие экономической эффективности, и, как следствие, не могут себе позволить бесконтрольно и безосновательно тратить материальные ресурсы на проведение каких-либо мероприятий. Таким образом, экономическая эффективность функционирования СЗИ становится для предприятия ее важнейшей характеристикой.

Можно рассмотреть такую ситуацию. В локальной сети коммерческого предприятия обрабатывается некоторая информация. Существует множество методов и средств защиты данной информации: физическая защита и управление доступом в помещения, установка специального ПО на рабочих станциях, использование межсетевых экранов. И это только элементы защиты самой сети. Кроме того, могут использоваться различные системы охраны и сигнализации, защиты выделенных помещений, средства выявления и противодействия работе ТСР.

Расходы на средства и мероприятия по защите информации могут составлять очень значительные суммы в денежном выражении. При этом не известна ни стоимость защищаемой информации, ни какой конкретный ущерб принесет её разглашение. К тоже же нет уверенности, что сотрудники, работающие с информацией, не готовы поделиться секретными данными за сумму меньшую, чем все расходы, произведенные для защиты информации.

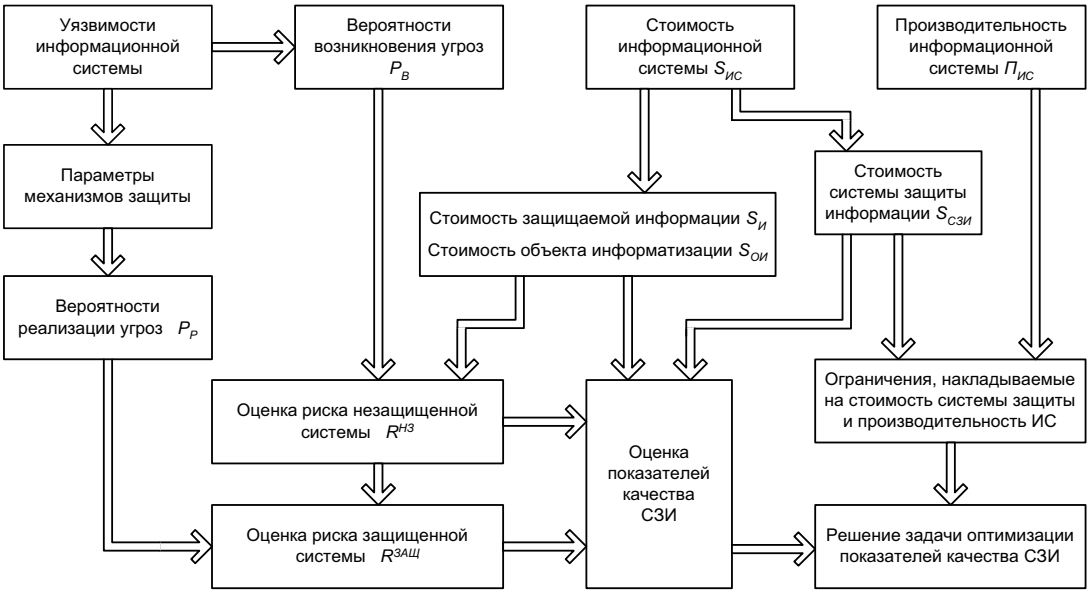
Следовательно, защита информационных ресурсов должна быть экономически эффективна, поскольку она предназначена, в том числе, и для сохранения финансовых ресурсов организации.

Методология оценки эффективности СЗИ предполагает использование следующих критериев:

- стоимость защищаемой информации $S_И$;
- стоимость защищаемого объекта информатизации $S_{ОИ}$;
- стоимость системы защиты информации $S_{СЗИ}$;
- суммарный риск информации $R_И$;
- суммарный риск объекта информатизации $R_{ОИ}$;
- суммарный риск системы защиты информации $R_{СЗИ}$;
- вероятности возникновения угроз безопасности $P_В$;
- вероятности реализации угроз безопасности $P_Р$.

Эти критерии можно назвать показателями качества ИС, или параметрами ИС. Зависящие от них показатели качества СЗИ являются оптимизируемыми. Основные показатели качества – коэффициент защищенности и экономическая эффективность.

Модель оценки показателей качества СЗИ представлена на рисунке.



Модель оценки показателей качества СЗИ

Параметры ИС взаимосвязаны и взаимозависимы. Можно отметить следующие взаимосвязи:

$S_И \leftrightarrow S_{СЗИ}$, $S_{ОИ} \leftrightarrow S_{СЗИ}$.

Существуют следующие зависимости:

$R_И = f(S_И, S_{СЗИ}, P_В, P_Р)$,

$R_{ОИ} = f(S_{ОИ}, S_{СЗИ}, P_В, P_Р)$,

$R_{СЗИ} = f(S_{СЗИ}, P_В, P_Р)$,

$P_B = f(S_И, S_{ОИ})$,

$P_P = f(P_B, S_И, S_{ОИ}, S_{СЗИ})$.

Данные зависимости носят вероятностный характер. Математическая статистика и теория вероятностей используют экспериментальные данные, обладающие точностью и достоверностью. В данном случае понятия точности и достоверности не всегда применимы, так как эти вероятности зависят от «человеческих знаний», поэтому для достоверной количественной оценки указанных зависимостей можно использовать теорию нечетких множеств.

Инвестиции в СЗИ преследуют цель снижения риска экономического ущерба для предприятия от реализации угроз безопасности. Но как можно сравнить две различные системы защиты и сказать, что одна из них лучше другой? Основным критерием сравнения различных СЗИ служит эффективность как мера достижения цели. При этом цель ЗИ – недопущение реализации максимально возможного числа угроз в отношении ИС предприятия. Необходимое условие ее достижения – построение КСИБ.

Как известно, смысл основных постулатов разработки КСИБ заключается в следующем: невозможно создать абсолютную защиту, СЗИ должна быть комплексной и адаптируемой к изменяющимся условиям.

Вместе с тем главная цель предприятия – получение прибыли. Следовательно, оценивать эффективность СЗИ можно и с функциональной, и с экономической точки зрения.

Оценка сама по себе не является конечной целью построения СЗИ, она необходима для решения двух задач:

- построения оптимальной системы защиты;
- определения зависимости параметров функционирования СЗИ от изменяющихся внешних условий (построение адаптивной СЗИ).

Для многих показателей качества СЗИ, например экономической эффективности, необходимо получение количественного результата оценки, что существенно осложняется рядом факторов:

- наличием сложной опосредованной взаимосвязи показателей качества СЗИ с параметрами ИС;
- необходимостью учета и формализации ряда показателей ИС, многие из которых изначально задаются качественными величинами и имеют элементы неоднозначности;

➢ наличием существенной взаимосвязи и взаимозависимости этих показателей, имеющих противоречивый характер;

➢ трудностью получения исходных данных, необходимых для оценки СЗИ, в особенности на ранних этапах проектирования.

Экономически эффективной называется такая СЗИ, для которой выполняются следующие условия:

$$\begin{cases} S_{СЗИ} \le \Delta R_{И} + \Delta R_{ОИ} + \Delta R_{СЗИ}, \\ S_{СЗИ} \le S_{И} + S_{ОИ}, \end{cases} \quad (1.1)$$

где $\Delta R_{И} + \Delta R_{ОИ} + \Delta R_{СЗИ}$ – общее снижение рисков для ИС.

Если первое условие неоспоримо – получаемый эффект не должен быть меньше стоимости средств и мероприятий, т.е. затрат, то второе не настолько очевидно. И тем не менее действительно большая часть затрат предприятия направлена на выполнение его основной деятельности, а не на реализацию функций СЗИ.

1.2. Организация и проведение экспертизы ИС предприятия

Методы экспертных оценок

В условиях существования разнородности элементов и параметров ИС и преимущественно качественного описания многих показателей единственным адекватным способом проверки качества функционирования и уровня защищенности ИС является процедура экспертизы. В то время как для многих коммерческих ИС экспертиза носит добровольный характер, существует достаточно многочисленная категория ИС, для которых экспертиза, согласно действующему законодательству, – обязательное условие для начала или продолжения их эксплуатации. В их число входят ИС, предназначенные для обработки информации, составляющей государственную тайну, для управления экологически опасными объектами и для ведения секретных переговоров.

В настоящее время методы экспертных оценок применяют практически во всех областях науки. Сфера защиты информации – не исключение. Разработаны и используются различные методы, имеющие свои достоинства и недостатки и область применения.

Методы экспертных оценок – это методы организации работы со специалистами-экспертами и обработки мнений экспертов, выраженных в количественной и/или качественной форме с целью подготовки информации для принятия решений.

Для проведения экспертизы создают рабочую группу (аналитическую группу), которая и организует деятельность экспертов, объединенных в экспертную группу.

Организация опроса коллектива экспертов – одна из важнейших проблем, связанных с проведением экспертных оценок. Низкое качество собранных таким образом мнений не может быть компенсировано применением для обработки современных математических методов.

Можно выделить три типа процедур экспертного опроса:

- однотуровые анонимные процедуры;
- многотуровые анонимные процедуры;
- процедуры с личными контактами между экспертами.

Алгоритм проведения экспертизы

1. *Формулирование цели экспертизы и определение ее объектов.* Цель экспертизы качества ИС – проверка соответствия предъявляемым к ней требованиям безопасности. Основными критериями при проведении экспертизы служат требования, сформулированные в законах РФ, внутриведомственных, межведомственных, национальных и международных стандартах.

При определении объектов проведения экспертизы необходимо в равной степени учитывать организационный, физический и программно-технический уровни обеспечения безопасности. В противном случае результаты экспертизы не будут отражать реальный уровень защищенности ИС. Например, надежные технические методы защиты окажутся бесполезными, если неправильно определен состав административных мероприятий или меры обеспечения физической безопасности неадекватны.

Границы проведения экспертизы должны быть четко определены и обоснованы. Например, если ОС не попадает в границы объекта исследования, то нужно задокументировать предположение о том, что ОС обеспечивает достаточный базовый уровень защищенности в таких областях, как изоляция процессов, аутентификация, авторизация, мониторинг, контроль целостности, регистрация и учет событий и т. п.

2. *Формирование аналитической группы.* После определения объекта ИС и предъявленных требований безопасности к ИС формируется аналитическая группа (АГ). Ее задача заключается в подготовке экспертизы, оказании помощи в проведении оценки, обработке, анализе и обобщении ее результатов с целью выявления коллективного мнения экспертов. В большинстве случаев в подготовке и проведении экспертизы оценки защищенности ИС требуется участие специалистов различных технических профилей.

Состав АГ утверждается совместно заказчиком проведения экспертизы (руководителем, которому требуется провести исследование ИС своей организации) и организацией, занимающейся экспертной деятельностью. Если заказчик не прибегает к помощи специализированной организации, то он может сформировать АГ из собственных сотрудников.

При определении состава АГ и распределении работ учитывается ряд характеристик ИС. Основные характеристики, на которые обращают внимание, включают в себя количество и сложность программно-технических компонентов ИС.

В состав АГ входят организатор, ведущий специалист, программист, технические работники.

Организатор осуществляет методическое руководство работой на всех ее этапах и является руководителем всего проекта оценки объекта. Для выполнения этой задачи он должен квалифицированно разбираться в экспертных методах оценки объекта и методологии оценки защищенности ИС. Организатор составляет программу работ, участвует в опросе экспертов, формулирует выводы и рекомендации.

Основная задача ведущего специалиста заключается в анализе информации, полученной от экспертов, и корректировании программы дальнейшей работы.

Если ИС достаточно сложная, т.е. оценка проводится с учетом многих показателей качества, в состав рабочей группы может войти программист. Он анализирует полученные оценки с точки зрения уменьшения трудоемкости их обработки и извлечения максимально надежной и полной информации, выбирает и отлаживает стандартные программы и в случае необходимости разрабатывает новые программы.

Технические работники проводят опрос экспертов и предварительную обработку полученных результатов. Задача технического ра-

ботника заключается в разъяснении тех положений, которые недостаточно хорошо понимаются экспертами.

3. *Утверждение АГ состава экспертной группы (ЭГ).* Отбор и формирование группы экспертов начинается с определения области их компетенции, что позволяет надеяться на достаточную степень надежности экспертов, включаемых в ЭГ. Правильный отбор специалистов для участия в работе ЭГ очень важен, так как качество полученных оценок в значительной степени определяется качеством экспертной группы.

В состав ЭГ могут входить различные специалисты (не только в области информационной безопасности). Например, в связи с широким распространением методов социальной инженерии, используемых злоумышленниками, актуально участие в ЭГ специалистов-психологов.

4. *Подготовка необходимой информации об объектах экспертизы, её анализ и систематизация.* Существует два основных метода сбора информации:

- получение информации от персонала и разработчиков ИС;
- изучение документации.

При проведении экспертизы наибольшее количество времени тратится на изучение характеристик ИС. При изучении ИС рассматриваются два основных вопроса: назначение и принципы функционирования ИС и уровень защищенности ИС (угрозы безопасности, ресурсы, механизмы защиты, уязвимости).

Оба эти вопроса могут быть разрешены в ходе опросов пользователей и разработчиков ИС. Однако эти способы сбора информации требуют больших временных затрат.

Другой источник информации об объекте информатизации – проектная, рабочая и эксплуатационная документация. Иногда качество документации бывает низким или она просто отсутствует. Однако там, где она существует, ее объем может исчисляться сотнями и тысячами страниц печатного текста. Документация также может содержать устаревшие сведения.

Наиболее эффективный метод сбора информации об ИС – комплексный метод, при котором руководство организации, разрабатывающей либо эксплуатирующей ИС, ставит перед ее разработчиками или другим персоналом задачу подготовить такую информацию и представить ее экспертной группе.

Для проведения экспертизы должны быть подготовлены следующие документы:

- документы, содержащие требования безопасности;
- диаграммы информационных потоков;
- описание механизмов безопасности ИС.

5. *Предварительное ознакомление экспертов с материалами об объектах экспертизы и получение дополнительной информации.* Часто после ознакомления экспертов с подготовленной документацией, описывающей объект экспертизы, у них возникают различные вопросы, которые по возможности должны быть устранены изучением дополнительной информации. В основном это касается более детального описания информационных потоков и механизмов безопасности.

6. *Выбор процедуры проведения экспертизы.* Существует два принципа экспертного оценивания. В соответствии с первым принципом каждому объекту экспертизы дается оценка в целом, в соответствии со вторым – проводится многокритериальная оценка по каждому из критериев оценочной системы с последующим автоматизированным расчетом результирующей оценки. Кроме того, в рамках каждого принципа существует множество методов организации экспертного опроса.

Выбор того или иного вида опроса определяется многими факторами, из которых основные:

- цель и задачи экспертизы;
- существо и сложность анализируемой проблемы;
- полнота и достоверность исходной информации;
- требуемый объем информации, получаемой в результате опроса;
- время, отведенное на опрос и экспертизу в целом;
- допустимая стоимость опроса и экспертизы в целом;
- количество экспертов, степень их компетенции.

Каждый вид экспертного оценивания обладает своими преимуществами и недостатками, определяющими рациональную область применения. Во многих случаях наибольший эффект дает комплексное применение нескольких видов экспертизы.

7. *Определение оценочной системы.* Рациональное использование информации, полученной от экспертов, возможно при условии преобразования ее в форму, применимую для дальнейшего анализа.

Информация, полученная от экспертов, должна быть направлена на решение таких задач, которые содержат неопределенности, связан-

ные не только с измерением, но и с самим характером исследуемых целей, средств их достижения и внешних условий.

Если эксперт в состоянии сравнить и оценить возможные варианты действий, приписав каждому из них определенное число, значит, он обладает определенной системой предпочтений. В зависимости от того, по какой шкале могут быть заданы эти предпочтения, экспертные оценки содержат больший или меньший объем информации и обладают различной способностью к формализации.

8. *Оценка объектов экспертизы в соответствии с принятой процедурой и выбранной оценочной системой.* Данный этап предполагает получение массива первичных оценок экспертов по всем оцениваемым параметрам. Такие оценки чаще всего представляются в виде таблиц.

9. *Обработка первичных результатов экспертизы.* Полученные первичные оценки могут быть качественными, тогда для получения количественного результата необходимо их преобразование в количественные значения по таблицам соответствия или с использованием баз знаний. Кроме того, оценки параметров, имеющих разный физический смысл, даны в разных шкалах, следовательно, требуется сведение оценок в рамках единой модели и получение нескольких общих показателей.

Еще один важный вопрос обработки результатов – оценка согласованности экспертных суждений. В связи с невозможностью абсолютной формализации получения первичных оценок суждения экспертов будут расходиться. Степень такого расхождения (или обратный ей показатель – степень согласованности) показывает качество полученной единой оценки и ее адекватность.

10. *Обсуждение результатов экспертизы и принятие решения.* Если результаты экспертизы можно считать адекватными, тогда решением будет признание СЗИ эффективной или неэффективной, после чего возможна выработка рекомендаций по повышению ее эффективности. Если результаты экспертизы признаются аналитической группой недостаточно убедительными, проводится повторная экспертиза.

1.3. Методы организации экспертного опроса

Метод анкетирования. Анкета – это определенным образом организованный набор вопросов, ответы на которые позволяют получить информацию об объекте экспертизы, необходимую для проведе-

ния управленческого анализа. От вида анкеты, ее структуры, сформулированных в ней вопросов во многом зависит характер информации, получаемой в результате анкетирования.

Анкетирование – метод сбора первичного материала в виде письменного опроса большого количества респондентов, что дает возможность свести к минимуму нетипичные проявления, при этом не обязателен личный контакт с респондентом. Анкеты удобно подвергать математической обработке.

Анкеты бывают открытого и закрытого типов. В анкете закрытого типа на каждый вопрос даны варианты ответа, а в анкете открытого типа ответы могут быть выражены в произвольной форме.

Первый этап в разработке анкеты – определение ее содержания. Составление анкеты заключается в переводе основных гипотез исследования на язык вопросов. Если помимо самого мнения необходимо знать и его интенсивность, то в формулировку вопроса включают соответствующую шкалу оценок.

Второй этап заключается в выборе нужного типа вопросов (открытые – закрытые, основные – функциональные).

Третий этап связан с определением числа и порядка задаваемых вопросов.

Анкетные данные тем достовернее, чем больше лиц опрошено. Типичный недостаток метода анкетирования – неточность в формулировке вопросов, что порождает ошибочные ответы. Порой встречается обилие вопросов, сходных по содержанию, вызывающих недоумение и механические ответы без серьезных раздумий. Неумелая мотивировка важности анкетного опроса ведет к попытке угадывания ответа, нужного исследователю.

Грамотно составленные анкеты должны удовлетворять обычным критериям надежности и валидности, но помимо этого каждый вопрос анкеты проверяется по различным критериям. Например, предусмотрены ли такие варианты ответов, как «не знаю», «затрудняюсь ответить». Они предоставляют респонденту возможность уклониться от ответа, когда он сочтет это нужным.

Анкетирование при оценке защищенности ИС используется при проверке на соответствие системы защиты какому-либо стандарту.

Преимущество в сравнении с другими методами – возможность организации экспертизы любого объекта без использования каких-либо формальных моделей.

Недостаток – для адекватной оценки необходимо разработать анкеты с четкими описаниями всех аспектов исследуемого объекта, что ограничивает область применения, так как это не всегда возможно.

Метод комиссий. Суть метода комиссий заключается в том, что группа экспертов многократно собирается для обсуждения одного и того же вопроса. Организатор экспертизы не руководит обсуждением, а лишь обеспечивает активную работу каждого эксперта. При проведении данного метода эксперты используют большой объем исходной информации, т.е. они оперируют фактами не по одному вопросу, а по проблеме в целом.

Метод комиссий предусматривает проведение экспертизы в форме свободного обмена мнениями для получения общего суждения экспертов. Очная форма общения экспертов значительно сокращает время экспертизы, облегчает получение единого согласованного мнения. При использовании метода комиссий предварительно разрабатывается программа обсуждения. Группа экспертов формируется способом назначения. Обычно это 10 – 12 человек.

Средствами обеспечения открытости могут служить, в частности, личные высказывания экспертов и по возможности отказ от обезличенных суждений типа «обычно считается, что» или «говорят, что». В рамках обсуждения проблемы эксперты следуют принципу психологической безопасности: позиция эксперта и те суждения, которые он высказывает, не должны оскорблять достоинство других экспертов или превращать обсуждение проблемы в способ утверждения собственного превосходства.

Коллективное мнение экспертов определяется в результате открытого или тайного голосования. В некоторых случаях к голосованию не прибегают, выявляя результирующее мнение в процессе дискуссии.

Преимущества – рост информированности экспертов, поскольку при обсуждении они приводят обоснования оценок, и обратная связь: под воздействием полученной информации эксперт может изменить первоначальную точку зрения.

Недостатки – отсутствие анонимности, конформизм, т.е. присоединение мнения эксперта к мнению более компетентных и авторитетных экспертов, даже при наличии противоположной собственной точки зрения. Дискуссия часто сводится к полемике наиболее авторитетных экспертов.

Метод мозговой атаки. Разработан в 50 – 60-е гг. XX в. Основная задача – выявление новых идей. Обсуждаемая проблема должна быть четко сформулирована. Любая идея должна быть обсуждена и не должна быть признана ложной. В методе мозговой атаки большую роль играет человек, проводящий экспертизу. Но он не должен выделять более значимые и перспективные идеи, иначе результат экспертизы оказывается менее значительным.

В экспертную группу обычно входят 3–5 экспертов, составляющих ее основу, 5 специалистов в области проблематики, ведущий и секретарь, записывающий все предложения. В процедуре экспертизы не должны участвовать одни и те же лица – в этом случае, по мнению психологов, группа может перестать генерировать новые идеи.

Процесс принятия группового решения делится на две части: на первом этапе участники дискуссии предлагают любые, пусть даже самые авантюрные и невероятные варианты решения, на втором этапе начинается их обсуждение.

После завершения первой части ведущий анализирует все выработанные решения, отбрасывает возможные повторы и разбивает их на группы по принципу схожести. После этого эксперты проверяют на прочность каждую идею. Все предложения детально разбираются и подвергаются критике. Результат – наиболее удачные идеи, которые находят отражение в итоговом документе.

Область применения – экспертизы с выработкой рекомендаций. Если при анализе защищенности ИС требуется определить потенциальные угрозы и уязвимости объекта, влияющие на оценку возможных потерь, то метод мозговой атаки позволяет сформировать их детальный список.

Достоинство – не требуются формальные модели, анкеты и сама аналитическая группа.

Недостаток – низкая адекватность оценки.

Метод Дельфи. Разработан О. Хелмером и Н. Делки. В настоящее время он представляет собой, по существу, группу методов, объединенных общими требованиями к организации экспертных процедур и форме получения экспертных оценок.

В методе Дельфи предусматривается анонимность процедуры, с одной стороны, и возможность пополнить информацию о предмете экспертизы, с другой стороны, а также обратная связь, позволяющая экспертам корректировать свои суждения с учетом промежуточных усредненных оценок и пояснений экспертов, высказывавших крайние точки зрения.

Экспертизы по методу Дельфи проводятся чаще всего в четыре тура. В первом туре экспертам сообщают цель экспертизы, формулируют вопросы, ответы на которые составляют основное содержание экспертизы. Вопросы для эксперта представляют в виде анкеты, иногда с пояснительной запиской.

Информация, полученная от эксперта, поступает в распоряжение аналитической группы.

Во втором туре экспертам предъявляют усредненную оценку экспертной комиссии и обоснования экспертов, высказавших крайние оценки. Указания представляются анонимно. После получения дополнительной информации эксперты, как правило, корректируют свои оценки. Скорректированная информация вновь поступает в аналитическую группу.

Третий и четвертый туры аналогичны второму.

Характерная особенность метода Дельфи – уменьшающийся от тура к туру разброс оценок, их возрастающая согласованность. В некоторых случаях согласованная точка зрения экспертов может быть получена уже после второго и третьего тура. При некоторых экспертизах требуется проведение не менее пяти туров.

Достоинство – получение наиболее согласованной оценки экспертов.

Недостатки – итерационный процесс оценки, необходимость обоснования мнений экспертов, большой объем аналитической работы.

Метод Дельфи – универсальное средство при проведении экспертизы оценки качества ИС.

Метод сценариев. Даёт возможность с тем или иным уровнем достоверности определить возможные тенденции развития системы, взаимосвязи между действующими факторами, сформировать карти-

ну возможных состояний, к которым может прийти ситуация под влиянием тех или иных воздействий.

Профессионально разработанные сценарии позволяют более полно и отчетливо определить перспективы развития ситуации как при наличии различных воздействий, так и при их отсутствии.

Сценарии ожидаемого развития ситуации позволяют своевременно осознать опасности, которыми чреваты неудачные воздействия или неблагоприятное развитие событий.

Составление сценария обычно включает в себя несколько этапов.

1. Структурирование исходных данных и формулировка вопроса. Вопрос, выбранный для анализа, должен быть определен так точно, как это возможно. На данном этапе должна быть собрана и проанализирована базовая информация и построена структура проекта.

2. Определение системы. Для осуществления второго этапа необходимо выделить критические точки системы и оценить их влияние на будущее системы.

3. Установление показателей желаемого будущего системы. Необходимо определить возможное состояние критических точек в будущем исходя из намеченных целей. Показатели будущего состояния не должны быть чрезмерно завышенными.

4. Установление показателей реального будущего системы. Если на третьем этапе определилось будущее состояние системы исходя из собственных целей, то на четвертом этапе возможное развитие системы предполагают исходя из её сегодняшнего состояния и всевозможных изменений.

5. Сопоставление намеченных показателей будущего состояния системы с предположениями об их развитии. На этом этапе сопоставляются результаты третьего и четвертого этапов. Повышенные или заниженные показатели состояния среды корректируются при помощи данных, полученных на четвертом этапе.

6. Введение разрушительных событий. Разрушительное событие – это внезапно случившийся инцидент, который не был ранее спрогнозирован. Разрушительные события могут иметь как отрицательный характер, так и положительный. Из возможных разрушительных событий нужно выделить те, которые способны оказать наиболее сильное воздействие, и учесть их при составлении сценариев.

7. Установление последствий. На этом этапе сопоставляются возможные проблемы системы и выбранные варианты развития среды.

8. Принятие мер. Реорганизация системы в зависимости с выбранным прогнозом.

Достоинство – простота экспертизы иерархических систем.

Недостаток – большой объем аналитической работы.

Примером использования данного метода при оценке защищенности объекта может служить тестирование программного обеспечения по принципу «чёрного ящика» или «белого ящика».

Метод анализа формальной модели на основе сравнений альтернатив. Создают формальную модель, описывающую исследуемый объект. Параметры модели задают лингвистическими описаниями. Оценка экспертом параметра объекта заключается в выборе наиболее соответствующего ему описания. Метод требует представления оценок в виде матриц парных сравнений альтернатив для дальнейшей математической обработки с целью получения числовых значений, соответствующих лингвистическим описаниям.

Достоинства – достаточно адекватная оценка при отсутствии итерационной процедуры, формализация проведения оценки любого параметра, минимальный объем работы аналитической группы.

Недостаток – требуется формальная модель, описывающая исследуемый объект.

1.4. Преобразование первичной экспертной информации

Шкалы и оценочные системы

При формализации информации с помощью номинальных шкал в экспертных методах используют следующие аксиомы четкой логики:

- А либо есть В, либо есть не В;
- если А есть В, то В есть А;
- если А есть В и В есть С, то А есть С.

Критерии в данном случае выступают как ассоциативные показатели, обладающие информацией, которая может быть формализована в виде бинарных оценок двух уровней: 1 (идентичен) или 0 (различен).

В тех случаях, когда четкое описание оцениваемого объекта невозможно, использование данных аксиом недопустимо и оценочная

система должна основываться на математическом аппарате теории нечетких множеств.

Шкала порядка. В случаях, когда исследуемые объекты можно в результате сравнения расположить в определенной последовательности с учетом какого-либо существенного критерия (критериев), используют порядковые шкалы, позволяющие устанавливать равноценность или доминирование.

Предположим, что необходимо расположить в определенной последовательности n объектов по какому-либо критерию. Представим это упорядочение в виде матрицы $A(a_{ij})$, где $i, j = 1, 2, \ldots, n$.

Величины a_{ij} устанавливают соотношения между объектами и могут быть определены следующим образом:

$$a_{ij} = \begin{cases} +1, \text{если } i \text{ предпочтительнее } j, \\ -1, \text{если } j \text{ предпочтительнее } i, \\ 0, \text{ если } i, j \text{ равноценны.} \end{cases} \qquad (1.2)$$

Основные аксиомы, необходимые для соблюдения условий упорядочивания, следующие.

Соотношение $a_{ij} = +1$ должно быть ассиметричным, т.е. если $a_{ij} = +1$, то $a_{ji} = -1$, и транзитивным, т.е. если $a_{ij} = +1$, $a_{jk} = +1$, то $a_{ik} = +1$.

Соотношение $a_{ij} = 0$ называется соотношением эквивалентности. Такое соотношение должно быть:

а) рефлексивным, т.е. $a_{ij} = 0$;

б) симметричным, т.е. если $a_{ij} = 0$, то $a_{ji} = 0$;

в) транзитивным, т.е. если $a_{ij} = 0$ и $a_{jk} = 0$, то $a_{ik} = 0$.

Кроме того, эти два соотношения должны быть совместимы, т.е. если $a_{ij} = +1$ и $a_{jk} = 0$, то $a_{ik} = +1$, а также если $a_{ij} = 0$ и $a_{jk} = +1$, то $a_{ik} = +1$.

И, наконец, упорядочение должно быть связным, т.е. для любых i и j либо $a_{ij} = +1$, либо $a_{ij} = -1$, либо $a_{ij} = 0$.

Использование порядковых шкал позволяет различать объекты и в тех случаях, когда критерий не задан в явном виде, т.е. когда мы не знаем признака сравнения, но можем частично или полностью

упорядочить объекты на основе системы предпочтений, которой обладает эксперт.

Допустимыми преобразованиями для данного типа шкалы являются все монотонные преобразования, которые не нарушают порядок следования значений измеряемых величин.

Порядковая шкала может использоваться для оценки значимости любой характеристики объекта. Разновидностью шкалы порядка является *шкала рангов*, где используются только натуральные числа от единицы.

Шкала интервалов. Используется для отображения величины различия между свойствами объектов. Шкала может иметь произвольные масштаб и точки отсчета. Применяется для оценки практически всех количественных параметров.

Здесь между значениями x из первой шкалы и y – из второй допустимы линейные преобразования: $y = kx + b$, где k – любое положительное число, а b может быть как положительным, так и отрицательным. Это значит, что в разных шкалах может использоваться разный масштаб единиц (k) и разные начала отсчета (b).

В ряде случаев при формализации экспертных оценок используется свойство аддитивности, которое присуще только шкале отношений. Наличие аддитивности выражается следующими аксиомами:

а) если $j = a$ и $i > 0$, то $i + j > a$;

б) $i + j = j + i$;

в) если $i = a$ и $j = b$, то $i + j = a + b$;

г) $(i + j) + k = i + (j + k)$.

Шкала отношений. Используется для отражения отношения свойств объектов, т.е. во сколько раз свойство одного объекта превосходит свойство другого. При большом диапазоне измеряемых значений может использоваться логарифмический масштаб.

Разности между значениями на шкале интервалов становятся мерами на шкале отношений, т.е. на обычной числовой шкале, так как в результате вычитания можно избавиться от постоянного слагаемого b.

Для этого типа шкалы должно выполняться соотношение $y = kx$, где k – любое положительное число. Такая шкала используется для оценки числовых значений, если сложно установить единицу измерения (например для параметра «производительность системы»). Если указана единица измерения, то это *абсолютная шкала.*

Шкала разностей. Используется для измерения свойств объектов при необходимости указания, на сколько один объект превосходит другой по одному или нескольким признакам. Она является частным случаем шкалы интервалов при выборе единицы масштаба.

Шкала относительной значимости. Основывается на шкале рангов. Используется для описания отношения двух сравниваемых качественных значений. Соответствие описания отношений и присваиваемых им значений представлено в табл. 1.1. Ряд числовых значений представляет собой некую оценочную шкалу, например по методу Саати взяты значения от 1 до 9.

Таблица 1.1

Представление шкалы относительной значимости

Описание отношения первого объекта ко второму	Значение
Абсолютное (подавляющее) превосходство	9
Очевидное превосходство	7
Сильное (существенное) превосходство	5
Умеренное (слабое) превосходство	3
Равная значимость	1

Значения 2, 4, 6, 8 могут использоваться как промежуточные. При отношении 1-го объекта ко 2-му, равному, например, 5, отношение 2-го к 1-му равно 1/5.

Определение первичных значений параметров

Результаты первичной оценки параметров ИС – качественные или количественные описания. Примеры качественных описаний: «отсутствие решеток на окнах охраняемого помещения», «низкая значимость некоторой уязвимости», «для использования уязвимости требуются специальные средства», «высокий потенциал нарушителя», «реализация данной угрозы принесет существенный вред».

Примеры количественных описаний: «в защищаемом помещении двойная дверь с тремя врезными замками», «количество видеокамер – 1», «минимальная длина пароля – 5 символов», «период обновления антивирусных баз – 1 месяц».

Первичные оценки выставляются экспертами двумя способами:

- непосредственно как точечные значения на определенной шкале;
- путем парных сравнений.

Оцениваемые параметры разнородны и для их совместного использования в одной модели необходимо:

- преобразовать качественные описания в количественные;
- нормировать количественные данные с учетом их значимости.

Для решения первой задачи требуется построить оценочные таблицы (см. табл. 1.1).

Для решения второй задачи оценки, полученные с использованием однородных шкал, могут быть нормированы путем преобразования шкалы. Неоднородные оценки можно нормировать сведением к единичному интервалу [0, 1] с учетом весовых коэффициентов при последующих преобразованиях.

Типовые примеры лингвистических оценочных таблиц для различных качественных параметров приведены в табл. 1.2 – 1.5.

Таблица 1.2

Значимость уязвимости (по шкале относительной значимости)

Лингвистическая оценка сравнения 1-й и 2-й уязвимости	Значение
При наличии 1-й уязвимости наличие 2-й можно не учитывать	9
Существенное превосходство значимости 1-й уязвимости над 2-й уязвимостью	7
Использование 1-й уязвимости предпочтительнее, чем 2-й	5
Чуть более высокая значимость 1-й уязвимости против 2-й	3
Одинаковая значимость сравниваемых уязвимостей	1

Таблица 1.3

Доступность уязвимости (по ранговой шкале)

Лингвистическая оценка	Значение
Уязвимость общеизвестна, для ее использования не требуется спецсредств и особых способностей	9
Уязвимость общеизвестна, но для ее использования требуются относительно доступные технические средства	7
Уязвимость распространенная, для ее использования требуются дорогостоящие или широко не доступные спецсредства	5
Уязвимость малоизвестна и/или для ее использования требуются дорогостоящие или широко не доступные спецсредства, ресурсы, мероприятия и т.д.	3
Использование уязвимости требует таких ресурсов и средств, применение которых скрытно невозможно или требует огромных затрат времени	1

Таблица 1.4

Вред от реализации угрозы (по шкале относительной значимости)

Лингвистическая оценка	Значение
Последствия 2-й угрозы ничтожны по сравнению с последствиями 1-й угрозы	9
Вред, наносимый 1-й угрозой, на порядок больше, чем вред 2-й угрозы	7
Вред, наносимый 1-й угрозой, в несколько раз больше, чем вред 2-й угрозы	5
Вред, наносимый 1-й угрозой, в 1,1 – 2 раза больше, чем вред 2-й угрозы	3
Вред, наносимый 1-й и 2-й угрозами, отличается не более чем на 10 %	1

Таблица 1.5

Ценность информации (по ранговой шкале)

Лингвистическая оценка ценности ресурсов на основе расчета затрат на восстановление	Значение
Данный информационный ресурс важнейший для организации. Его потеря приведет к непоправимым последствиям для организации	9
Затраты на ликвидацию последствий из-за потери ресурса сопоставимы с годовыми экономическими показателями организации	8
Затраты на восстановление из-за потери ресурса существенны для организации	6
Затраты на восстановление несущественны, но требуется дополнительное время	2
Восстановление из-за потери ресурса будет проведено в штатном режиме	1

Описание множества сравниваемых параметров с использованием шкалы относительной значимости представляется в виде матрицы парных сравнений:

$$M_j^A = \begin{vmatrix} a_{11}^j & a_{12}^j & \dots & a_{1n}^j \\ a_{21}^j & a_{22}^j & \dots & a_{2n}^j \\ \dots & \dots & \dots & \dots \\ a_{n1}^j & a_{n2}^j & \dots & a_{nn}^j \end{vmatrix}, \qquad (1.3)$$

где $A = \{ a_1, a_2, ..., a_n \}$ – множество параметров, $j \in \{ 1, 2, ..., m \}$ – номер эксперта.

Матрица (1.3) обратносимметричная, т.е. для нее выполняется условие

$$a_{\alpha\beta}^{j} = \frac{1}{a_{\beta\alpha}^{j}}, \quad \forall \alpha,\beta \in \overline{1,n},\ \forall j \in \overline{1,m}. \tag{1.4}$$

То есть эксперт определяет только значения элементов матрицы выше (или, наоборот, ниже) главной диагонали. При этом количество сравниваемых элементов определяется по формуле

$$KC = \frac{n(n-1)}{2}. \tag{1.5}$$

Таким образом матрица (1.3) может быть преобразована к виду

$$M_{j}^{A} = \begin{vmatrix} 1 & \frac{1}{a_{21}^{j}} & \dots & \frac{1}{a_{n1}^{j}} \\ a_{21}^{j} & 1 & \dots & \frac{1}{a_{n2}^{j}} \\ \dots & \dots & \dots & \dots \\ a_{n1}^{j} & a_{n2}^{j} & \dots & 1 \end{vmatrix}. \tag{1.6}$$

Для нахождения числовых значений параметров необходимо определить собственные значения матрицы (1.6) и собственный вектор

$$A_j = \left\{ x_i^j \right\}, \quad i = \overline{1,n}, \tag{1.7}$$

соответствующий максимальному собственному значению $\lambda_{\max}^{j}$ оценок j-го эксперта.

Данная матрица положительно определенная, обратносимметричная и, как известно из линейной алгебры, ее ранг равен единице, а максимальное собственное число $\lambda_{\max}$ – размерности этой матрицы (т.е. n).

При проведении сравнений в реальной ситуации вычисленное максимальное собственное число $\lambda_{\max}^{j}$ будет отличаться от соответствующего собственного числа $\lambda_{\max}$ для идеальной матрицы вследствие нарушения ее транзитивности. Найденные значения тем точнее, чем ближе $\lambda_{\max}^{j}$ к n. Причем всегда $\lambda_{\max}^{j} \geq n$. Разница $\lambda_{\max}^{j} - n$ дает абсолютную меру несогласованности оценок. Относительная мера (коэффициент рассогласования)

$$K_P^j = \frac{\lambda_{\max}^{j} - n}{n-1} \tag{1.8}$$

может быть использована для коррекции коэффициента авторитета j-го эксперта.

Собственный вектор матрицы (1.6) определяется из уравнения

$$\left(M_j^A - \lambda_{\max}^j E\right) A_j = 0. \qquad (1.9)$$

Оно имеет ненулевое решение тогда и только тогда, когда определитель матрицы $\left(M_j^A - \lambda E\right)$ равен нулю:

$$\det \begin{vmatrix} 1-\lambda & \frac{1}{a_{21}^j} & \dots & \frac{1}{a_{n1}^j} \\ a_{21}^j & 1-\lambda & \dots & \frac{1}{a_{n2}^j} \\ \dots & \dots & \dots & \dots \\ a_{n1}^j & a_{n2}^j & \dots & 1-\lambda \end{vmatrix} = 0. \qquad (1.10)$$

Максимальное значение λ, определенное из выражения (1.10), – искомое максимальное собственное число $\lambda_{\max}^j$.

Собственный вектор (1.6) определяется при решении уравнения

$$\begin{vmatrix} 1-\lambda_{\max}^j & \frac{1}{a_{21}^j} & \dots & \frac{1}{a_{n1}^j} \\ a_{21}^j & 1-\lambda_{\max}^j & \dots & \frac{1}{a_{n2}^j} \\ \dots & \dots & \dots & \dots \\ a_{n1}^j & a_{n2}^j & \dots & 1-\lambda_{\max}^j \end{vmatrix} \cdot \begin{vmatrix} x_1^j \\ x_2^j \\ \dots \\ x_n^j \end{vmatrix} = 0. \qquad (1.11)$$

Получаем систему

$$\begin{cases} \left(1-\lambda_{\max}^j\right) x_1^j + \frac{x_2^j}{a_{21}^j} + \dots + \frac{x_n^j}{a_{n1}^j} = 0, \\ \dots \\ a_{n1}^j x_1^j + a_{n2}^j x_2^j + \dots + \left(1-\lambda_{\max}^j\right) x_n^j = 0, \end{cases} \qquad (1.12)$$

которая имеет только нулевое решение.

Для нахождения собственного вектора заменяем одно из уравнений системы (1.12) условием нормировки $\sum_{i=1}^{n} x_i^j = 1$.

1.5. Вычисление коэффициентов авторитета экспертов

Коэффициент авторитета (степень компетентности эксперта) – это число, которое показывает, с каким весом включаются в стати-

стическую обработку оценки данного эксперта. Этот коэффициент влияет на достоверность результатов экспертизы и имеет важное психологическое значение для экспертов.

Существует ряд способов определения коэффициентов авторитета на основе статистики предыдущих экспертиз. В этих способах коэффициенты авторитета задают непосредственно как некоторые числа из [0, 1].

Также возможно вычисление коэффициентов авторитета на основе матрицы парных сравнений компетентности экспертов:

$$M_v = \begin{vmatrix} v_{11} & v_{12} & \dots & v_{1m} \\ v_{21} & v_{22} & \dots & v_{2m} \\ \dots & \dots & \dots & \dots \\ v_{m1} & v_{m2} & \dots & v_{mm} \end{vmatrix}, \qquad (1.13)$$

где $\nu_{\alpha\beta} = \dfrac{1}{\nu_{\beta\alpha}}, \quad \forall \alpha, \beta \in \overline{1, m}, -$ сравнительные описания компетентности, построенные на основе шкалы относительной значимости.

Проблема этого способа состоит в том, что разработчик матрицы должен быть экспертом в области оценки экспертов. Этот способ может применяться только в экспертных организациях.

Если статистики не существует или она недостаточная и невозможно построить матрицу сравнения компетентности, то коэффициенты авторитета могут быть определены на основе формальных сведений об эксперте и нормированы по условию

$$\sum_{j=1}^{m} v_j^0 = 1. \qquad (1.14)$$

Могут использоваться следующие сведения об экспертах:

A) образование;

B) научная подготовка;

C) стаж работы по приоритетному направлению;

D) количество проведенных экспертиз.

Оценка может быть проведена с использованием шкалы баллов (табл. 1.6).

Таблица 1.6

Шкала оценки компетентности экспертов

Направление	Описание внутри направления	Балл
A	по приоритетному направлению	5
	по смежной специальности	4
	по направлению (неоконченное)	3
	по смежной специальности (неоконченное)	2
	не совпадает с профилем экспертизы	0
B	академик	5
	доктор наук	4
	кандидат наук	3
	аспирант, снс	2
	без степени	0
C	не менее 10 лет	5
	не менее 5 лет	4
	не менее 1 года	3
	менее 1 года	1
	отсутствует	0
D	более 20	5
	10 – 20	4
	4 – 9	3
	1 – 3	1
	нет	0

Количество баллов по пунктам A, B, C, D суммируется, таким образом определяется первичный балл эксперта B_j^0.

Коэффициент авторитета с учетом нормирования вычисляется по формуле:

$$\nu_j^0 = \frac{B_j^0}{\sum_{j=1}^{m} B_j^0}. \qquad (1.15)$$

При проведении сложных экспертиз СЗИ обращения к экспертам сопряжены с определенными финансовыми издержками. Учитывая это обстоятельство, при формировании экспертной группы можно использовать следующую методику.

Пусть C_k – условная стоимость обращения к *k*-му эксперту, а C – граничная суммарная стоимость обращения ко всем экспертам.

Пусть $x_k = 1$, если эксперт включен в группу, и $x_k = 0$, если нет.

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

$$\begin{cases} \sum_k v_k \cdot x_k \to \max, \\ \sum_k C_k \cdot x_k \le C. \end{cases} \qquad (1.16)$$

Краткие выводы

Для коммерческих предприятий защита информации рассматривается в контексте экономической эффективности. Методология оценки эффективности СЗИ предполагает использование различных критериев, называемых показателями качества, или параметрами ИС. Они определяют показатели качества самой СЗИ, которые можно оптимизировать. Оценка эффективности СЗИ не является самоцелью, а служит для построения оптимальной и адаптивной СЗИ.

Элементы и параметры ИС разнородные, многие показатели имеют преимущественно качественное описание. В этих условиях единственный адекватный способ проверки качества функционирования и уровня защищенности ИС – процедура экспертизы.

Качество результатов экспертизы определяется грамотным выбором одного из множества методов организации экспертного опроса и строгим следованием формальному алгоритму ее проведения.

Оценка параметров ИС экспертами проводится в рамках определенных шкал и оценочных систем. Результатами первичной оценки могут быть как количественные, так и качественные значения. Для получения вторичных и интегральных оценок качественные значения необходимо преобразовать в количественные, а значения, полученные по разнородным шкалам, следует нормировать сведением к одному интервалу с учетом весовых коэффициентов.

Оценки одного параметра, получаемые разными экспертами, могут существенно отличаться друг от друга. В большей степени это касается качественных описаний. Для получения оценки, общей для всей ЭГ, прежде всего необходимо определиться с тем, с каким весом будут включены в интегральный результат значения каждого эксперта, т.е. определить коэффициенты авторитета. Наиболее простой и

адекватный способ – их вычисление на основе формальных сведений об экспертах по нескольким направлениям. По результатам таких вычислений, если есть возможность выбора, можно сформировать экспертную группу, обладающую наибольшей компетентностью.

Контрольные вопросы

1. Перечислите основные критерии оценки эффективности СЗИ.
2. Расскажите о зависимостях и взаимосвязи параметров ИС.
3. С каких точек зрения можно оценивать эффективность СЗИ?
4. Какие факторы оказывают влияние на получение количественного результата оценки эффективности СЗИ?
5. Запишите и поясните условие, при котором СЗИ считается экономически эффективной.
6. Что такое методы экспертных оценок и какие типы процедур экспертного опроса существуют?
7. Опишите в целом алгоритм проведения экспертизы.
8. Опишите метод анкетирования для организации экспертного опроса.
9. Опишите метод комиссий для организации экспертного опроса.
10. Опишите метод мозговой атаки.
11. Опишите метод Дельфи для организации экспертного опроса.
12. Опишите метод сценариев для организации экспертного опроса.
13. Опишите метод анализа формальной модели на основе сравнений альтернатив для организации экспертного опроса.
14. Опишите свойства шкалы порядка.
15. Опишите свойства шкалы интервалов.
16. Опишите свойства шкалы отношений.
17. Опишите свойства шкалы относительной значимости.
18. Как используют различные шкалы при проведении экспертизы?
19. Какие существуют виды результатов первичной оценки параметров ИС? Какие задачи возникают при их дальнейшем использовании и как они решаются?
20. Приведите примеры оценочных таблиц качественных параметров.
21. Как математически решается задача получения значений параметров ИС из матрицы парных сравнений?
22. Что такое коэффициент рассогласования?
23. Для чего нужен коэффициент авторитета эксперта и на основе каких формальных сведений о нем он может быть вычислен?

Глава 2. ОСНОВЫ ТЕОРИИ НЕЧЕТКИХ ОЦЕНОК КАЧЕСТВЕННЫХ ПОКАЗАТЕЛЕЙ

2.1. Нечеткие множества и нечеткие числа

Определение и свойства нечеткого множества

Пусть $X = \{ x \}$ – универсальное множество, т.е. полное множество, охватывающее всю проблемную область.

Нечеткое множество $A \subset X$ представляет собой набор пар $\{(x, \mu_A(x))\}$, где $x \in X$ и $\mu_A : X \to [0, 1]$ – функция принадлежности как некоторая субъективная мера соответствия элемента нечеткому множеству. $\mu_A(x)$ может принимать значения от нуля, который обозначает абсолютную непринадлежность, до единицы, которая, наоборот, говорит об абсолютной принадлежности элемента x нечеткому множеству A.

Если нечеткое множество A определено на конечном универсальном множестве $X = \{ x_1, x_2, ..., x_n \}$, то его можно обозначить следующим образом:

$$A = \mu_A(x_1) / x_1 + \mu_A(x_2) / x_2 + ... + \mu_A(x_n) / x_n, \qquad (2.1)$$

где $\mu_A(x_i) / x_i$ – пара «значение функции принадлежности / элемент», называемая синглтоном, а “+” обозначает совокупность пар.

Пример. Пусть $X = \{ 1, 2, ..., 10 \}$. Тогда нечеткое множество «большие числа» может быть представлено следующим образом:

A = «большие числа» = 0,1/5 + 0,2/6 + 0,5/7 + 0,8/8 + 1/9 + 1/10.

Это следует понимать так: 9 и 10 с абсолютной уверенностью можно отнести к «большим числам»; 8 – «большое число» со степенью 0,8; 1, 2, ..., 4 абсолютно не являются «большими числами».

Нечеткое множество может быть представлено графиком функции принадлежности. В частном случае функция принадлежности может быть аппроксимирована, как показано на рис. 2.1. Тогда для рассматриваемого типа нечеткого множества потребуется только два значения: $\underline{a}$ и $\overline{a}$.

Типы нечетких множеств могут быть и другими, тогда может потребоваться больше значений.

Свойства нечетких множеств. 1. Нечеткое множество $A \subset X$ пустое, т.е. $A = \varnothing$, если $\mu_A(x) = 0, \ \forall x \in X$.

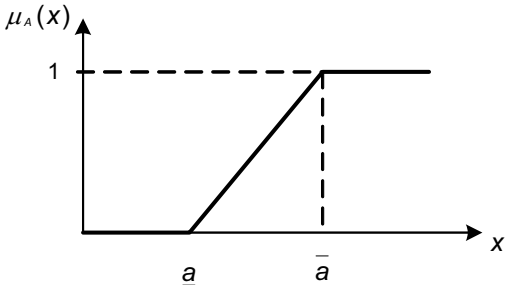


Рис. 2.1. Аппроксимация функции принадлежности нечеткого множества

2. Нечеткие множества $A, B \subset X$ эквивалентны, т.е. $A = B$, если $\mu_A(x) = \mu_B(x), \ \forall x \in X$.

3. Нечеткое множество $A \subset X$ – подмножеством нечеткого множества $B \subset X$, т.е. $A \subset B$, если $\mu_A(x) \le \mu_B(x), \ \forall x \in X$.

Пример. Пусть $X = \{1, 2, 3\}$. $A = 0{,}3/1 + 0{,}5/2 + 1/3$, $B = 0{,}4/1 + 0{,}6/2 + 1/3$. Тогда $A \subset B$.

Кардинальное число (мощность) нечеткого множества (2.1)

$$\text{card } A = |A| = \sum_{i=1}^{n} \mu_A(x_i). \qquad (2.2)$$

Пример. Если $X = \{1, 2, 3, 4\}$, $A = 0{,}1/1 + 0{,}4/2 + 0{,}7/3 + 1/4$, то $|A| = 2{,}2$.

Операции над нечеткими множествами

1. Дополнением нечеткого множества A называется нечеткое множество $\overline{A}$, функция принадлежности которого равна

$$\mu_{\overline{A}}(x) = 1 - \mu_A(x), \forall x \in X. \qquad (2.3)$$

2. Пересечением двух нечетких множеств $A, B \subset X$ называется нечеткое множество $A \cap B$, функция принадлежности которого

$$\mu_{A \cap B}(x) = \min(\mu_A(x), \mu_B(x)), \forall x \in X \qquad (2.4)$$

либо

$$\mu_{A \cap B}(x) = \mu_A(x) * \mu_B(x), \forall x \in X. \qquad (2.5)$$

3. Объединением двух нечетких множеств $A, B \subset X$ называется нечеткое множество $A \cup B$, функция принадлежности которого

$$\mu_{A \cup B}(x) = \max(\mu_A(x), \mu_B(x)), \forall x \in X \qquad (2.6)$$

либо

$$\mu_{A \cup B}(x) = \begin{cases} \mu_A(x) + \mu_B(x) < 1, \\ 1, \mu_A(x) + \mu_B(x) \ge 1. \end{cases} \ \forall x \in X \qquad (2.7)$$

4. Концентрацией нечеткого множества (2.1) называется нечеткое множество

$$A^{(n)} = \{\mu_A^n(x)/x\}, n - \text{целое}, n > 1, \qquad (2.8)$$

если $n < 1$, то эта операция называется размытием множества.

5. α-срезом (множеством уровня α) нечеткого множества $A \subset X$ называется четкое множество $A_\alpha \subset X$ такое, что

$$A_\alpha = \{x_i\},\ \forall \mu_A(x_i) \geq \alpha,\ \alpha \in [0,1],\ \forall x \in X. \qquad (2.9)$$

Примеры. Пусть $X = \{1, 2, ..., 10\}$,

A = «малые числа» = 1/1 + 1/2 + 0,8/3 + 0,5/4 + 0,3/5 + 0,1/6;

B = «большие числа» = 0,1/5 + 0,2/6 + 0,5/7 + 0,8/8 +1/9+1/10.

Тогда

$\overline{A}$ = «НЕ малые числа» = 0,2/3 + 0,5/4 + 0,7/5 + 0,9/6 + 1/7 + 1/8 +1/9 + 1/10;

$A \cap B$ = «малые числа» И «большие числа» = 0,1/5 + 0,1/6 (0,03/5 + 0,01/6);

$A \cup B$ = «малые числа» ИЛИ «большие числа» = 1/1 + 1/2 + 0,8/3 + + 0,5/4 + 0,3/5 + 0,2/6 + 0,5/7 + 0,8/8 + 1/9 + 1/10 (1/1 + 1/2 + 0,8/3 + + 0,5/4 + 0,4/5 + 0,3/6 + 0,5/7 + 0,8/8 + 1/9 + 1/10).

Если A = 1/1 + 0,8/2 + 0,5/3 + 0,1/4, то $A^{(2)}$ = 1/1 + 0,64/2 + 0,25/3 + + 0,01/4. $A_{0,1} = \{1, 2, 3, 4\}$, $A_{0,5} = \{1, 2, 3\}$, $A_1 = \{1\}$.

Законы. 1. Коммутативный: $A \cap B = B \cap A$; $A \cup B = B \cup A$.

2. Ассоциативный:

$A \cap (B \cap C) = (A \cap B) \cap C$; $A \cup (B \cup C) = (A \cup B) \cup C$.

3. Дистрибутивный:

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

4. Поглощение: $A \cap (A \cup B) = A$.

5. Теорема Моргана: $\overline{A \cup B} = \overline{A} \cap \overline{B}$; $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Отличие от законов теории четких множеств проявляется в том, что $A \cup \overline{A} \neq U$; $A \cap \overline{A} \neq \varnothing$.

Отображение множеств. Пусть функция f представляет собой отображение $f: X \to Y$ и A есть нечеткое множество в X. Тогда функция f отображает нечеткое множество A в нечеткое множество $B \subset Y$ такое, что

$$\mu_B(y) = \begin{cases} \mu_A(x),\ f(x) \in Y, \\ 0,\ f(x) \notin Y. \end{cases} \qquad (2.10)$$

Пример. Пусть $X = \{1, 2, 3, 4\}$, $Y = \{1, 2, 3, 4, 5\}$ и $y = f(x) = x + 2$. Если $A = 0{,}1/1 + 0{,}2/2 + 0{,}7/3 + 1/4$, то $B = 0{,}1/3 + 0{,}2/4 + 0{,}7/5$.

Нечеткие отношения

Пусть $X = \{x_1, x_2, ..., x_n\}$ и $Y = \{y_1, y_2, ..., y_n\}$.

Нечетким отношением R называется нечеткое множество, определенное на декартовом произведении $X \times Y$, которому соответствует функция принадлежности $\mu_R : X \times Y \to [0,1]$.

Здесь $\mu_R(x, y)$ отражает силу зависимости между $x \in X$ и $y \in Y$.

Если $R \subset X \times Y$ и $S \subset Y \times Z$, то max-min композицией называется нечеткое множество $R \circ S$, определенное на $X \times Z$, функция принадлежности которого имеет вид

$$\mu_{R \circ S}(x, z) = \sup_{y \in Y} \left[\mu_R(x, y) \wedge \mu_S(y, z) \right].$$

Max-min композиция позволяет ответить на вопрос, какое нечеткое множество в Y следует поставить в соответствие нечеткому множеству $A' \subset X$, если известно, что нечеткое множество $B \subset Y$ соответствует нечеткому множеству $A \subset X$. Операция нахождения такого соответствия называется нечетким логическим выводом и выполняется следующим образом:

$$B' = A' \circ R = A' \circ (A \times B),$$

где R – нечеткое отношение,

$$R = A \times B = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} \{ \mu_A(x_i) \wedge \mu_B(y_j) \} / (x_i, y_j); \qquad (2.11)$$

$\circ$ – max-min композиция, в соответствии с которой

$$B' = A' \circ R = \bigcup_{j=1}^{m} \bigvee_{i=1,n} \{ \mu_{A'}(x_i) \wedge \mu_R(x_i, y_j) \} / y_j . \qquad (2.12)$$

Пример. Даны универсальные множества $X = \{6, 7, 8, 9, 10, 11, 12\}$, $Y = \{8, 9, 10, 11\}$.

Нечеткие множества $A, A' \subset X$, $B, B' \subset Y$.

$A = 0{,}12/6 + 0{,}24/7 + 0{,}36/8 + 0{,}12/9$,

$B = 0{,}20/8 + 0{,}15/9 + 0{,}50/10$,

$A' = 0{,}05/6 + 0{,}15/7 + 0{,}20/8 + 0{,}25/9$.

Необходимо найти множество $B' \subset Y$, подобное множеству $A' \subset X$ в той же степени, как B подобно A.

Решение

R = 0,12/(6, 8) + 0,12/(6, 9) + 0,12/(6, 10) + 0,20/(7, 8) + 0,15/(7, 9) + + 0,24/(7, 10) + 0,20/(8, 8) + 0,15/(8, 9) + 0,36/(8, 10) + 0,12/(9, 8) + + 0,12/(9, 9) + 0,12/(9, 10).

B' = 0,20/8 + 0,15/9 + 0,20/10.

Графическое представление нечетких множеств A, B, A', B' дано на рис. 2.2.

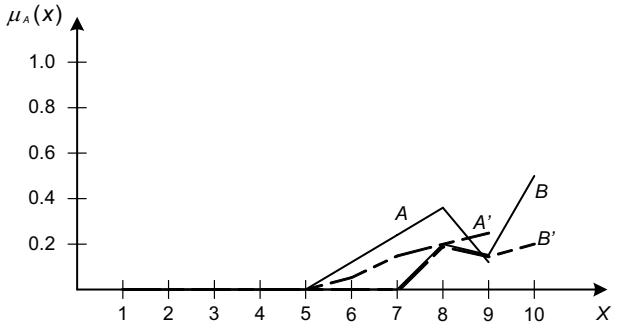


Рис. 2.2. Подобные нечеткие множества

Нечеткие числа

Нечеткое число – это нечеткое множество A, определенное на множестве X, если его функция принадлежности соответствует условиям:

$$\begin{cases} \max\limits_{x\in X} \mu_A(x) = 1, \\ x \le y \le z \Rightarrow \mu_A(y) \ge \min\left(\mu_A(x), \mu_A(z) \right). \end{cases} \qquad (2.13)$$

Качественному описанию параметра ИС, имеющего числовое значение, которое может находиться в некоторых пределах, соответствует один из нескольких видов функции принадлежности нечеткого числа: треугольный (рис. 2.3, *а*), трапециевидный (рис. 2.3, *б*), нормальный (рис. 2.3, *в*). Функция принадлежности, в свою очередь, может быть симметричной или несимметричной (см. рис. 2.3).

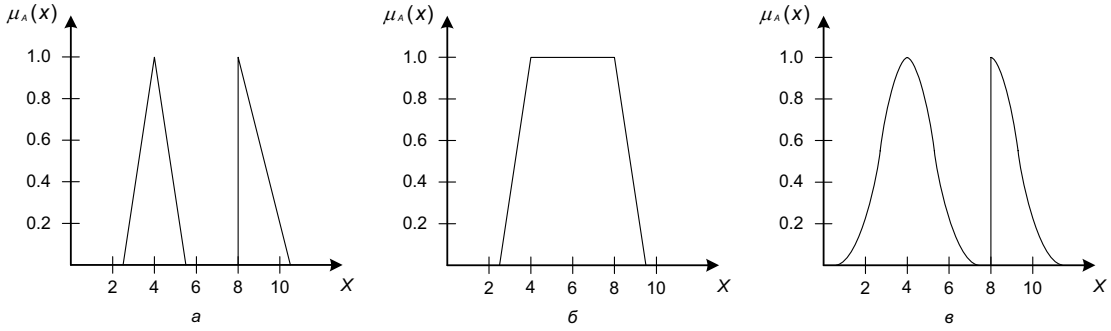


Рис. 2.3. Формы функций принадлежности нечетких чисел

На рис. 2.3, *а* показаны функции принадлежности двух нечетких чисел, соответствующих описаниям «около 4» и «чуть больше 8».

Трапециевидная форма (см. рис. 2.3, *б*) соответствует описанию «значение параметра примерно от 4 до 8».

Нормальный вид функции принадлежности (см. рис. 2.3, *в*) показывает, что адекватность описанию резко снижается по мере удаления значения параметра от наиболее подходящего, но при этом сохраняется минимальная адекватность и при больших отличиях.

Рассмотренные формы функций принадлежности наиболее распространены, но возможны и другие их виды.

2.2. Нечеткие меры

Мера энтропии нечетких множеств

Нечеткие множества используют для описания плохо определенных, неоднозначно понимаемых ситуаций, объектов, понятий. Существует общий показатель этой неопределенности или неоднозначности, называемый мерой энтропии (или показателем размытости) нечетких множеств. Он аналогичен энтропии в теории информации. В настоящее время существуют различные альтернативные подходы к определению меры энтропии нечеткого множества.

Меру энтропии можно рассматривать с двух сторон: во-первых, как показатель внутренней неопределенности, двусмысленности, противоречивости, обусловленных неполной, частичной, принадлежностью объектов множеству; во-вторых, как меру отличия нечеткого множества от четкого.

Аксиоматический подход к определению меры энтропии. Показатель размытости нечеткого множества можно определить как меру двусмысленности объектов множества X по отношению к некоторому свойству A, характеризующему эти объекты и определяющему в X нечеткое множество объектов A. Если некоторый объект $x \in X$ обладает свойством A, но лишь в частичной мере: $0 \le \mu_A(x) \le 1$, то неопределенность, двусмысленность, объекта x по отношению к свойству A проявляется в том, что он, хотя и в разной степени, принадлежит сразу двум противоположным классам: классу объектов, «обладающих свойством A», и классу объектов, «не обладающих свойством A».

Эта неопределенность максимальна, когда степени принадлежности объекта x к обоим классам равны, т.е. $\mu_A(x) = \mu_{\bar{A}}(x) = 0{,}5$. И, наобо-

рот, минимальна, когда объект принадлежит только к одному из этих классов, т.е. либо $\mu_A(x)=1,\quad \mu_{\bar{A}}(x)=0$, либо $\mu_A(x)=0,\quad \mu_{\bar{A}}(x)=1$.

Таким образом, меру энтропии нечеткого множества A можно определить в виде функции d, удовлетворяющей следующим условиям:

1) $d(A)=d(B)$, если $\mu_A(x)=\mu_B(x)$;

2) $d(A)<d(B)$, если $\mu_A(x)<\mu_B(x)$ при $\mu_B(x)<0{,}5$,

если $\mu_A(x)>\mu_B(x)$ при $\mu_B(x)>0{,}5$,

$\mu_A(x)\in[0,\ 0{,}5)\cup(0{,}5,\ 1]$ при $\mu_B(x)=0{,}5$;

3) $d(A)=d(\bar{A})$;

4) если $A\cap B=\varnothing$, то $d(A\cup B)=d(A)+d(B)$.

Примером показателя размытости может служить логарифмическая энтропия нечетких множеств:

$$d(A)=\frac{1}{n}\sum_{i=1}^{n}S_i\left(\mu_A(x_i)\right), \tag{2.14}$$

где $\begin{cases}S(y)=-y\ln(y)-(1-y)\ln(1-y),\ y\in(0,\ 1),\\ 0,\ y=0 \text{ или } y=1\end{cases}$ – функция Шеннона.

Метрический подход к определению меры энтропии нечетких множеств. Меру энтропии нечетких множеств можно определить как меру отличия нечеткого множества от ближайшего к нему обычного множества.

Существует два способа: определение с помощью расстояния до максимального размытого множества $A_{0,5}$: $\forall x\in X,\ \mu_{A_{0,5}}(x)=0{,}5$ и расстояния между нечетким множеством и его дополнением.

Множеством, ближайшим к нечеткому множеству A, называется неразмытое множество $\underline{A}$ такое, что

$$\mu_{\underline{A}}(x)=\begin{cases}1,\ \text{если } \mu_A(x)>0{,}5,\\ 0,\ \text{если } \mu_A(x)\le 0{,}5.\end{cases} \tag{2.15}$$

Мерой энтропии называется функционал

$$d(A)=\frac{2}{n}\sum_{i=1}^{n}\left|\ \mu_A(x_i)-\mu_{\underline{A}}(x_i)\ \right|. \tag{2.16}$$

Из (2.16) следует, что

$d(A)_{\max}=1,\quad A=A_{0,5}$,

$d(A)_{\min}=0,\quad \forall x\in X,\ \mu_A(x)=\{0,1\}$.

Если вместо расстояния Хэмминга использовать евклидово расстояние, то получим

$$d(A) = \frac{2}{\sqrt{n}} \sqrt{\sum_{i=1}^{n} \left(\mu_A(x_i) - \mu_{\underline{A}}(x_i) \right)^2}. \qquad (2.17)$$

Меру энтропии можно задать и с помощью расстояния между нечетким множеством и его дополнением:

$$d(A) = \frac{1}{n} \sum_{i=1}^{n} \left(1 - \left| \mu_A(x_i) - \mu_{\overline{A}}(x_i) \right| \right) = \frac{1}{n} \sum_{i=1}^{n} \left(1 - \left| 2\mu_A(x_i) - 1 \right| \right). \qquad (2.18)$$

Для евклидова расстояния

$$d(A) = \frac{1}{\sqrt{n}} \sqrt{\sum_{i=1}^{n} \left(1 - \left| \mu_A(x_i) - \mu_{\underline{A}}(x_i) \right| \right)^2} = \frac{1}{\sqrt{n}} \sqrt{\sum_{i=1}^{n} \left(1 - \left| 2\mu_A(x_i) - 1 \right| \right)^2}. \qquad (2.19)$$

Значения энтропии по формулам (2.16) и (2.18), (2.17) и (2.19) совпадают.

В табл. 2.1 приведены диапазоны значений меры энтропии в трех вариантах для нечетких множеств в диапазонах случайного распределения значений функций принадлежности элементов.

Таблица 2.1

Диапазоны значений меры энтропии

Диапазон $\mu_A(x_i)$	$d(A)_{\text{логарифм}}$	$d(A)_{\text{хемм}}$	$d(A)_{\text{евклид}}$
[0,4; 0,6]	0,68 – 0,69	0,87 – 0,93	0,88 – 0,94
[0,6; 0,8] или [0,2; 0,4]	0,58 – 0,62	0,56 – 0,64	0,57 – 0,65
[0,8; 1,0] или [0,0; 0,2]	0,25 – 0,35	0,16 – 0,24	0,19 – 0,27
[0,3; 0,7]	0,65 – 0,67	0,75 – 0,84	0,76 – 0,85
[0,6; 1,0] или [0,0; 0,4]	0,35 – 0,53	0,29 – 0,50	0,37 – 0,54

Мера внутренней неопределенности

Мера внутренней неопределенности показывает внутреннюю противоречивость элементов нечеткого множества. Если некоторое высказывание A представляется нечетким множеством, то данная мера показывает, что степень доверия высказыванию A, которое истинно, не обязательно равна единице. Это также означает, что сумма степеней доверия высказыванию A и его отрицанию $\overline{A}$ также не обязательно равна единице, а может быть либо равной единице, либо меньше её.

Тогда эта мера называется функцией доверия. Она определяет степень $D \in [0,1]$ истинности высказывания A. Существует два способа (аналогично (2.16) и (2.17)):

$$1)\ D(A) = 1 - \frac{2}{n}\sum_{i=1}^{n}\left| \mu_A(x_i) - \mu_A^{CP} \right|; \tag{2.20}$$

$$2)\ D(A) = 1 - \frac{2}{\sqrt{n}}\sqrt{\sum_{i=1}^{n}\left(\mu_A(x_i) - \mu_A^{CP}\right)^2}, \tag{2.21}$$

где $\mu_A^{CP} = \frac{|A|}{n} = \frac{1}{n}\sum_{i=1}^{n}\mu_A(x_i)$, (2.22)

где n – число элементов множества A.

В табл. 2.2 приведены диапазоны значений функции доверия для нечетких множеств с типовыми формами функций принадлежности элементов.

Таблица 2.2

Диапазоны значений функции доверия

Форма функции принадлежности	Параметры		$D(A)_{\text{хемм}}$	$D(A)_{\text{евклид}}$
Случайное распределение	диапазон [0,4; 0,6] 20 %		0,89 – 0,92	0,87 – 0,90
	диапазон [0,3; 0,7] 40 %		0,77 – 0,84	0,74 – 0,80
	диапазон [0,1; 0,9] 80 %		0,53 – 0,66	0,48 – 0,60
	диапазон [0,0; 1,0] 100 %		0,41 – 0,57	0,35 – 0,48
Треугольная форма	$\mu_{\max} = 0{,}2$		0,90	0,88
	$\mu_{\max} = 0{,}5$		0,75	0,71
	$\mu_{\max} = 0{,}7$		0,65	0,59
	$\mu_{\max} = 1{,}0$		0,50	0,42
Трапециевидная форма	$\mu_{\max}$	длина горизонтального участка, %		
	0,2	80 %	0,93	0,90
		60 %	0,92	0,90
		20 %	0,91	0,89
	0,5	80 %	0,83	0,75
		60 %	0,82	0,74
		20 %	0,76	0,72
	0,7	80 %	0,76	0,65
		60 %	0,73	0,64
		20 %	0,68	0,62
	1,0	80 %	0,65	0,49
		60 %	0,57	0,47
		20 %	0,52	0,44

Распределение значений функции принадлежности элементов было взято для полного набора значений $X = \{ x_1, x_2, ..., x_n \}$. При сокращении числа ненулевых значений x_i (например когда треугольная или трапециевидная форма стремятся к виду, представленному на рис. 2.3, *а, б*) значение функции доверия значительно возрастает, но если оно остается меньше 0,5, то описание, представленное такой функцией принадлежности, неадекватно и не может рассматриваться как достаточно истинное.

Мера вероятности

Введем дополнительную функцию $v_A(x_i) \in [0,1],\ \forall i = \overline{1,n}$, отражающую степень доверия функции принадлежности нечеткого множества для каждого элемента. Мера вероятности показывает среднее значение функции принадлежности при стремлении степени доверия каждому элементу к максимальной:

$$p(A) = \frac{1}{n} \sum_{i=1}^{n} \lim_{v_A(x_i) \to v_{\max}} \mu_A(x_i). \tag{2.23}$$

Учитывая взаимосвязь значений функции принадлежности для отдельных элементов, меру вероятности можно считать средним значением композиции функции принадлежности и функции распределения доверия ей:

$$p(A) = \frac{2(n-2)!}{n!} \sum_{i=1}^{n-1} \sum_{j=i}^{n} (\mu_i, \mu_j) \times (v_i, v_j). \tag{2.24}$$

Композиция лежит в диапазоне $[0,1]$:

$$(\mu_i, \mu_j) \times (v_i, v_j) = \begin{cases} h_{ij}, & 0 < h_{ij} < 1, \\ 0, & h_{ij} \le 0, \\ 1, & h_{ij} \ge 1 \end{cases} \tag{2.25}$$

и равна

$$h_{ij} = \frac{v_{\max} - v_i}{v_i - v_j} (\mu_i - \mu_j) + \mu_i. \tag{2.26}$$

Краткие выводы

Для математического представления описаний качественных параметров ИС может быть использована теория нечетких множеств. Значения таких параметров, как «криптостойкость замка двери в за-

щищаемом помещении», «значимость некоторой уязвимости», «использование данной уязвимости злоумышленником требует специальных средств», «потенциал нарушителя», «реализация данной угрозы наносит существенный вред организации», могут быть представлены нечетким множеством.

Нечеткое множество – это представление не только набора некоторых элементов, но и степеней их принадлежности множеству, т.е. соответствия описанию параметра.

Нечеткие множества по своим свойствам и математическому аппарату во многом похожи на четкие множества, отличие заключается в том, что элемент нечеткого множества может быть отнесен к таковому с некоторой долей уверенности, находящейся в диапазоне от 0 до 1. Эта степень не одно и то же, что вероятность отнесения элемента в ряде каких-либо опытов, так как при величине функции принадлежности больше нуля элемент безусловно входит в множество. Но при этом имеет как бы не полный вес или значимость.

Два нечетких множества могут находиться в некотором соответствии друг с другом, описываемом нечетким отношением, что позволяет найти подобные данному множества, если описаны отношения подобия.

Выпуклые функции принадлежности нечетких множеств соответствуют описанию нечеткого числа. Форма таких описаний различна. В задаче анализа качества СЗИ нечеткие числа используют для описания соответствия некоторого качественного параметра требованиям стандарта.

Нечеткие множества отличаются от четких, и это отличие описывается мерой энтропии. Она может быть определена различными способами: с помощью логарифмической меры, расстояния Хэмминга, евклидова расстояния. В большинстве видов распределения функций принадлежности нечетких множеств при одинаковом значении мера энтропии, определенная через евклидово расстояние, показывает меньшую размытость множества, а логарифмическая мера – большую.

Нечеткие множества, по своей сути, несут в себе также свойство внутренней неопределенности, т.е. имеют меру внутренней неопреде-

ленности. Если множество характеризует некоторое описание элемента СЗИ, то функция доверия, отражающая внутреннюю неопределенность множества, может служить показателем достоверности такого описания.

Если нечеткое число получено на основе экспертной оценки и определена степень доверия полученному значению каждого элемента нечеткого множества, то функция вероятности такого множества показывает наиболее возможное четкое значение исследуемого параметра.

Контрольные вопросы

1. Дайте определение нечеткого множества и приведите примеры описаний, представленных таким множеством.
2. Расскажите о свойствах нечеткого множества и поясните его отличие от четкого множества.
3. Какие операции применимы к нечеткому множеству и какой смысл они имеют?
4. Что такое отображение нечетких множеств?
5. Как получить нечеткое множество, подобное данному, если известно отношение подобия?
6. Что такое нечеткое число и какое нечеткое множество может служить представлением нечеткого числа?
7. Какие формы функций принадлежности нечетких чисел могут использоваться для отображения описаний количественных параметров ИС?
8. Что такое мера энтропии нечеткого множества и какие существуют подходы к ее определению?
9. Расскажите об аксиоматическом подходе к определению меры энтропии нечеткого множества.
10. Расскажите о метрическом подходе к определению меры энтропии нечеткого множества.
11. Проанализируйте значения меры энтропии из табл. 2.1.
12. Вычислите меру энтропии нечеткого множества с треугольной и трапециевидной формами функции принадлежности и параметрами, взятыми из табл. 2.2, при том, что ненулевые значения функции составляют 70 % от общего диапазона значений.

13. Вычислите меру энтропии нечеткого множества (см. вопрос 12), при том, что ненулевые значения функции составляют 50 % от общего диапазона значений.

14. Вычислите меру энтропии нечеткого множества (см. вопрос 12), при том, что ненулевые значения функции составляют 20 % от общего диапазона значений.

15. Что такое мера внутренней неопределенности нечеткого множества и как ее можно вычислить?

16. Рассчитайте функции доверия для нечетких множеств по условиям вопроса 12.

17. Рассчитайте функции доверия для нечетких множеств по условиям вопроса 13.

18. Рассчитайте функции доверия для нечетких множеств по условиям вопроса 14.

19. Что такое мера вероятности нечеткого множества, как ее можно вычислить и для чего использовать при анализе ИС?

Глава 3. АУДИТ СТЕПЕНИ СООТВЕТСТВИЯ ПАРАМЕТРОВ СЗИ ТРЕБОВАНИЯМ СТАНДАРТОВ БЕЗОПАСНОСТИ

3.1. Цели и задачи аудита СЗИ

Современные требования, предъявляемые к определению уровня обеспечения ИБ, и существенный рост рисков потерь (материальных, финансовых и др.) от нарушения ИБ диктуют необходимость использования обоснованных технико-экономических методов и средств, позволяющих количественно и качественно измерять уровень защищенности ИС. Одно из направлений обеспечения безопасности – аудит ИБ.

Основа аудита ИБ – установление степени соответствия применяемых в организации защитных мер выбранным критериям и анализ результативности системы управления ИБ при достижении конкретных целей.

Результаты аудита дают возможность идентифицировать уязвимости ИС организации, выявить неоцененные риски, определить соответствующие корректирующие и превентивные меры.

Анализ защищенности современных организаций от угроз информационной безопасности – работа сложная, многоплановая и трудоемкая.

Для ее качественного проведения необходимо знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, методологий оценки соответствия параметров СЗИ требованиям стандартов.

Аудит ИБ сегодня – один из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищённости предприятия от угроз информационной безопасности. Кроме того, результаты аудита – основа для формирования стратегии развития системы обеспечения информационной безопасности организации. В частности, результаты аудита могут служить

исходными данными для оценки качества СЗИ, в том числе ее экономической эффективности.

В широком смысле слова аудит – это систематический независимый документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных требований к СЗИ. Аудитор – это физическое лицо, отвечающее квалификационным требованиям, установленным уполномоченным федеральным органом, и имеющее квалификационный аттестат аудитора.

Существуют следующие разновидности аудита.

1. Аудит ИС – системный процесс получения и оценки объективных данных о текущем состоянии информационной системы, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенным критериям.

2. Аудит ИТ – это процесс установления степени выполнения требований по обеспечению состояния защищенности системы информационных технологий, позволяющий определить, обеспечиваются ли безопасность ресурсов компании, необходимые параметры целостности и доступности данных, достигаются ли цели предприятия в части эффективности информационных технологий.

3. Аудит ИБ – это процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с определенными критериями информационной безопасности.

Для объективной оценки состояния защищенности ИС организации процесс аудита должен проводиться независимыми от объекта аудита специалистами. Объективная оценка – это залог качества проводимой работы и один из основных принципов аудита ИБ.

Два других принципа проведения аудита ИБ выглядят следующим образом:

- полнота аудита ИБ. Аудит должен охватывать все области ИБ и защитные меры, используемые в СЗИ;
- необходимость понимания аудитором деятельности проверяемой организации, компетентность и этичность. Доверие процессу аудита зависит от компетентности тех, кто проводит аудит, и от этичности их поведения.

Цели аудита ИБ:

- удовлетворение потребности в оценке защищенности конфиденциальной информации, оценке полноты и качества выполнения требований по обеспечению ИБ и защите информации;
- оценка полноты и качества выполнения требований, предъявляемых к организации или системе информационных технологий при их сертификации на соответствие законодательным требованиям, стандартам по ИБ, нормативным документам;
- оценка результативности системы управления ИБ при достижении конкретных целей;
- определение областей совершенствования системы обеспечения ИБ организации и защиты конфиденциальной информации.

Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора оказываются задействованы представители большинства структурных подразделений компании. Действия всех участников этого процесса должны быть скоординированы, поэтому на этапе инициирования процедуры аудита должны быть решены различные организационные вопросы.

Этап сбора информации аудита – наиболее сложный и длительный. Это может быть связано с отсутствием необходимой документации на ИС и необходимостью плотного взаимодействия аудитора со многими должностными лицами организации.

Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

Методика аудита – это совокупность теоретических и практических способов проведения аудита, разработанных аудитором на базе стандартизированных правил и норм проведения аудита в предметной области и в определенной степени на основе личного профессионального опыта.

Аудиторский отчет – основной результат проведения аудита. Его качество характеризует качество работы аудитора. Отчет должен содержать описание целей проведения аудита, характеристику обследуемой ИС, границы проведения аудита и используемые методы, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности ИС, и, конечно, реко-

мендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

3.2. Нормативная база проведения аудита

В последнее время в разных странах появилось новое поколение стандартов информационной безопасности компьютерных ИС, посвященных практическим вопросам обеспечения и аудита ИБ. В соответствии с этими стандартами обеспечение ИБ в любой компании предполагает следующее: во-первых, определение целей обеспечения ИБ ИС; во-вторых, создание эффективной системы управления ИБ; в-третьих, расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности заявленным целям; в-четвертых, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния; в-пятых, использование методик (с обоснованной системой метрик и мер обеспечения ИБ) проведения аудита ИБ, позволяющих объективно оценить текущее состояние дел.

Прежде всего следует выделить международные и национальные стандарты оценки и управления информационной безопасностью: ISO 15408, ISO 17799-2005 (BS 7799-1), ISO 27001 (BS 7799-2); стандарты аудита информационных систем и информационной безопасности: COBIT, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им.

При проведении аудита ИБ компании наибольшую известность и распространение получили стандарты ISO 17799-2005 (BS 7799-1), ISO 27001 (BS 7799-2). В их основе лежит британский стандарт BS 7799-95, состоящий из двух частей: рекомендации и обязательные требования.

В 1999 г. по согласованию с Британским институтом стандартов был принят международный стандарт ISO/IEC 17799, базирующийся на британском стандарте BS 7799-1 (часть 1), а в 2005 г. – ISO/IEC 27001, отражающий BS 7799-2 (часть 2).

В настоящее время актуальны стандарты реализации 2005 г. В декабре 2005 г. появился также новый британский стандарт BS 7799-3:2005 «Information Security Management Systems. Guidelines for Information Security Risk Management» (Системы управления ИБ. Руководство по управлению рисками ИБ).

По своей сути, стандарт ISO/IEC 17799-2005 – это практическое руководство по созданию системы обеспечения ИБ организации, которое определяет 133 регулятора ИБ (меры, средства, механизмы, контрмеры), сгруппированные по 11 разделам. Поскольку он носит сугубо рекомендательный характер, экспертиза организаций по нему не предусматривается.

Сертификация производится на соответствие стандарту ISO/IEC 27001-2005, который определяет комплекс требований к СМИБ (вытекающих из стандарта ISO/IEC 17799) и формирует спецификации для создания, внедрения, эксплуатации, мониторинга, пересмотра, сопровождения и совершенствования СМИБ.

На данный момент стандарт ISO 27001 занимает лидирующие позиции в Европе и Азии, он стал стандартом де-факто при построении систем информационной безопасности.

Число компаний в мире, получивших официальный сертификат соответствия стандарту, – 3500. В России таких компаний 6.

В 1990 г. в Международной организацией стандартов (ISO) была начата работа по созданию международных критериев оценки безопасности компьютерных систем. Результатом явился стандарт «Общие критерии безопасности информационных технологий» (ОК), который на данный момент признается одним из наиболее функциональных стандартов в сфере ИБ. Его разработка велась совместными усилиями сертификационных центров США, Канады, Франции, Германии, Нидерландов и Великобритании. «Общие критерии» неоднократно редактировались. В результате 8 июня 1999 г. был утвержден Международный стандарт ISO/IEC 15408.

Общие критерии безопасности информационных технологий содержат в себе два типа требований безопасности – функциональные требования и требования гарантированности.

Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д. Требования гарантированности относятся к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

К настоящему времени аудиторскими компаниями образованы различные государственные и негосударственные ассоциации, объе-

диняющие профессионалов в области аудита информационных систем, которые занимаются созданием и сопровождением, как правило, закрытых, тщательно охраняемых от посторонних глаз стандартов и концепций аудиторской деятельности в области информационных технологий, таких как COBIT, SAC, COSO, SAS 55/78.

В Российской Федерации ситуация следующая. В 2006 г. вышел ГОСТ 17799, который представляет собой перевод стандарта ISO 17799-2000. В ближайшее время ожидается выход в свет ГОСТа 17799-2005 и ГОСТа 27001.

ГОСТ 27001 включает в себя возможные функциональные спецификации корпоративных систем управления ИБ с точки зрения их проверки на соответствие требованиям ГОСТ 17799. Положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ «АС. Защита от НСД к информации. Классификация АС и требования по защите информации» и «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации».

Однако в настоящее время описанные РД средства уже устарели и содержащаяся в них классификация АС, СВТ и МЭ не может признаваться состоятельной. Достаточно заметить, что классификация АС и СВТ разрабатывалась без учета распределенной (сетевой) природы современных АС, а все современные коммерческие МЭ по своим возможностям существенно превосходят требования 1-го класса защищенности (за исключением требования по использованию сертифицированных криптографических алгоритмов).

Развитие нормативной базы в этом направлении – разработка профилей защиты для различных классов СВТ, АС и МЭ на базе «Общих критериев». В настоящее время создано уже большое количество англоязычных профилей защиты. Значительные усилия в этом направлении предпринимаются и в России под эгидой Гостехкомиссии.

Проект РД Гостехкомиссии России «Специальные требования и рекомендации по защите конфиденциальной информации» (СТРК)

содержит достаточно полный набор требований и рекомендаций организационного уровня по защите речевой информации, информации, обрабатываемой средствами вычислительной техники, а также по защите информации при подключении к сетям общего пользования. В документе рассматриваются, в том числе, следующие вопросы:

- защита информации на рабочих местах на базе автономных ПЭВМ;
- защита информации при использовании съемных накопителей большой емкости для автоматизированных рабочих мест на базе автономных ПЭВМ;
- защита информации в локальных вычислительных сетях;
- защита информации при межсетевом взаимодействии;
- защита информации при работе с СУБД.

СТРК может использоваться при проведении аудита и аттестации безопасности АС для оценки полноты и правильности реализации организационных мер защиты информации в АС. Аттестация АС и сертификация СВТ по требованиям безопасности информации, аудит и обследование безопасности в отдельных случаях предполагают использование помимо перечисленных и других нормативных документов.

3.3. Алгоритм проведения аудита ИБ

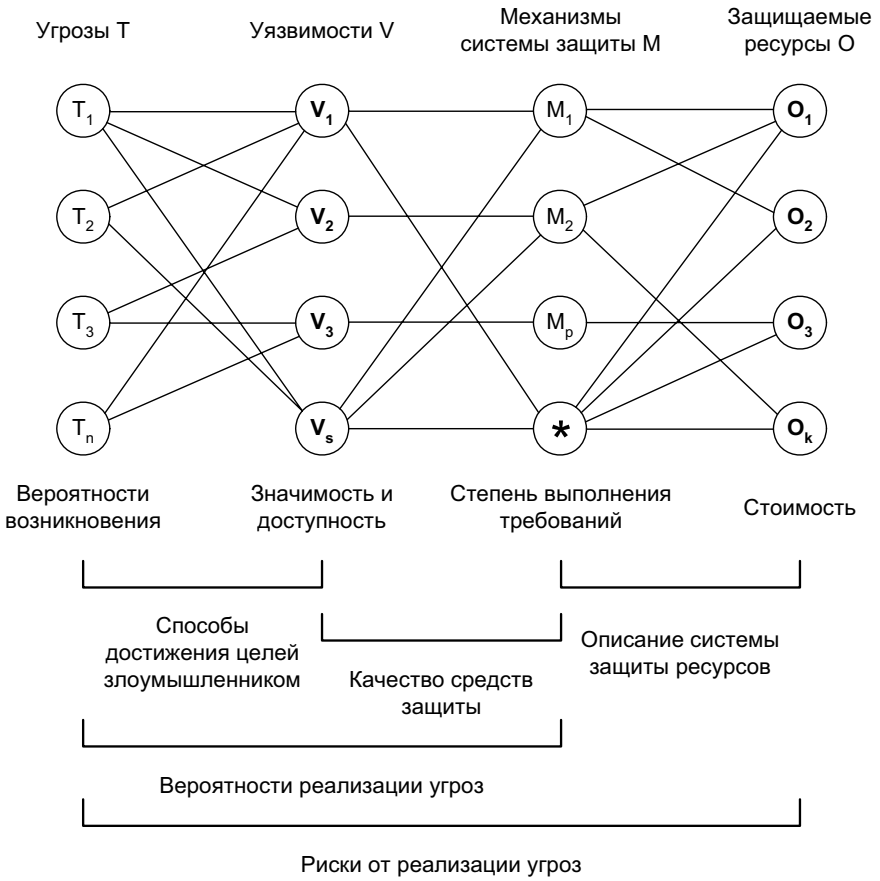
Параметры ИС и показатели СЗИ, исследуемые аудитором

Стандарты ИБ определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут указывать разные наборы требований безопасности в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация, государственное учреждение), а также назначения (финансы, промышленность, связь и т.п.). Аудитору необходимо правильно определить набор требований стандарта, соответствие которым должно обеспечиваться в данной ИС.

В процессе аудита проводится исследование ИС организации в соответствии с формальной моделью, представленной на рисунке.

В данной модели область угроз T представляет собой список всех возможных угроз для данной информационной системы, причем

каждой угрозе присваивается вероятность ее возникновения в результате подробного изучения обстановки вокруг деятельности организации (географическое расположение, состояние основных фондов, наличие конкурентов, недоброжелателей и т.д.).



Модель взаимосвязи параметров ИС и показателей качества СЗИ

Множество уязвимостей *V* представляет собой перечень всех существующих уязвимостей в данной ИС, основные характеристики которых – значимость и доступность для злоумышленника. В совокупности множества угроз и уязвимостей и их взаимосвязи образуют перечень способов достижения цели – воздействие на защищаемые ресурсы.

Система защиты *M* представляет собой имеющийся в организации набор средств защиты информации, характеризующихся степенью выполнения требований стандартов безопасности. Качество средств защиты определяется при рассмотрении множества *V* – множества уязвимостей ИС и множества *M* – системы защиты с их взаимосвязями, при этом ведется расчет возможности преодоления каждого барьера, ассоциированного с каждой уязвимостью. Здесь искусст-

венно добавлен элемент (*), показывающий, что использование ряда уязвимостей может быть вообще не перекрыто каким-либо барьером.

Защищаемая область *O* представляет собой совокупность защищаемых ресурсов, основная характеристика которых – их стоимость, определяемая исходя из финансовых потерь организации, ассоциированных с восстановлением ресурса либо с упущенной выгодой, связанной с уничтожением, тиражированием либо блокированием доступа к защищаемому ресурсу.

Вместе множество *M*, множество *O* и их взаимосвязи дают полное описание системы защиты ресурсов организации.

Вероятности реализации угроз ИС организации выделяются из совокупности определенных ранее способов достижения целей и качества средств защиты. Здесь подробно рассматриваются взаимосвязи всех существующих угроз ИБ и уязвимостей ИС, а также уязвимостей ИС и защитных средств.

В целом риск от реализации существующих угроз ИБ организации определяется при подробном рассмотрении всех областей графа (см. рисунок), т.е. показателей вероятности реализации каждой угрозы и описания системы защиты ресурсов.

Определение полного множества угроз ИБ предприятия

В большинстве коммерческих предприятий угрозы ИБ однотипны. Ниже приведены наиболее распространенные угрозы.

Угрозы конфиденциальности:

- разглашение информации о клиентах или технологии производства;
- получение доступа к конфиденциальной информации путем взлома криптографической защиты;
- утечка информации по акустическим и виброакустическим каналам;
- утечка информации по электрическим каналам;
- утечка информации по каналам ПЭМИН;
- утечка информации в процессе передачи по линиям связи;
- утечка информации по линиям электропитания и заземления;
- установка ТСР в защищаемом помещении;
- кража, дублирование данных, содержащих коммерческую тайну с носителей информации;

- перехват конфиденциальной информации, циркулирующей в локальной сети;
- получение информации вследствие негарантированного уничтожения «мусора».

Угрозы целостности:

- ввод сотрудниками неверных данных или намеренное искажение информации;
- нарушение целостности данных в БД;
- подмена информации на съемных носителях;
- потеря информации в результате отключения электропитания;
- потеря информации в результате пожара и других ЧС;
- невозможность восстановления при отсутствии резервных копий критически важной информации;
- нарушение целостности программной среды, в том числе изменение настроек ПО.

Угрозы доступности:

- потеря или кража информации на резервных носителях;
- саботирование рабочего процесса;
- физическая порча оборудования, в частности серверов;
- вывод из строя линий связи;
- нарушение адресности и своевременности информационного обмена;
- нарушение передачи информации между филиалами организации;
- нарушение работы СКУД.

Часть угроз имеет отношение к нарушению двух из трех или всех трех защищаемых качеств информации и ИС:

- возникновение техногенных аварий;
- проникновение посторонних в защищаемое помещение;
- НСД путем использования чужих атрибутов разграничения доступа;
- злоупотребление полномочиями;
- несанкционированный доступ к информации сотрудниками предприятия;
- нецелевое использование программно-аппаратных средств сотрудниками организации;
- внедрение в ИС различных вредоносных программ и заражение компьютерными вирусами;

- НСД к ресурсам операционной системы;
- технические сбои в работе систем сигнализации и охраны;
- порча оборудования ТСО.

Выделение наиболее значимых уязвимостей ИС

Любая ИС имеет множество уязвимостей, общее количество которых может составлять сотни и тысячи, но при этом некоторые из них настолько специфичны, что неизвестны большинству внешних злоумышленников. Уязвимости ИС можно условно разделить на три направления: физические, программные и информационные.

Типовые физические уязвимости:

- отсутствие или низкое качество ограждения и контроля за территорией предприятия;
- отсутствие или недоработки в системе контроля экологически вредных производств;
- отсутствие физической защиты окон в выделенном помещении или неправильная установка решеток на окнах;
- слабая техническая укрепленность дверей выделенного помещения;
- отсутствие пропусков у сотрудников организации;
- отсутствие или недостаточное количество источников бесперебойного питания, электрогенераторов;
- неукомплектованность охраны, в том числе средствами активной обороны;
- отсутствие охранной сигнализации в выделенном помещении;
- отсутствие пожарной сигнализации;
- отсутствие или недостатки в системе видеонаблюдения;
- отсутствие средств защиты от утечки по различным ТКУИ;
- отсутствие автоматизированной СКУД;
- отсутствие выделенного помещения для сервера или физической защиты сервера;
- наличие физической связи локальной сети и компьютеров, обрабатывающих конфиденциальную информацию, с внешней средой;
- недоработки или простота аутентификационного механизма.

Типовые программные уязвимости:

- отсутствие или недостаточное использование криптографической защиты информации;

- отсутствие системы резервирования данных;
- отсутствие или ограниченность аудита событий в КС;
- отсутствие или недостатки системы разграничения доступа пользователей;
- неорганизованность работы с паролями;
- отсутствие контроля доступа к ПО;
- отсутствие или недостатки в работе программных МЭ;
- редкое обновление антивирусных баз;
- использование нелицензионного ПО;
- отсутствие контроля целостности файлов прикладных программ.

Типовые организационные уязвимости:

- отсутствие аттестованных АРМ и выделенных помещений;
- отсутствие на предприятии или неадекватность КИБ;
- отсутствие инструкций работы пользователей с конфиденциальной информацией и неопределенность в отношении ответственности за нарушение требований ИБ;
- неукомплектованность штата сотрудников службы безопасности;
- отсутствие учета съемных носителей информации;
- отсутствие специального хранилища носителей информации;
- отсутствие аппаратных средств ЗИ.

На конкретном предприятии могут встречаться различные особенности перечисленных уязвимостей, а также могут быть и другие уязвимости.

Краткие выводы

Основа аудита ИБ – установление степени соответствия применяемых в организации защитных мер выбранным критериям и анализ результативности системы управления ИБ при достижении конкретных целей.

Аудит информационной безопасности сегодня – один из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищённости предприятия от угроз информационной безопасности.

Для объективной оценки состояния защищенности ИС организации аудит должен проводиться независимыми от объекта аудита

специалистами. Результаты аудита могут служить исходными данными для оценки качества СЗИ, в том числе ее экономической эффективности.

Методика аудита – это совокупность теоретических и практических способов проведения аудита, разработанных аудитором на базе стандартизированных правил и норм проведения аудита в предметной области и в определенной степени на основе личного профессионального опыта.

Аудит проводится на основе международных и российских стандартов и других нормативных документов. Стандарты ИБ определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Аудитору необходимо правильно указать набор требований стандарта, соответствие которым должно обеспечиваться в данной ИС.

В процессе аудита проводится исследование ИС организации в соответствии с формальной моделью, включающее в себя анализ угроз ИБ предприятия, уязвимостей ИС и степени исполнения требований ИБ. Для большинства коммерческих предприятий характерны однотипные угрозы ИБ, хотя количество и характер уязвимостей достаточно индивидуальны.

Контрольные вопросы

1. Что такое аудит ИБ?
2. Какие существуют разновидности аудита?
3. Что является целями аудита ИБ?
4. Что такое методика аудита ИБ?
5. Перечислите международные стандарты оценки и управления ИБ и укажите их особенности.
6. Перечислите российские стандарты и другие нормативные документы оценки и управления ИБ и укажите их особенности.
7. Расскажите о взаимосвязи параметров ИС и показателей качества СЗИ, исследуемой в процессе проведения аудита.
8. Классифицируйте и перечислите основные угрозы ИБ для типового коммерческого предприятия.
9. Классифицируйте и назовите наиболее распространенные уязвимости ИС коммерческих предприятий.

Глава 4. МЕТОДИКА ОЦЕНКИ ПОКАЗАТЕЛЕЙ КАЧЕСТВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

4.1. Экономическая модель ИС предприятия

Пусть существует конечное множество угроз безопасности, которые характеризуются вероятностями возникновения p_i^B и ущербом, наносимым предприятию u_i, где $i = \overline{1, n}$.

СЗИ выполняет функцию полной или частичной компенсации угроз для ИС. Основная характеристика средства защиты – вероятность устранения каждой *i*-й угрозы $p_i^У$, которая связана с вероятностью реализации угрозы p_i^P через соотношение

$$p_i^У = 1 - p_i^P . \tag{4.1}$$

Ущерб, нанесенный незащищенной системе, может быть представлен как суммарный по каждой угрозе:

$$U = \sum_{i=1}^{n} u_i . \tag{4.2}$$

Остаточный ущерб также представляет собой сумму потерь от всех угроз:

$$W = \sum_{i=1}^{n} w_i . \tag{4.3}$$

Риск для незащищенной системы представляет собой функцию вероятностей возникновения угроз и ущерба в случае их реализации:

$$R^{НЗ} = f\left(p_i^B, u_i \right) = \sum_{i=1}^{n} p_i^B u_i , \tag{4.4}$$

а риск для защищенной системы зависит также и от вероятностей их устранения:

$$R^{ЗАЩ} = f\left(p_i^B, u_i, p_i^У \right) = \sum_{i=1}^{n} p_i^B u_i \left(1 - p_i^У \right). \tag{4.5}$$

Учитывая вероятностный характер угроз, можно заменить предотвращенный ущерб $\Delta W = U - W$ на устраненный риск $\Delta R = R^{НЗ} - R^{ЗАЩ}$. Тогда

экономическая эффективность функционирования СЗИ может быть определена как

$$Ef = \frac{R^{НЗ} - R^{ЗАЩ}}{S_{СЗИ}} = \frac{\sum_{i=1}^{n} p_i^B u_i - \sum_{i=1}^{n} p_i^B u_i \left(1 - p_i^У\right)}{S_{СЗИ}}. \quad (4.6)$$

Коэффициент защищенности определяется по формуле

$$K_{ЗАЩ} = 1 - \frac{R^{ЗАЩ}}{R^{НЗ}} = 1 - \frac{\sum_{i=1}^{n} p_i^B u_i \left(1 - p_i^У\right)}{\sum_{i=1}^{n} p_i^B u_i}. \quad (4.7)$$

Для расчета экономической эффективности и коэффициента защищенности необходимо провести экспертизу таких параметров ИС, как значимость и доступность уязвимостей, степень воздействия каждой угрозы на ИС, а также определить список защищаемых ресурсов и их стоимость. Экспертиза параметров ИС неразрывно связана с аудитом ИБ, который предполагает определение полного списка актуальных угроз и уязвимостей, а также оценку степени выполнения количественных и качественных требований к СЗИ.

В процессе проведения такого исследования также уточняются коэффициенты авторитета экспертов и дается общая оценка адекватности всей экспертизы. Если экспертиза проводится не ЭГ, а одним экспертом, то дать оценку ее адекватности невозможно.

4.2. Вероятности возникновения угроз безопасности

Вероятности возникновения угроз безопасности зависят от коэффициентов значимости уязвимостей и показателей их доступности.

Значимость уязвимостей определяется матрицей парных сравнений в соответствии табл. 1.2:

$$M_j^Г = \begin{vmatrix} \gamma_{11}^j & \gamma_{12}^j & \cdots & \gamma_{1s}^j \\ \gamma_{21}^j & \gamma_{22}^j & \cdots & \gamma_{2s}^j \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_{s1}^j & \gamma_{s2}^j & \cdots & \gamma_{ss}^j \end{vmatrix}. \quad (4.8)$$

Матрица (4.8) удовлетворяет выражениям (1.3) – (1.5).

Вектор показателей доступности определяется по табл. 1.3:

$$D_j = \left(d_1^j, d_2^j, ..., d_s^j\right). \quad (4.9)$$

Взаимосвязь между угрозами и уязвимостями определяется матрицами причинно-следственных связей:

$$M_j^{ПСС} = \begin{vmatrix} \rho_{11}^j & \rho_{12}^j & \dots & \rho_{1s}^j \\ \rho_{21}^j & \rho_{22}^j & \dots & \rho_{2s}^j \\ \dots & \dots & \dots & \dots \\ \rho_{n1}^j & \rho_{n2}^j & \dots & \rho_{ns}^j \end{vmatrix}, \quad (4.10)$$

где $\rho_{ik}^j = 1$ указывает на то, что k-я уязвимость может быть причиной появления i-й угрозы по мнению j-го эксперта, $\rho_{ik}^j = 0$ указывает соответственно на то, что не может.

Умножая матрицу (4.10) размерностью $n \times s$ на матрицу (4.8) размерностью $s \times s$, получим матрицу размерностью $n \times s$ показателей значимости уязвимостей для возникновения угроз:

$$M_j^{ПЗ} = M_j^{ПСС} \times M_j^{Г} = \begin{vmatrix} \omega_{11}^j & \omega_{12}^j & \dots & \omega_{1s}^j \\ \omega_{21}^j & \omega_{22}^j & \dots & \omega_{2s}^j \\ \dots & \dots & \dots & \dots \\ \omega_{n1}^j & \omega_{n2}^j & \dots & \omega_{ns}^j \end{vmatrix}. \quad (4.11)$$

Величина ω_{ik}^j показывает степень влияния k-й уязвимости на появление i-й угрозы. Величины ω_{ik}^j, $\forall i = \overline{1, n}$, $k = \overline{1, s}$, не нормализованы, но при этом максимальное значение такой величины показывает максимальную степень влияния.

Матрица (4.11) дополняется вектором (4.9):

$$\begin{vmatrix} 10 - d_1 & 10 - d_2 & \dots & 10 - d_s \\ \omega_{11}^j & \omega_{12}^j & \dots & \omega_{1s}^j \\ \omega_{21}^j & \omega_{22}^j & \dots & \omega_{2s}^j \\ \dots & \dots & \dots & \dots \\ \omega_{n1}^j & \omega_{n2}^j & \dots & \omega_{ns}^j \end{vmatrix}. \quad (4.12)$$

Нулевая строка данной матрицы показывает влияние уязвимостей на возникновение в любой момент времени ситуации, когда нет никаких угроз.

Далее необходимо определить интегральный показатель влияния всех уязвимостей на возникновения i-й угрозы:

$$\omega_i^j = \sum_{k=1}^{s} \omega_{ik}^j, \ \forall i = \overline{0, n}. \quad (4.13)$$

Нормализация вектора $\Omega_j = \left(\omega_0^j, \omega_1^j, ..., \omega_n^j \right)$ должна быть проведена так, чтобы максимальному значению ω_i^j соответствовала величина 9, а минимальному – 1:

$$\overline{\omega}_i^j = 8 \frac{\omega_i^j - \min\limits_{i=0,...,n} \omega_i^j}{\max\limits_{i=0,...,n} \omega_i^j - \min\limits_{i=0,...,n} \omega_i^j} + 1. \qquad (4.14)$$

Далее необходимо получить матрицу отношений элементов:

$$M_j^{\Omega} = \begin{vmatrix} 1 & \frac{1}{\omega_{21}^j} & ... & \frac{1}{\omega_{n1}^j} \\ \omega_{21}^j & 1 & ... & \frac{1}{\omega_{n2}^j} \\ ... & ... & ... & ... \\ \omega_{n1}^j & \omega_{n2}^j & ... & 1 \end{vmatrix}, \qquad (4.15)$$

используя преобразование вида

$$\omega_{ab}^j = \frac{\overline{\omega}_a^j}{\overline{\omega}_b^j}, \quad \forall a,b \in \overline{0,n} \ . \qquad (4.16)$$

Задача нахождения вероятностей возникновения угроз безопасности по оценкам j-го эксперта p_{ij}^B сводится к задаче нахождения собственных чисел матрицы (4.15) и собственного вектора $P_j^B = \left\{ p_{ij}^B \right\}$, $i = \overline{0,n}$, соответствующего максимальному собственному значению, с использованием формул (1.9) – (1.12).

Так как матрица (4.15) согласованная (из-за преобразований (4.16)), то ее максимальное собственное число всегда равно размерности $(n+1)$.

4.3. Ущерб от реализации угроз безопасности

Ущерб, наносимый i-й угрозой u_i незащищенной ИС, может определяться в абсолютных единицах: экономических потерях, временных затратах, объеме уничтоженной или «испорченной» информации и т.д.

Однако определение ущерба для каждой угрозы непосредственно – очень сложная задача. Выход из этой ситуации – расчет ущерба как некоторой величины относительно стоимости ИС. Коэффициент h_i, представляющий это отношение, можно трактовать как степень

воздействия *i*-й угрозы на ИС. Степень воздействия может быть определена экспертным путем в предположении, что все угрозы составляют полную группу событий, т.е. коэффициенты h_i удовлетворяют условиям

$$\begin{cases} 0 \le h_i \le 1, \ \forall i \in \overline{1, n}, \\ \sum_{i=1}^{n} h_i = 1. \end{cases} \tag{4.17}$$

Тогда ущерб, наносимый *i*-й угрозой незащищенной ИС,

$$u_i = h_i \left(S_И + S_{ОИ} + S_{СЗИ} \right). \tag{4.18}$$

Исходные данные для расчета степеней воздействия угроз – матрицы парных сравнений степени вреда, наносимого угрозами, построенные по данным всех экспертов. Матрица данных одного эксперта строится на основе табл. 1.4 и представляется в виде

$$M_j^H = \begin{vmatrix} h_{11}^j & h_{12}^j & \dots & h_{1n}^j \\ h_{21}^j & h_{22}^j & \dots & h_{2n}^j \\ \dots & \dots & \dots & \dots \\ h_{n1}^j & h_{n2}^j & \dots & h_{nn}^j \end{vmatrix}, \tag{4.19}$$

где $h_{\alpha\beta}^j, \ \forall \alpha, \beta = \overline{1, n},$ показывает, насколько вред, наносимый α-й угрозой, существеннее вреда, наносимого β-й угрозой.

Матрица (4.19) удовлетворяет выражениям (1.3) – (1.5).

Для нахождения собственного вектора $H_j = \left\{ h_i^j \right\}, \ i = \overline{0, n}$, необходимо выполнить преобразования по формулам (1.9) – (1.12).

4.4. Затраты и стоимость ИС

Расходы на СЗИ

Затраты в ИС предприятия могут быть вычислены с помощью методики оценки совокупной стоимости владения, что позволяет определить прямые и косвенные расходы на аппаратно-программные средства ИС, организационные мероприятия, обучение и повышение квалификации сотрудников, реорганизацию и реструктуризацию ИС и т.д.

Обобщенный показатель ССВ представляет собой сумму прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение СЗИ предприятия в течение года.

Прямые затраты включают в себя:

- капитальные затраты (стоимость информационных активов предприятия и компонентов СЗИ);
- заработную плату сотрудников СИБ;
- затраты на организацию службы поддержки и вычислительной инфраструктуры для удаленных пользователей.

Косвенные затраты показывают влияние ИС предприятия, в том числе СЗИ, на сотрудников предприятия посредством таких показателей, как простои и зависания, затраты на операции и поддержку, не относящиеся к прямым.

В ходе оценки ССВ проводится сбор информации и расчет показателей по следующим позициям:

- компоненты ИС предприятия (информация, элементы ВС, физические элементы СЗИ);
- расходы на аппаратные и программные средства ЗИ;
- затраты на функционирование ИБ.

Затраты на функционирование ИБ подразделяют:

- на организационные расходы (разработка концепции и политики безопасности, проведение организационных мероприятий);
- затраты на определение и подтверждение достигнутого уровня защищенности ресурсов;
- внутренние затраты на ликвидацию последствий нарушения ПИБ;
- внешние затраты на ликвидацию последствий нарушения ПИБ, связанные с утечкой информации, ухудшением имиджа предприятия;
- затраты на ТО СЗИ и мероприятия по предотвращению нарушений ПИБ.

Затраты также можно подразделять на единовременные и систематические.

К единовременным относят расходы на разработку концепции и политики безопасности и расходы на приобретение и установку базовой конфигурации средств ЗИ.

Систематические затраты (затраты на соответствие и затраты на несоответствие ПИБ) – все остальные, в том числе и затраты на обновление средств ЗИ.

Первая группа систематических затрат – затраты на обслуживание СИБ.

1. Управление СЗИ:

- планирование СЗИ;
- изучение информационной инфраструктуры предприятия;
- техническая поддержка производственного персонала при внедрении средств и процедур ЗИ;
- проверка сотрудников на лояльность, выявление угроз безопасности;
- организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства.

2. Регламентное обслуживание средств ЗИ:

- обслуживание и настройка программно-технических средств защиты, ОС и сетевого оборудования;
- организация сетевого взаимодействия;
- поддержание системы резервного копирования и ведения архива данных;
- проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, СВТ.

3. Аудит СИБ:

- контроль изменения состояния информационной среды предприятия;
- система контроля за действиями исполнителей.

4. Поддержка качества технологий:

- обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов, влияющих на целостность и доступность информации;
- доставка (обмен) конфиденциальной информации;
- удовлетворение субъективных требований пользователей (удобство интерфейсов).

5. Поддержка доверия к технологии – обеспечение соответствия принятым стандартам и требованиям достоверности информации.

6. Обучение персонала:

- повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности;
- развитие нормативной базы СБ.

7. Другие затраты, непосредственно не связанные с предупредительными мероприятиями.

Вторая группа систематических затрат – затраты на контроль.

1. Плановые проверки и испытания:

- проверки и испытания программно-технических средств ЗИ;
- проверка навыков эксплуатации средств защиты персоналом предприятия;
- обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности;
- оплата работ по контролю правильности ввода данных в прикладные системы.

2. Внеплановые проверки и испытания:

- оплата работы испытательного персонала специализированных организаций;
- затраты на материально-технические средства, предоставляемые испытательному персоналу.

3. Анализ политики безопасности предприятия:

- идентификация угроз безопасности;
- поиск уязвимостей системы защиты информации;
- оплата работы специалистов по оценке рисков.

4. Соблюдение политики безопасности:

- затраты на контроль реализации функций управления защитой коммерческой тайны;
- затраты на проведение аудита безопасности АС обработки информации;
- материально-техническое поддержание СКУД к объектам и ресурсам предприятия.

5. Контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере ЗИ.

Третья группа включает в себя затраты на ликвидацию последствий нарушения ПБ.

1. Выявление причин нарушения ПБ:

- расследование нарушений ПБ (сбор данных о методах совершения, механизме и способах сокрытия нарушения, поиск следов, орудий и предметов посягательства, выявление мотивов нарушений);

- обновление планов обеспечения деятельности службы безопасности.

2. Восстановление системы безопасности до соответствия требованиям ПИБ:

- приобретение технических средств взамен пришедших в негодность;
- проведение дополнительных испытаний средств ЗИ;
- установка обновлений программных средств ЗИ;
- утилизация скомпрометированных ресурсов.

3. Восстановление информационных ресурсов предприятия:

- восстановление БД и прочих информационных массивов;
- проведение мероприятий по контролю достоверности данных после нарушения их целостности.

4. Реорганизация СЗИ:

- внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности;
- повторные проверки и испытания СЗИ.

Четвертую группу образуют внешние затраты на ликвидацию последствий нарушения ПБ. Они связаны со следующими фактами.

1. Обязательства перед государством и партнерами:

- восстановление доверия потребителей, партнеров, государства;
- юридические споры и выплата компенсаций;
- разрыв деловых отношений.

2. Утрата ведущих позиций:

- проведение дополнительных исследований и разработка новой рыночной стратегии;
- отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, и расходы на разработку новых решений.

3. Продвижение продукции:

- ликвидация проблем в снабжении, производстве и сбыте продукции;
- устранение последствий компрометации производимой предприятием продукции и падения цен на нее;
- устранение трудностей при приобретении оборудования или технологий.

Неизбежны следующие затраты:

- обслуживание технических средств защиты;
- конфиденциальное делопроизводство;
- обеспечение функционирования и аудит системы безопасности;
- поддержание минимального уровня проверок и контроля с привлечением специализированных организаций;
- обучение персонала методам ИБ.

Соблюдение ПИБ и проведение профилактики нарушений позволяет исключить или существенно снизить затраты:

- на восстановление системы безопасности до соответствия требованиям ПИБ;
- восстановление информационных ресурсов предприятия;
- реорганизацию СЗИ;
- восстановление доверия потребителей, партнеров, государства;
- юридические споры и компенсации;
- выявление причин нарушения ПИБ.

Качественное соотношение систематических затрат на предотвращение нарушений ИБ, затрат на контроль и затрат на предотвращение последствий нарушений показано на рис. 4.1.

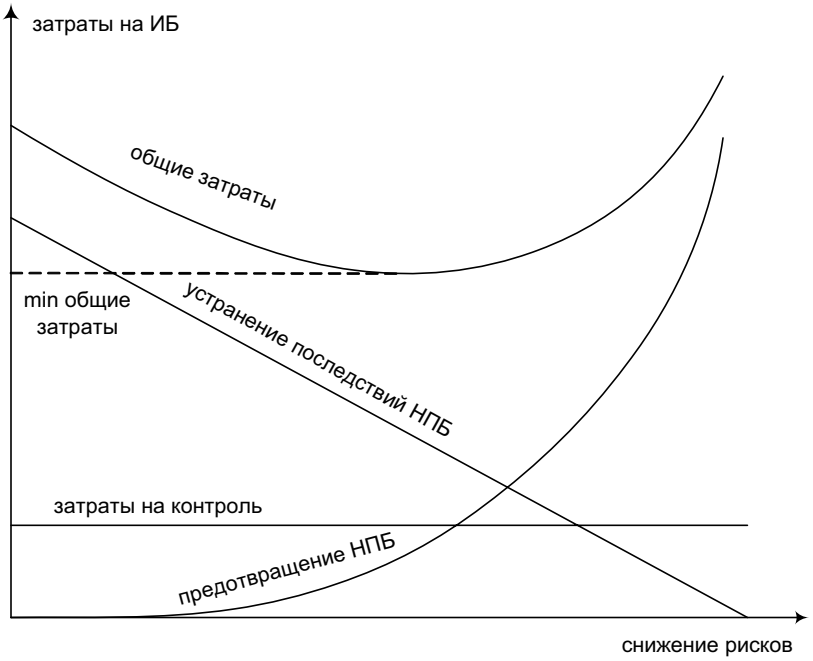


Рис. 4.1. Качественное соотношение различных затрат

График построен с учетом двух допущений:

1) мероприятия по ТО комплекса программно-технических средств СЗИ и предупреждению нарушений ПИБ соответствуют пра-

вилу Парето: в первую очередь рассматриваются проблемы, решение которых приводит к наибольшему снижению рисков;

2) величина рисков, соответствующая минимальным общим затратам, не изменяется во времени; в действительности из-за возникновения новых уязвимостей в СЗИ требуется увеличение затрат на предотвращение НПБ, что приводит к изменению этой величины рисков.

Определение стоимости ИС

Стоимость ресурсов ИС вычисляют следующим образом. Для всех ресурсов, стоимость которых (исходя из перечисленных выше затрат) можно непосредственно определить, проводится именно такой расчет стоимости ресурса на один год.

Ценность информационных ресурсов может определяться на основе ранговой шкалы (по табл. 1.5), тогда вектор ценности $C_j = \left(c_1^j, c_2^j, ..., c_z^j \right)$ должен быть преобразован в матрицу парных сравнений:

$$M_j^C = \begin{vmatrix} 1 & \frac{1}{c_{21}^j} & ... & \frac{1}{c_{z1}^j} \\ c_{21}^j & 1 & ... & \frac{1}{c_{z2}^j} \\ ... & ... & ... & ... \\ c_{z1}^j & c_{z2}^j & ... & 1 \end{vmatrix} \qquad (4.20)$$

с использованием преобразования вида

$$c_{ab}^j = \frac{c_a^j}{c_b^j}, \quad \forall a,b \in \overline{1,n}. \qquad (4.21)$$

Если ценность ресурсов определяется методом парных сравнений, то матрица (4.20) получается непосредственно.

Далее находят вектор относительной ценности $\overline{C}_j = \left\{ \bar{c}_i^j \right\}, \quad i = \overline{1,z}$. Для этого необходимо выполнить преобразования по формулам (1.9) – (1.12).

Стоимость каждого информационного ресурса определяется на основе вектора ценности после выделения опорного элемента по формуле

$$S_{Ии} = \frac{\bar{c}_i}{\bar{c}_x} S_{Их}, \; i = \overline{1,z}, \qquad (4.22)$$

где $\bar{c}_x$ – относительная ценность опорного ресурса; $S_{Их}$ – его стоимость.

Опорным выбирается элемент, стоимость которого можно рассчитать легче, чем стоимость других элементов, например на основе затрат на его использование и/или прибыли, которую он приносит.

Стоимость элементов ОИ, подверженных воздействию угроз, $S_{ОИ}$ определяется элементарным суммированием стоимости всех устройств в расчете на один год:

$$S_{ОИ} = \sum_{i=1}^{r} \frac{S_{ОИk}}{t_k}, \qquad (4.23)$$

где $S_{ОИk}$ – стоимость элемента; t_k – срок службы (в годах).

Стоимость элементов СЗИ $S_{СЗИ}$ также определяется в расчете на один год путем суммирования затрат на ИБ по всем позициям.

4.5. Вероятности устранения угроз безопасности

Вероятность устранения *i*-й угрозы p_i^Y определяется тем, насколько полно учтены качественные и количественные требования к СЗИ при их проектировании, т.е.

$$p_i^Y = f\left(x_{iq}, \forall q \in \overline{1,t}\right), \quad \forall i = \overline{1,n},$$

где x_{iq} – степень выполнения *q*-го требования к СЗИ для устранения *i*-й угрозы.

Пусть первые l требований будут количественными ($q = \overline{1,l}$), остальные $(t-l)$ – качественными ($q = \overline{l+1,t}$).

Оценка степени выполнения требований производится посредством аудита параметров ИС на соответствие требованиям стандартов безопасности (см. гл. 3).

Оценка степени выполнения количественных требований

Степень выполнения каждого количественного требования определяется его отношением к требуемому (оптимальному) количественному значению одного параметра СЗИ. Для оценки степени выполнения требования при разнородности параметров необходимо использовать нормированное значение $0 \le \bar{x}_{iq} \le 1$.

Множество значений степени выполнения количественного требования, определенных всеми экспертами,

$$A\left(x_{iq}\right) = \left\{x_{iq}^j, \quad \forall j = \overline{1,m}\right\} \qquad (4.24)$$

является функцией принадлежности степени соответствия параметра СЗИ его оптимальному значению.

Обозначим $x_{iq}^{MIN}, x_{iq}^{MAX}, x_{iq}^{НЛ}, x_{iq}^{НХ}, x_{iq}^{ОПТ}$ минимальное, максимальное, наилучшее, наихудшее и оптимальное значения q-го параметра. Очевидно, что не всегда максимальное значение является наилучшим, а минимальное – наихудшим. Но также можно отметить, что не всегда экстремальное значение параметра оптимально с точки зрения организации СЗИ.

Для нормирования могут быть использованы следующие преобразования:

- если максимальное значение параметра оптимальное, т.е. $x_{iq}^{MAX} \to x_{iq}^{НЛ} = x_{iq}^{ОПТ}, \quad x_{iq}^{MIN} \to x_{iq}^{НХ}$, то

$$\bar{x}_{iq} = \frac{x_{iq} - x_{iq}^{MIN}}{x_{iq}^{MAX} - x_{iq}^{MIN}}; \tag{4.25}$$

- если минимальное значение параметра оптимальное, т.е. $x_{iq}^{MIN} \to x_{iq}^{НЛ} = x_{iq}^{ОПТ}, \quad x_{iq}^{MAX} \to x_{iq}^{НХ}$, то

$$\bar{x}_{iq} = \frac{x_{iq}^{MAX} - x_{iq}}{x_{iq}^{MAX} - x_{iq}^{MIN}}; \tag{4.26}$$

- если оптимальное значение параметра находится между минимальным и максимальным, которые оба являются наихудшими, т.е. $x_{iq}^{НЛ} = x_{iq}^{ОПТ}, \quad x_{iq}^{MIN} \to x_{iq}^{НХ}, \quad x_{iq}^{MAX} \to x_{iq}^{НХ}, \quad x_{iq}^{MIN} \le x_{iq}^{ОПТ} \le x_{iq}^{MAX}$, то

$$\bar{x}_{iq} = \begin{cases} 0, \ x_{iq} = x_{iq}^{МИН} \ \text{ или } \ x_{iq} = x_{iq}^{MAX}, \\ 1, \ x_{iq} = x_{iq}^{ОПТ}, \\ \dfrac{x_{iq} - x_{iq}^{МИН}}{x_{iq}^{ОПТ} - x_{iq}^{MIN}}, \quad x_{iq}^{MIN} < x_{iq} < x_{iq}^{ОПТ}, \\ \dfrac{x_{iq}^{MAX} - x_{iq}}{x_{iq}^{MAX} - x_{iq}^{ОПТ}}, \quad x_{iq}^{ОПТ} < x_{iq} < x_{iq}^{MAX}. \end{cases} \tag{4.27}$$

Оценка степени выполнения качественных требований

Для оценки степени выполнения качественных требований (а таких требований в различных стандартах несравнимо больше, чем

количественных) необходимо использовать теорию нечетких множеств.

Степень выполнения каждого качественного требования определяется функцией принадлежности ряда характеристик СЗИ, от которых зависит выполнение этого требования, к их оптимальным значениям.

Пусть $G = \{g_1, g_2, ..., g_p\}$ – универсальное множество характеристик СЗИ. На множестве G задается нечеткое множество A_q, отражающее степень принадлежности СЗИ к оптимальной по q-му требованию.

Нечеткое множество A_q определяется:

1) множеством степеней соответствия каждой характеристики СЗИ выполнению q-го качественного требования $Y_q = \{y_1, y_2, ..., y_p\}$.

2) множеством степеней влияния характеристик на выполнение требования в целом $\Sigma_q = \{\sigma_1, \sigma_2, ..., \sigma_p\}$.

Степень соответствия определяется из предположения, что если некоторая характеристика полностью удовлетворяет требованию, то ее степень соответствия равна единице, если полностью не удовлетворяет, то – нулю.

В упрощенном варианте значение степени соответствия может быть присвоено характеристике непосредственно. Для нечетких количественных характеристик, описание которых соответствует выражению «примерно <требуемое значение z>», т.е. имеющих нормальный вид функции распределения (см. рис. 2.3, *в*), можно воспользоваться выражением

$$x_{iq} = e^{-\beta\left(z_q^{треб} - z_q^{реал}\right)^2}, \qquad (4.28)$$

где β зависит от требуемой степени нечеткости и определяется из выражения

$$\beta = \frac{\ln \alpha}{\delta^2}, \qquad (4.29)$$

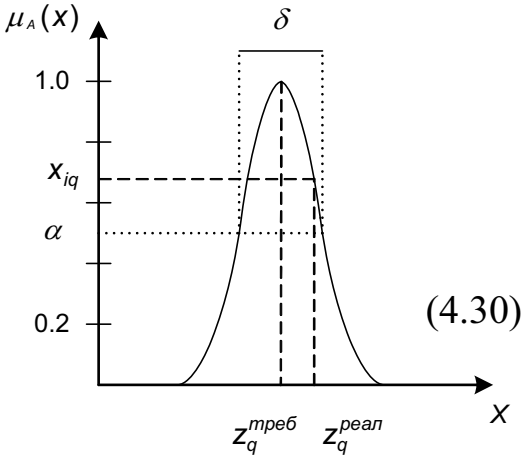
где δ – расстояние между точками перехода для функции принадлежности, т.е. точками, в которых функция принимает значение α.

Уровень α определяет степень допущения принадлежности реального значения параметра $z_q^{реал}$ требуемому $z_q^{треб}$. Обычно $\alpha \in [0{,}5;\ 1{,}0]$.

Расстояние δ определяет удвоенную максимальную величину отклонения параметра от требуемого значения (рис. 4.2).

Степень влияния характеристики СЗИ на выполнение требования можно найти из матрицы парных сравнений:

$$M_j^{\Sigma} = \begin{vmatrix} \sigma_{11}^j & \sigma_{12}^j & \dots & \sigma_{1p}^j \\ \sigma_{21}^j & \sigma_{22}^j & \dots & \sigma_{2p}^j \\ \dots & \dots & \dots & \dots \\ \sigma_{p1}^j & \sigma_{p2}^j & \dots & \sigma_{pp}^j \end{vmatrix}, \quad (4.30)$$



(4.30)

Рис. 4.2. Графическое представление степени принадлежности качественного описания количественного параметра

где σ_{ab}^j, $\forall a,b = \overline{1,p}$, показывает, насколько влияние *a*-й характеристики существеннее влияния *b*-й.

Матрица (4.30) удовлетворяет выражениям (1.3) – (1.5).

Для нахождения собственного вектора $\Sigma_j = \left\{ \sigma_i^j \right\}$, $i = \overline{1,p}$, необходимо выполнить преобразования по формулам (1.9) – (1.12).

Степень выполнения *q*-го качественного требования по оценкам *j*-го эксперта в упрощенном варианте может быть найдена по формуле

$$x_{iq}^j = \sum_{k=1}^{p} y_k^j \sigma_k^j . \quad (4.31)$$

Вероятность устранения *i*-й угрозы по оценкам *j*-го эксперта p_{ij}^V определяется из выражения

$$p_{ij}^V = \sum_{q=1}^{l} v_{iq}^j \bar{x}_{iq}^j + \sum_{q=l+1}^{t} v_{iq}^j x_{iq}^j , \quad (4.32)$$

где v_{iq}^j – весовой коэффициент, значимость *q*-го требования для устранения *i*-й угрозы по оценке *j*-го эксперта.

Данный коэффициент можно определить из матрицы парных сравнений:

$$M_j^V = \begin{vmatrix} v_{11}^j & v_{12}^j & \dots & v_{1t}^j \\ v_{21}^j & v_{22}^j & \dots & v_{2t}^j \\ \dots & \dots & \dots & \dots \\ v_{t1}^j & v_{t2}^j & \dots & v_{tt}^j \end{vmatrix}, \quad (4.33)$$

где v_{ab}^{j}, $\forall a,b=\overline{1,t}$, показывает, насколько влияние *a*-го требования больше влияния *b*-го для устранения *i*-й угрозы по оценке *j*-го эксперта.

Матрица (4.33) удовлетворяет выражениям (1.3) – (1.5).

Для нахождения собственного вектора $V_{ij}=\left\{v_{iq}^{j}\right\}$, $q=\overline{1,\ t}$, необходимо выполнить преобразования по формулам (1.9) – (1.12).

В том случае, если требований много или они имеют примерно одинаковое влияние на устранение *i*-й угрозы, значимость требованиям можно проставить непосредственно, чтобы она удовлетворяла условию нормирования $\sum_{i=1}^{n} v_{iq}^{j}=1$.

4.6. Агрегирование частных оценок параметров СЗИ

Частными называются оценки параметра ИС, полученные одним экспертом. Для определения общей оценки параметра необходимо произвести агрегирование частных оценок, например, путем усреднения. Но известно, что в ЭГ могут входить эксперты с разным уровнем подготовки, т.е. они будут давать оценки разной степени адекватности. Именитость и ученость эксперта не всегда является гарантией высочайшего качества даваемых им оценок.

Уточнение коэффициента авторитета эксперта может быть проведено на основе согласованности его суждений. Проще всего такая согласованность выявляется в матрицах парных сравнений.

Уточненные коэффициенты авторитета могут быть использованы для нетривиальной обработки частных оценок и получения общего результата.

Коррекция коэффициентов авторитета экспертов

Первичные коэффициенты авторитета экспертов (1.15) могут быть скорректированы на основе полученных коэффициентов рассогласования оценок (1.8).

Средний коэффициент рассогласования определяется как среднее арифметическое

$$K_{CP}^{j}=\frac{1}{k}\sum_{i=1}^{k}K_{Pi}^{j}, \qquad (4.34)$$

где k – количество матриц парных сравнений, построенных экспертом; K_{Pi}^{j} – коэффициент рассогласования i-й матрицы, вычисленный по формуле (1.15).

Уточнение коэффициента авторитета вычисляется как

$$\Delta\nu_j = \frac{1}{2}\left(\nu_j^0 + \frac{\nu_j^0}{\sqrt{K_{CP}^{j}}}\right). \qquad (4.35)$$

Уточнение предполагает, что исправленный коэффициент будет средним арифметическим первичного коэффициента и его снижения из-за рассогласования оценок. Такое снижение будет различным для всех экспертов.

Скорректированный коэффициент, удовлетворяющий правилу нормирования, определяется по формуле

$$\nu_j = \frac{\Delta\nu_j}{\sum_{j=1}^{m}\Delta\nu_j}. \qquad (4.36)$$

Вычисление показателей качества СЗИ

Значения i-го параметра из L-й группы параметров, найденного всеми экспертами, можно считать функцией принадлежности данного параметра его истинному значению.

Например, для группы параметров «вероятности возникновения угроз» нечеткое значение каждой i-й вероятности можно записать следующим образом:

$$A_L(p_i^B) = \left\{p_{i1}^B, p_{i2}^B, \ldots, p_{im}^B\right\}. \qquad (4.37)$$

Мера вероятности нечеткого множества (4.37), вычисленная по формулам (2.24) – (2.26), дает искомое значение i-й вероятности p_i^B.

Аналогично определяют параметры всех остальных групп:

- степени воздействия угроз безопасности $h_i, \forall i$ по формуле (4.19);
- относительную ценность информационных ресурсов $c_i, \forall i$ по формуле (4.20);
- вероятности устранения угроз безопасности $p_i^Y, \forall i$ по формуле (4.32).

Эти группы параметров используют для вычисления:

1) стоимости информационных ресурсов (4.22);

2) ущерба, наносимого угрозами (4.18);

3) риска в незащищенной системе (4.4);
4) риска в защищенной системе (4.5);
5) экономической эффективности (4.6);
6) коэффициента защищенности (4.7).

Оценка достоверности экспертизы

Мера внутренней неопределенности $D(A_{Li})$ нечеткого множества (4.37), вычисленная по формулам (2.21), (2.22), показывает степень доверия оценке *i*-го параметра из *L*-й группы.

Степени доверия оценкам всех параметров из *L*-й группы образуют нечеткое множество

$$B_L = \{ D(A_{L1}),\ D(A_{L2}),\ ...,\ D(A_{Ln}) \}. \qquad (4.38)$$

Меру энтропии (показатель размытости) нечеткого множества (4.38), определенную по формуле (2.19), можно считать вероятностью того, что экспертиза всех параметров из *L*-й группы оказалась ошибочной.

Показатель

$$\Theta_L = 1 - d(B_L) \qquad (4.39)$$

является степенью доверия оценке параметров *L*-й группы.

Среднее значение по всем группам параметров

$$\Theta = \frac{1}{k} \sum_{L=1}^{k} \Theta_L \qquad (4.40)$$

показывает степень доверия всей экспертизе.

Краткие выводы

Основные показатели качества СЗИ – экономическая эффективность и коэффициент защищенности. Их вычисление основывается на расчете вероятностей возникновения и реализации угроз безопасности, ущерба, наносимого реализацией угроз, и стоимости ресурсов ИС. Расчет таких параметров производится путем экспертизы ИС и аудита степени выполнения требований ИБ.

Экспертиза ряда параметров ИС, таких как уязвимости, ценность информационных ресурсов, ущерб от реализации угроз, проводится по методу парных сравнений альтернатив.

Расчет затрат, стоимости оборудования СЗИ и мероприятий по поддержанию ИБ может быть проведен по методу оценки ССВ.

Для оценки степени выполнения качественных требований необходимо использовать теорию нечетких множеств.

Частные оценки, предоставляемые каждым экспертом, должны быть агрегированы в интегральную оценку параметра с учетом коэффициентов авторитета.

Если ЭГ состояла из более чем одного эксперта, то можно оценить и достоверность самой экспертизы. Но такой оценкой можно руководствоваться, если, во-первых, был корректно реализован алгоритм проведения экспертизы и, во-вторых, количество экспертов составляло не менее пяти человек.

Контрольные вопросы

1. Какие параметры СЗИ оказывают влияние на ее экономическую эффективность?
2. Какие параметры СЗИ оказывают влияние на коэффициент защищенности?
3. Опишите алгоритм определения вероятностей возникновения угроз безопасности ИС.
4. Опишите алгоритм определения ущерба от реализации угроз безопасности ИС.
5. Перечислите основные статьи затрат на СЗИ.
6. Перечислите основные статьи систематических затрат на поддержание ИБ предприятия.
7. Какие затраты неизбежны и какие можно существенно сократить посредством соблюдения ПИБ?
8. Поясните графически соотношение различных затрат на СЗИ.
9. Опишите алгоритм определения стоимости ресурсов ИС.
10. Опишите алгоритм оценки степени выполнения количественных требований к СЗИ.
11. Опишите алгоритм оценки степени выполнения качественных требований к СЗИ.
12. Каким образом и с какой целью проводится коррекция коэффициентов авторитета экспертов?
13. Каким образом агрегируются частные оценки для получения интегральной оценки параметра?
14. Каким образом и при каких условиях можно оценить достоверность проведения всей экспертизы?

ЗАКЛЮЧЕНИЕ

Для коммерческих предприятий защита информации рассматривается в контексте экономической эффективности. Методология оценки эффективности СЗИ предполагает использование различных критериев, которые определяют оптимизируемые показатели качества самой СЗИ, т.е. оценка эффективности СЗИ не является самоцелью, а служит для построения оптимальной и адаптивной СЗИ.

Элементы и параметры ИС разнородные, многие показатели имеют преимущественно качественное описание. В этих условиях единственный адекватный способ проверки качества функционирования и уровня защищенности ИС – процедура экспертизы.

Оценки одного и того же параметра, получаемые разными экспертами, могут существенно отличаться друг от друга. В большей степени это касается качественных описаний. Для получения оценки, общей для всей ЭГ, необходимо определить коэффициенты авторитета экспертов на основе формальных сведений о них по нескольким направлениям.

Для математического представления описаний качественных параметров ИС необходимо использовать теорию нечетких множеств.

Для установления степени соответствия применяемых в организации защитных мер выбранным критериям и анализа результативности системы управления ИБ при достижении конкретных целей используют аудит ИБ, который является на данный момент одним из наиболее эффективных инструментов получения независимой и объективной оценки текущего уровня защищённости предприятия от угроз информационной безопасности.

Аудит проводится на основе международных и российских стандартов и других нормативных документов. Стандарты ИБ определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики.

В процессе аудита проводится исследование ИС организации в соответствии с формальной моделью, включающее в себя анализ угроз ИБ предприятия, уязвимостей ИС и степени исполнения требований ИБ. Для большинства коммерческих предприятий характерны однотипные угрозы ИБ, хотя количество и характер уязвимостей достаточно индивидуальны.

Основные показатели качества СЗИ – экономическая эффективность и коэффициент защищенности, вычисление которых основывается на расчете вероятностей возникновения и реализации угроз безопасности, ущерба, наносимого реализацией угроз, и стоимости ресурсов ИС. Расчет таких параметров производится путем экспертизы ИС и аудита степени выполнения требований ИБ.

Экспертиза ряда параметров ИС, таких как уязвимости, ценность информационных ресурсов, ущерб от реализации угроз, проводится по методу парных сравнений альтернатив.

Расчет затрат, стоимости оборудования СЗИ и мероприятий по поддержанию ИБ может быть проведен по методу оценки ССВ.

Для больших экспертных групп можно оценить достоверность проведения самой экспертизы.

ПРИЛОЖЕНИЕ

ПРИМЕР РАСЧЕТА ПОКАЗАТЕЛЕЙ КАЧЕСТВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

В рассматриваемом примере в связи с ограниченностью объема данного учебного пособия приведены сведения и расчеты экспертной группы только для параметра «вероятность возникновения угроз»; информация по другим параметрам и показателям качества дана только от одного эксперта. Как следствие, не проведена оценка достоверности экспертизы.

Объект исследования – предприятие «Владимирский филиал ЗАО "Банковские системы и сервисы"».

Аудит угроз и уязвимостей

В процессе аудита выявлены следующие угрозы ИБ исследуемого предприятия:

1) хищение (в том числе путем копирования) информации;
2) хищение средств обработки информации;
3) модификация (искажение) информации;
4) сбои в работе средств обработки информации;
5) блокирование либо уничтожение информации;
6) блокирование средств обработки информации;
7) физическое проникновение на защищаемый объект;
8) невозможность идентификации нарушителя, обнаружения факта попытки НСД.

В процессе аудита выявлены следующие уязвимости ИС исследуемого предприятия:

1) наличие незащищенного чердачного помещения;
2) чердачное помещение не оснащено пожарной сигнализацией;
3) на одном окне организации на первом этаже здания не установлена решетка;
4) на окнах установлены распашные решетки, фиксированные навесными замками;
5) отсутствие видеокамер внутри здания;
6) часть компьютеров, обрабатывающих защищаемую информацию, не оснащена источниками бесперебойного питания;

7) слабая защищенность объекта в обеденное время (открытая входная дверь или отсутствие охраны);

8) видеокамера на входной двери в здание не имеет режима видеорегистрации;

9) создание образов логических дисков не регулярно, не охватывает все компьютеры организации, образы хранятся на локальном компьютере;

10) не предусмотрены места хранения лицензионных установочных копий ПО;

11) отсутствие сейфов, хранилищ и других мест защищенного хранения документов;

12) пароли (для доступа в Интернет, электронную почту) прописаны в соответствующем ПО и не требуют ввода;

13) не ведется аудит доступа к ресурсам;

14) каждый сотрудник имеет права администратора к ресурсам своего компьютера. Отсутствие ограничений доступа;

15) доступность БД 1С с любого компьютера сети организации;

16) ключ-дискета для казначейской системы электронного документооборота лежит на столе у кассира;

17) компьютер, осуществляющий работу с электронной цифровой подписью, входит в состав сети организации, подключенной к сети Интернет;

18) не выполняется полное сканирование программной среды на наличие вредоносных программ;

19) отсутствуют памятки, инструкции для пользователей по антивирусному контролю, по резервированию/восстановлению данных.

Формирование экспертной группы

В состав ЭГ вошли четыре эксперта. Все четверо имели на момент проведения экспертизы неоконченное высшее образование по приоритетному направлению (3 балла по табл. 1.6). Кроме того, первый эксперт имел опыт работы по специальности два года (3 балла).

Согласно (1.15) первичные коэффициенты авторитета составили:

1-й эксперт – (3+0+3+0)/15 = 0,40;

2-й эксперт – (3+0+0+0)/15 = 0,20;

3-й эксперт – (3+0+0+0)/15 = 0,20;

4-й эксперт – (3+0+0+0)/15 = 0,20.

Экспертиза уязвимостей ИС

Значимость уязвимостей определена на основе табл. 1.2 и построена матрица парных сравнений (4.8).

Данные эксперта № 1

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
1	1	9	3	5	1/7	1/7	1/9	7	1/7	1/7	1/9	1/9	7	1/7	1/9	1/9	1/7	1/7	3
2	1/9	1	1/7	5	1/7	1/9	1/9	7	1/7	1/7	1/9	1/3	7	1/9	1/9	1/9	1/9	1/7	7
3	1/3	7	1	9	7	1/7	1/9	7	1/7	1	1/7	1/7	5	1/9	1/9	5	7	1/7	9
4	1/5	1/5	1/9	1	1/7	1/9	1/9	1	1/7	1/5	5	1/7	1	1/9	1/7	1/7	1/9	1/7	1
5	7	7	1/7	7	1	1/7	1/9	1	1/7	1/7	1/7	1/7	1/7	1/9	1/9	1/7	1/9	1/7	7
6	7	9	7	9	7	1	1	7	1	1	1/7	1/7	7	1/7	1/7	1/7	1/9	5	7
7	9	9	9	9	9	1	1	9	7	9	9	1/7	7	1	9	9	1/7	7	9
8	1/7	1/7	1/7	1	1	1/7	1/9	1	1/7	1/7	1/7	1/7	1	1/9	1/3	1/7	1/5	1/7	7
9	7	7	7	7	7	1	1/7	7	1	1/5	1/5	1/7	1	1/7	1/7	1/9	1/7	1	7
10	7	7	1	5	7	1	1/9	7	5	1	1	1	7	1/7	1/3	1	1/3	1/7	7
11	9	9	7	1/5	1/7	7	1/9	7	5	1	1	1/5	9	7	7	1	1/5	7	7
12	9	3	7	7	7	7	7	7	7	1	5	1	7	1	7	7	1	7	7
13	1/7	1/7	1/5	1	7	1/7	1/7	1	1	1/7	1/9	1/7	1	1/7	1/7	1/7	1/3	7	7
14	7	9	9	9	9	7	1	9	7	7	1/7	1	7	1	1	1/3	1	7	7
15	9	9	9	7	9	7	1/9	3	7	3	1/7	1/7	7	1	1	1/3	1	9	9
16	9	9	1/5	7	7	7	1/9	7	9	1	1	1/7	7	3	3	1	3	7	9
17	7	9	1/7	9	9	9	7	5	7	3	5	1	3	1	1	1/3	1	7	9
18	7	7	7	7	7	1/5	1/7	7	1	7	1/7	1/7	1/7	1/7	1/9	1/7	1/7	1	7
19	1/3	1/7	1/9	1	1/7	1/7	1/9	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/9	1/9	1/9	1/7	1

Данные эксперта № 2

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
1	1	3	1/7	3	3	1/5	1/9	1/7	1/3	1/7	1/9	1/7	1/7	1/7	1/9	1/9	1/7	1/7	1/3
2	1/3	1	1/7	3	1/3	1/5	1/7	1/3	1/3	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7
3	7	7	1	9	1/3	3	1/9	7	1/3	1/7	1/7	1/7	1/7	1/7	1/7	1/9	1/5	1/7	1/7
4	1/3	1/3	1/9	1	1/3	1/7	1/9	1/7	1/7	1/9	1/9	1/9	1/7	1/9	1/9	1/9	1/7	1/7	1/7
5	1/3	3	3	3	1	7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/9	1/7	1/7	1/3
6	5	5	1/3	7	1/7	1	1/7	3	1/3	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/7	1/5	1/5
7	9	7	9	9	7	7	1	9	7	1/3	1/3	1/3	1/3	1/3	1/3	1/3	3	3	7
8	7	3	1/7	7	7	1/3	1/9	1	1/3	1/7	1/7	1/7	1/7	1/9	1/5	1/7	1/7	1/7	1/7
9	3	3	3	7	7	3	1/7	3	1	3	1/7	1/7	1/3	1/7	1/7	1/7	1/5	3	3
10	7	7	7	9	7	7	3	7	1/3	1	1/7	1/7	1/7	1/7	1/7	1/7	1/7	3	3
11	9	7	7	9	7	7	3	7	7	7	1	9	7	7	3	1	7	7	7
12	7	7	7	7	1/3	7	1/3	7	1/3	1/3	1/9	1	1/7	1/9	1/9	1/7	1/5	3	3
13	7	7	7	7	7	7	3	7	3	7	1/7	7	1	1/3	1/7	1/3	3	3	3
14	7	7	7	9	7	7	3	9	7	7	1/7	9	3	1	3	1/3	7	7	9
15	9	7	7	9	7	7	3	5	7	7	1/3	9	7	1/3	1	1/7	1/7	1/5	3
16	9	7	9	9	9	7	3	7	7	7	1	7	7	7	7	1	7	7	9
17	7	7	5	7	7	7	1/3	7	5	7	1/7	5	1/3	1/7	7	1/7	1	5	5
18	7	7	7	7	7	5	1/3	7	1/3	1/3	1/7	1/3	1/3	1/7	5	1/7	1/5	1	7
19	3	7	7	7	3	5	1/7	7	1/3	1/3	1/7	1/3	1/3	1/9	1/3	1/9	1/5	1/7	1

Данные эксперта № 3

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
1	1	6	1/4	8	1/5	1/6	1/9	7	1/3	1/6	1/7	1/4	5	1/9	3	1/5	1/7	1/6	5
2	1/6	1	1/3	7	1/7	1/7	1/9	5	1/5	1/7	1/7	1/7	3	1/9	1	1/5	1/7	1/6	5
3	4	3	1	9	3	1/5	1/9	6	1/3	1/5	1/6	1/3	4	1/9	2	1/4	1/6	1/5	6
4	1/8	1/7	1/9	1	1/5	1/7	1/9	5	1/5	1/7	1/8	1/5	5	1/9	1/3	1/6	1/7	1/7	3
5	5	7	1/3	5	1	1/5	1/7	5	1/2	1/4	1/3	5	5	1/8	5	1	3	1/3	7
6	6	7	5	7	5	1	1/6	7	1	1	1/3	7	8	1/7	7	1/3	1/3	1	7
7	9	9	9	9	7	6	1	9	8	9	3	7	9	1	8	3	3	3	8
8	1/7	1/5	1/6	1/5	1/5	1/7	1/9	1	1/5	1/7	1/7	1/5	1	1/9	1/3	1/5	1/7	1/7	1/3
9	3	5	3	5	2	1	1/8	5	1	1/5	1/3	5	7	1/5	3	1/3	1/3	3	5
10	6	7	5	7	4	1	1/9	7	5	1	1	7	9	1/3	7	1	3	5	7
11	7	7	6	8	3	3	1/3	7	3	1	1	7	9	1/4	5	1	2	3	6
12	4	7	3	5	/5	1/7	1/7	5	1/5	1/7	1/7	1	1	1/9	1/3	1/7	1/5	1/5	3
13	1/5	1/3	1/4	1/5	1/5	1/8	1/9	1	1/7	1/9	1/9	1	1	1/9	1/3	1/5	1/5	1/6	2
14	9	9	9	9	8	7	1	9	5	3	4	9	9	1	7	3	5	7	9
15	1/3	1	1/2	3	1/5	1/7	1/8	3	1/3	1/7	1/5	3	3	1/7	1	1/5	1/5	/5	3
16	5	5	4	6	1	3	1/3	5	3	1	1	7	5	1/3	5	1	1	3	7
17	7	7	6	7	1/3	3	1/3	7	3	1/3	1/2	5	5	1/5	5	1	1	5	7
18	6	6	5	7	3	1	1/3	7	1/3	1/5	1/3	5	6	1/7	5	1/3	1/5	1	3
19	1/5	1/5	1/6	1/3	1/7	1/7	1/8	3	1/5	1/7	1/6	1/3	1/2	1/9	1/3	1/7	1/7	1/3	1

Данные эксперта № 4

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
1	1	5	1/3	1/3	1/5	1	1	3	1/3	5	1/7	1/3	1/3	1	1/5	1	1/7	1	1
2	1/5	1	1/5	1/5	1/7	1/3	1/3	1	1/5	3	1/9	1/5	1/5	1/3	1/7	1/3	1/9	1	1/3
3	3	5	1	1	1/3	1	1	1	1/3	1	1/7	1	1	3	1/3	1	1/7	3	1
4	3	5	1	1	1/5	1	1	3	1/3	5	1/7	1/3	1/3	1	1/5	1	1/7	3	1
5	5	7	3	5	1	5	3	3	1	7	1/3	1	1	5	1/3	3	1/3	5	3
6	1	3	1	1	1/5	1	3	1	1	5	1/5	1	1	5	1/3	3	1/3	3	3
7	1	3	1	1	1/3	1/3	1	1	1	5	1/5	1	1	5	1/3	3	1/5	3	1
8	1/3	1	1	1/3	1/3	1	1	1	1/3	3	1/7	1/3	1/3	3	1/3	1	1/7	3	1
9	3	5	3	3	1	1	1	3	1	5	1/7	1	1	3	1/3	1	1/5	3	1
10	1/5	1/3	1	1/5	1/7	1/5	1/5	1/3	1/5	1	1/7	1/3	1/5	3	1/5	1	1/7	3	1
11	7	9	7	7	3	5	5	7	7	7	1	5	5	7	3	5	1	7	3
12	3	5	1	3	1	1	1	3	1	3	1/5	1	1	3	1/3	3	1/5	3	1
13	3	5	1	3	1	1	1	3	1	5	1/5	1	1	5	1/3	3	1/3	5	3
14	1	3	1/3	1	1/5	1/5	1/5	1/3	1/3	1/3	1/7	1/3	1/5	1	1/3	3	1/5	3	1
15	5	7	3	5	3	3	3	3	3	5	1/3	3	3	3	1	5	1/3	5	3
16	1	3	1	1	1/3	1/3	1/3	1	1	1	1/5	1/3	1/3	1/3	1/5	1	1/7	3	1
17	7	9	7	7	3	3	5	7	5	7	1	5	3	5	3	7	1	7	5
18	1	1	1/3	1/3	1/5	1/3	1/3	1/3	1/3	1/3	1/7	1/3	1/5	1/3	1/5	1/3	1/7	1	3
19	1	3	1	1	1/3	1/3	1	1	1	1	1/3	1	1/3	1	1/3	1	1/5	1/3	1

Доступность уязвимостей определена на основе табл. 1.3 и построен вектор (4.9).

Данные эксперта № 1

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
3	5	7	3	7	3	7	3	5	3	3	3	7	3	3	3	5	9	5

Данные эксперта № 2

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
7	7	9	7	9	7	9	3	9	9	7	9	3	7	7	7	5	7	9

Данные эксперта № 3

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
9	5	7	5	3	5	9	3	9	9	9	5	3	9	3	9	5	7	3

Данные эксперта № 4

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
5	3	7	5	5	3	6	3	5	6	5	5	5	7	7	6	7	5	7

Далее были построены матрицы причинно-следственных связей между угрозами и уязвимостями (4.10).

Данные эксперта № 1

		Уязвимости																		
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
Угрозы	**1**	1	0	1	0	0	0	1	0	1	1	1	1	0	1	1	1	1	0	0
	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0
	3	0	0	0	0	0	1	0	0	1	0	0	1	0	1	1	0	1	1	0
	4	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1	0	1	0
	5	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1
	6	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0
	7	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
	8	0	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0

Данные эксперта № 2

		Уязвимости																		
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
Угрозы	**1**	1	0	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	0	0
	2	0	1	0	0	0	1	1	0	1	1	1	1	0	1	1	1	1	1	1
	3	1	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	1	1	1
	4	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	1	1
	5	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0
	6	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	1	0	1	1
	7	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0
	8	0	0	0	0	1	0	1	1	0	0	0	1	1	1	1	0	1	0	0

Данные эксперта № 3

		Уязвимости																		
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
Угрозы	**1**	0	0	0	0	0	0	1	0	0	1	1	0	0	1	1	1	1	0	0
	2	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1
	3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0
	4	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	1
	5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	6	0	0	0	0	0	1	1	0	0	1	1	0	0	1	0	1	1	1	1
	7	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
	8	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0

Данные эксперта № 4

		Уязвимости																		
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
Угрозы	**1**	1	1	1	1	1	0	1	1	0	1	1	0	0	0	1	1	1	0	1
	2	0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	1	1
	3	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	1	1	1
	4	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1
	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	6	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0
	7	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	8	0	0	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0

Определение ценности информационных ресурсов

Сформирован перечень защищаемых информационных ресурсов:

1) лицензионные копии установочного ПО;
2) БД 1С;
3) документы в бумажном виде;
4) документы в электронном виде;
5) ключ-дискета для казначейской системы электронного документооборота.

Вектор ценности информационных ресурсов построен по таблице 1.5 (здесь и далее приведены сведения только эксперта № 1).

1	**2**	**3**	**4**	**5**
6	9	6	6	4

Далее приводится расчет показателей качества СЗИ. Он может быть произведен с использованием ПО, предназначенного для обработки табличных данных, например программы MS Excel. Также могут использоваться программы типа MathCad.

Расчет вероятностей возникновения угроз безопасности $\{p_{ij}^{B}\}$ (4.11) – (4.16) дал следующие результаты.

	Вероятности возникновения угроз								
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Эксперт 1	0,043	0,280	0,042	0,176	0,121	0,031	0,189	0,082	0,036
Эксперт 2	0,021	0,185	0,185	0,177	0,073	0,043	0,157	0,045	0,114
Эксперт 3	0,044	0,208	0,125	0,103	0,106	0,027	0,247	0,103	0,037
Эксперт 4	0,069	0,259	0,103	0,140	0,097	0,029	0,110	0,095	0,098

Степени воздействия угроз $\{h_i\}$ определены по табл. 1.4 и формулам (4.17), (4.19). Приводится только окончательный результат.

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0,192	0,235	0,116	0,038	0,018	0,341	0,040	0,020

Вектор относительной ценности ресурсов $\{\bar{c}_i\}$ построен по (4.20).

1	**2**	**3**	**4**	**5**
0,193	0,290	0,194	0,194	0,129

В качестве опорного элемента выбран 2-й ресурс (БД 1С). Его стоимость определена исходя из затрат на обслуживание:

S_{Ux} = 20 000 руб./мес. · 12 мес. = 240 000 руб.

Стоимость всех информационных ресурсов в расчете на один год S_{Ui} вычислена по (4.22).

1	**2**	**3**	**4**	**5**
160 000	240 000	160 000	160 000	107 000

Далее был составлен перечень всех элементов ИС, подверженных воздействию угроз.

1. ПК сервер 1С. Стоимость оборудования – 30 000 руб.
2. Серверная операционная система Windows 2003 Server. Затраты на восстановление при наличии установочной копии – 2 000 руб.
3. Программные средства для бухгалтерского учета (1С 7.7 Бюджет, 1С: Налогоплательщик, версия 7.7 Сетевая). Затраты на восстановление при наличии установочных копий – 1 500 руб.
4. ПК с казначейской системой электронного документооборота. Стоимость оборудования – 24 000 руб.

5. Операционная система Windows XP для ПК с казначейской системой. Затраты на восстановление при наличии установочной копии – 1 500 руб.

6. Программные средства для казначейской системы. Затраты на восстановление при наличии установочной копии – 1 000 руб.

7. Средства передачи данных (модем, концентратор). Стоимость оборудования – 2 000 руб.

8. Сейф для хранения бумажных документов, различных информационных носителей (дискет, CD- и DVD-дисков) TOPAZ BDS-900D. Стоимость сейфа – 36 000 руб.

9. Вспомогательные средства охраны. Техническое обслуживание системы охранной сигнализации (при заключении годового договора на ТО) – 1 500 руб.

10. Вспомогательные средства пожарной сигнализации. Техническое обслуживание системы пожарной сигнализации (при заключении годового договора на ТО) – 2 500 руб.

11. Проводной телефон. Стоимость аппарата – 700 руб.

12. Системы контроля доступа посетителей в помещение – видеодомофон Commax DPV-4KE. Состоит из видеомонитора, установленного внутри помещения, и вызывной панели домофона, которая крепится рядом с входной дверью. Стоимость оборудования – 2 200 руб.

Стоимость элементов ОИ, подверженных воздействию угроз, $S_{ОИk}$, их срок службы и стоимость в расчете на один год представлены ниже.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Стоимость	30000	2000	1500	24000	1500	1000	2000	36000	1500	2500	700	2200
Срок службы	5	3	1	5	2	0,5	5	12	1	1	10	5
Стоимость на 1 год	6000	667	1500	4800	750	2000	400	3000	1500	2500	70	440

Далее был составлен перечень элементов СЗИ и мероприятий по поддержанию ИБ и определена их стоимость $S_{СЗИi}$ в расчете на один год.

1. Расходы на программные средства ЗИ (антивирус – 4 шт. по 1 000 руб., приобретается на один год).

2. Проведение анализа рисков информационной безопасности (6 000 руб. в год).

3. Приобретение средств обработки информации взамен пришедших в негодность (20 000 руб. в год).

4. Утилизация средств, пришедших в негодность (1 000 руб. в год).

5. Техническая поддержка персонала при внедрении средств и процедур ЗИ (6 000 руб. в год).

6. Решение основных задач по обеспечению информационной безопасности дополнительными средствами в сочетании со штатными средствами ОС (12 000 руб. в год).

7. Учебные курсы («Технология обеспечения информационной безопасности», «Сетевая безопасность», «Безопасность сетевых операционных систем» и др.) (12 000 руб. в год).

8. Контроль событий, связанных с нарушением работоспособности компонентов СЗИ (6 000 руб. в год).

9. Обслуживание и настройка программно-технических средств защиты, ОС и сетевого оборудования (1 000 руб. в месяц).

10. Поддержание системы резервного копирования и ведения архива данных (1 000 руб. в месяц).

11. Удовлетворение субъективных требований пользователей, помощь и обучение (1 000 руб. в месяц).

12. Восстановление баз данных и прочих информационных массивов (2 000 руб. в месяц).

13. Анализ политики безопасности предприятия (1 000 руб. в месяц).

14. Работа с системными журналами (журналы регистрации Windows и журналы регистрации Secret Net) (1 000 руб. в месяц).

15. Управление разграничением доступа пользователей к ресурсам (500 руб. в месяц).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
4000	6000	20000	1000	6000	12000	12000	6000	12000	12000	12000	24000	12000	12000	6000

Аудит степени выполнения требований к СЗИ

Был составлен перечень количественных требований к СЗИ с их оптимальными значениями:

1) количество камер видеонаблюдения, оптимальное значение – 3;

2) регулярность резервирования данных, оптимальное значение – 24 раза в год;

3) количество источников бесперебойного питания для компьютеров, обрабатывающих защищаемую информацию, оптимальное значение – 4;

4) регулярность полного сканирования данных на наличие вредоносных программ, оптимальное значение – 48 раз в год;

5) количество датчиков пожарной сигнализации, оптимальное значение – 14;

6) количество решеток на окнах первого этажа, оптимальное значение – 10;

7) количество сейфов для хранения документов и информационных носителей, оптимальное значение – 3.

Путем анализа реального положения были получены нормированные значения степени выполнения количественного требования для устранения угрозы $\bar{x}_{iq}$ (*заполнены только ячейки для требований, имеющих отношение к устранению данной угрозы; в остальных ячейках – значение 0*). Нормирование проведено по формулам (4.25) – (4.27).

	Количественные требования, (q)							
		1	**2**	**3**	**4**	**5**	**6**	**7**
Угрозы, (i)	**1**	0,33	0,04	0	0	0	0,90	0,33
	2	0	0,04	0,33	0,23	0,57	0	0,33
	3	0	0,04	0	0,23	0	0	0
	4	0	0	0,33	0	0	0	0
	5	0,33	0	0	0	0,57	0	0
	6	0	0,04	0,33	0,23	0,57	0,90	0
	7	0,33	0	0	0	0	0,90	0
	8	0,33	0	0	0	0	0	0

Также был составлен перечень характеристик СЗИ, от которых зависит выполнение качественных требований:

1) финансирование диагностики; регулярность проверок работоспособности оборудования;

2) финансирование устранения неполадок или приобретения нового средства;

3) регулярность резервирования информации;

4) наличие антивирусных программ в сети организации;

5) аудит доступа к ресурсам;

6) своевременное оповещение о начавшейся нештатной ситуации;

7) обучение персонала, финансирование курсов, тренингов и т.д.

Был составлен перечень качественных требований к СЗИ с указанием характеристик, от которых зависит их выполнение:

1) поддержка целостности БД 1С (зависит от 3, 4, 5, 6);

2) поддержка работоспособности оборудования: диагностика, устранение неполадок (зависит от 1, 2, 6);

3) своевременное выявление фактов НСД, утечки информации, ее хищения (зависит от 5, 6);

4) поддержка работоспособности сети передачи данных (зависит от 1, 2, 4, 6);

5) регулярная работа с персоналом (обучение, ознакомление с инструкциями, помощь и др.) (зависит от 7);

6) надежная работа охранной, пожарной сигнализаций, системы контроля доступа (зависит от 1, 2, 6).

В результате аудита определены степени соответствия каждой характеристики СЗИ выполнению каждого качественного требования $Y_q = \{y_1, y_2, ..., y_p\}$.

		Степени соответствия, (p)						
		1	**2**	**3**	**4**	**5**	**6**	**7**
Требования, (q)	**1**	-	-	0,08	0,15	0	0,2	-
	2	0,10	0,30	-	-	-	0,08	-
	3	-	-	-	-	0	0,08	-
	4	0,05	0,10	-	0,15	-	0,20	-
	5	-	-	-	-	-	-	0,05
	6	0,05	0,20	-	-	-	0,10	-

Степени влияния характеристик на выполнение требования в целом $\Sigma_q = \{\sigma_1, \sigma_2, ..., \sigma_p\}$ проставлены непосредственно.

		Степени влияния, (p)						
		1	**2**	**3**	**4**	**5**	**6**	**7**
Требования, (q)	**1**	-	-	0,22	0,12	0,17	0,49	-
	2	0,31	0,50	-	-	-	0,19	-
	3	-	-	-	-	0,57	0,43	-
	4	0,17	0,33	-	0,50	-	-	-
	5	-	-	-	-	-	-	1,00
	6	0,17	0,50	-	-	-	0,33	-

Степени выполнения качественных требований для устранения угрозы x_{iq} (*заполняются только ячейки для требований, имеющих*

отношение к устранению данной угрозы; в остальных ячейках – значение 0) рассчитаны по формуле (4.31). Было также сделано допущение, что степень выполнения требования одинакова для каждой угрозы, которую оно перекрывает.

	Качественные требования, (q)						
		1	2	3	4	5	6
Угрозы, (i)	1	0	0	0,057	0	0,050	0,142
	2	0,251	0,196	0,057	0,117	0	0
	3	0,251	0	0,057	0,117	0	0
	4	0,251	0,196	0	0,117	0	0,142
	5	0,251	0,196	0	0	0,050	0,142
	6	0	0	0,057	0	0	0,142
	7	0	0,196	0	0	0	0,142
	8	0	0,196	0,057	0	0,050	0

Весовые коэффициенты значимости количественных и качественных требований для устранения угроз v_{iq} так же, как и степени влияния характеристик, проставлены непосредственно.

		Требования, (q)												
		количественные							качественные					
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Угрозы, (i)	**1**	0,09	0,09	0,09	-	-	0,11	0,27	0,09	-	0,11	0,03	0,05	0,07
	2	0,14	0,07	0,12	0,07	-	-	0,12	0,14	0,12	0,12	0,04	0,02	0,04
	3	-	0,16	0,14	0,31	0,07	-	-	0,11	-	0,05	0,11	-	0,05
	4	-	-	0,15	-	0,11	-	-	0,11	0,30	-	0,28	0,05	-
	5	0,12	-	-	-	0,35	-	-	-	-	0,16	-	0,21	0,16
	6	-	0,10	0,10	0,12	0,10	0,12	0,24	0,10	-	-	-	0,05	0,07
	7	0,27	-	-	-	-	0,43	-	-	-	-	-	0,12	0,18
	8	0,30	-	-	-	-	-	-	-	0,12	0,16	-	0,22	0,20

Вероятности устранения угроз безопасности $\left\{ p_i^Y \right\}$ рассчитаны по (4.32).

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0,240	0,168	0,121	0,169	0,272	0,240	0,502	0,143

По результатам экспертизы вероятностей возникновения угроз безопасности рассчитаны максимальные собственные числа $\lambda_{\max}^j$, коэффициенты рассогласования K_P^j матриц парных сравнений значимо-

сти уязвимостей ИС (1.8), уточнены коэффициенты авторитета $\Delta\nu_j$ (4.35) и скорректированы коэффициенты ν_j (4.36) для всех экспертов.

Общие характеристики	Эксперты			
	1	2	3	4
Первичный коэффициент авторитета	0,4	0,2	0,2	0,2
Max собственное число матрицы	34,5	26,5	23,8	23,4
Коэффициент рассогласования	0,86	0,42	0,27	0,28
Уточнение коэффициента авторитета	0,42	0,26	0,29	0,30
Скорректированный коэффициент	0,33	0,20	0,23	0,24

Также определены агрегированные значения вероятностей возникновения угроз безопасности $\left\{ p_i^B \right\}$ (2.24), (2.26), (4.37).

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0,11	0,23	0,11	0,11	0,10	0,02	0,18	0,10	0,04

Итоговые показатели качества СЗИ подсчитаны по формулам (4.4) – (4.7).

Показатель	Значение
Риск для незащищенной системы, руб.	154 300
Риск для защищенной системы, руб.	120 000
Стоимость СЗИ, руб.	157 000
Экономическая эффективность	0,22
Коэффициент защищенности	0,23

Выводы по результатам экспертизы и аудита

СЗИ исследуемого предприятия оказалась экономически неэффективной – эффект от вложения средств в СЗИ (снижение риска) меньше затрат на его достижение в 4,6 раза.

Защищенность, т.е. вероятность успешного противостояния любой угрозе, составляет в целом 23 %, что вызвано крайне низкой степенью выполнения требований стандартов ИБ и, как следствие, малой вероятностью устранения угроз.

Совершенствование данной системы возможно посредством повышения степени выполнения требований стандартов безопасности, что в разумных пределах даст незначительное увеличение расходов на СЗИ по сравнению со стоимостью информационных ресурсов.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ*

1. *Анин, Б. Ю.* Защита компьютерной информации / Б. Ю. Анин. – СПб. : БХВ-Петербург, 2000. – 376 с. – ISBN 5-8206-0104-1.

2. *Барсуков, В. С.* Безопасность: технологии, средства, услуги / В. С. Барсуков. – М. : Кудиц-Образ, 2001. – 500 с. – ISBN 5-93378-017-0.

3. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий : руководящий док. Гостехкомиссии России от 19.06.2002 г. № 187. – М. : Воен. изд-во, 2001.

4. *Водолазкий, В. В.* Современные технологии безопасности / В. В. Водолазкий. – М. : Нолидж, 2000. – 496 с. – ISBN 5-89251-073-5.

5. ГОСТ Р ИСО/МЕК 15408-1-2001. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.

6. ГОСТ Р ИСО/МЕК 15408-2-2001. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности.

7. Защита от несанкционированного доступа к информации. Термины и определения : руководящий док. Гостехкомиссии России от 30.03.1992 г. – М. : Воен. изд-во, 1992.

8. Защита программ и данных : учебник / П. Ю. Белкин [и др.]. – М. : Радио и связь, 1999. – 188 с. – ISBN 5-256-01533-8.

9. *Конеев, И. Р.* Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 752 с. – ISBN 5-94157-280-8.

10. Организация и современные методы защиты информации / под общ. ред. С. А. Диева, А. Г. Шаваева. – М. : Банк. деловой центр, 1998. – 472 с. – ISBN 5-89280-022-9.

11. *Панкова, Л. А.* Организация экспертизы и анализ экспертной информации / Л. А. Панкова, А. М. Петровский, М. В. Шнейдерман. – М. : Наука, 1984. – 120 с.

* Приводится в авторской редакции.

12. *Петраков, А. В.* Основы практической защиты информации / А. В. Петраков. – М. : МТУСИ, 2001. – 360 с. – ISBN 5-256-01592-2.

13. Положение по аттестации объектов информатизации по требованиям безопасности информации : руководящий док. Гостехкомиссии России от 25.11.1994 г. – М. : Воен. изд-во, 2000.

14. *Полянский, Д. А.* Оценка защищенности : учеб. пособие / Д. А. Полянский. – Владимир : Изд-во Владим. гос. ун-та, 2005. – 80 с. – (Комплексная защита объектов информатизации. Кн. 10). – ISBN 5-89368-613-6.

15. *Романец, Ю. В.* Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. – 376 с. – ISBN 5-256-01518-4.

16. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Термины и определения : руководящий док. Гостехкомиссии России от 30.03.1992 г. – М. : Воен. изд-во, 1992.

17. *Устинов, В. Н.* Теория вероятностей и моделирование вероятностных процессов в информационной безопасности : учеб. пособие / В. Н. Устинов, Д. А. Полянский, Ж. Ф. Таннинг, Л. М. Груздева. – Владимир : Изд-во Владим. гос. ун-та, 2005. – 80 с. – (Комплексная защита объектов информатизации. Кн. 9). – ISBN 5-89368-623-3.

18. *Хорев, А. А.* Способы и средства защиты информации / А. А. Хорев ; М-во обороны РФ. – М., 1999. – 256 с. – ISBN 5-7695-1839-1.

19. International standard ISO/IEC 15408:1999. Information technology – Security techniques – Evaluation criteria for IT security. – Part 1 – 3.

20. International standard ISO/IEC 17799:1999. Information technology – Code of practice for information security management.

21. Trusted computer system evaluation criteria (Orange Book). – Department of Defence Standart, USA, 1983.

Учебное издание

Комплексная защита объектов информатизации. Книга 16

ПОЛЯНСКИЙ Дмитрий Александрович
ФАЙМАН Ольга Игоревна

ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Подписано в печать 16.11.09.
Формат 60x84/16. Усл. печ. л. 5,58. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета.
600000, Владимир, ул. Горького, 87.