Модель комплексной оценки СЗИ

25

В этой главе

- *БлокпоказателейОСНОВЫ*
- *БлокпоказателейНАПРАВЛЕНИЯ*
- *БлокпоказателейЭТАПЫ*
- *Структура модели оценки СЗИ*
- *Методика оценки качества СЗИ на основе матрицы знаний*
- *Оценка качества СЗИ на основе анализа профиля безопасности*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Модель комплексной оценки СЗИ

Предлагается рассмотреть следующую модель создания и комплексной оценки системы защиты информации.

Модель СЗИ представлена в виде следующих основных блоков показателей:

- Блок показателей "ОСНОВЫ";
- Блок показателей "НАПРАВЛЕНИЯ";
- Блок показателей "ЭТАПЫ".

Рассмотрим содержание этих блоков.

Блок показателей ОСНОВЫ (Oi)

Проведенный анализ основных подходов к созданию СЗИ позволяет выделить следующую группу показателей:

O_1. Нормативно-правовая и научная база;

O_2. Структура и задачи органов;

O_3. Организационные меры и методы (политика безопасности);

O_4. Программно-технические способы и средства.

Значение каждого из перечисленных показателей блока "ОСНОВЫ" должно быть детализировано для конкретной ИС.

Блок показателей НАПРАВЛЕНИЯ (Hj)

Проведенный анализ существующих способов и методов защиты информации позволяет выделить следующие основные показателей создания и оценки СЗИ:

H_1. Защита объектов корпоративных систем;

H_2. Защита процессов, процедур и программ обработки информации;

H_3. Защита каналов связи;

H_4. Подавление побочных электромагнитных излучений;

H_5. Управление системой защиты.

Совершенно очевидно, что каждый из показателей блока НАПРАВЛЕНИЙ должен быть структурирован в зависимости от заданной глубины детализации СЗИ.

Блок показателей ЭТАПЫ (Mk)

В настоящее время рассматривают различные этапы построения СЗИ все они достаточно эффективны и позволяют решать поставленные задачи. На основе проведенного анализа предлагается рассмотрение следующих показателей создания СЗИ, подлежащих оценке:

M_1. Определение информации, подлежащей защите;

M_2. Выявление полного множество потенциально возможных угроз и каналов утечки информации;

M_3. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

M_4. Определение требований к системе защиты;

M_5. Осуществление выбора средств защиты информации и их характеристик;

M_6. Внедрение и организация использования выбранных мер, способов и средств защиты;

M_7. Осуществление контроля целостности и управление системой защиты.

Этапы могут быть разбиты на более детальные пункты (шаги).

Структура модели оценки СЗИ

Структура модели оценки СЗИ наглядно показана на Рис. 25.1. Она заключается в логическом объединении показателей блоков "ОСНОВЫ", "НАПРАВЛЕНИЯ" и "ЭТАПЫ" в МАТРИЦУ ЗНАНИЙ (ОЦЕНОК), состоящую из K элементов.

Пример МАТРИЦЫ ЗНАНИЙ (ОЦЕНОК) в виде таблицы (массива) показателей наглядно представлен на Рис. 25.2.

В общем случае количество элементов "матрицы" может быть определено из соотношения

$$K = O_i \cdot H_j \cdot M_k$$

На основе проведенного выше анализа в данном варианте (при условии, что $O_i = 4$, $H_j = 5$, $M_k = 7$) общее количество элементов "матрицы" составляет

$$K = 4 \cdot 5 \cdot 7 = 140.$$

Следует обратить внимание на содержание обозначения каждого из элементов матрицы, который формируется из совокупности трех частных показателей:

Первое знакоместо обозначает номер показателя "ЭТАПЫ", второе знакоместо – номер показателя "НАПРАВЛЕНИЯ", а третье знакоместо – номер показателя "ОСНОВЫ".

На Рис. 25.3. представлен пример, элемента матрицы 321, который формируется с учетом следующих показателей:

3 – Проведение оценки уязвимости и рисков (показатель № 3 блока "ЭТАПЫ");

2 – Защита процессов и программ (показатель № 2 блока "НАПРАВЛЕНИЯ")

1 – Нормативная база (показатель № 1 блока "ОСНОВЫ")

В зависимости от этапов работ по созданию СЗИ "матрица" имеет различное содержание. Другими словами это несколько одинаковых по структуре, но разных по содержанию "матриц", а именно:

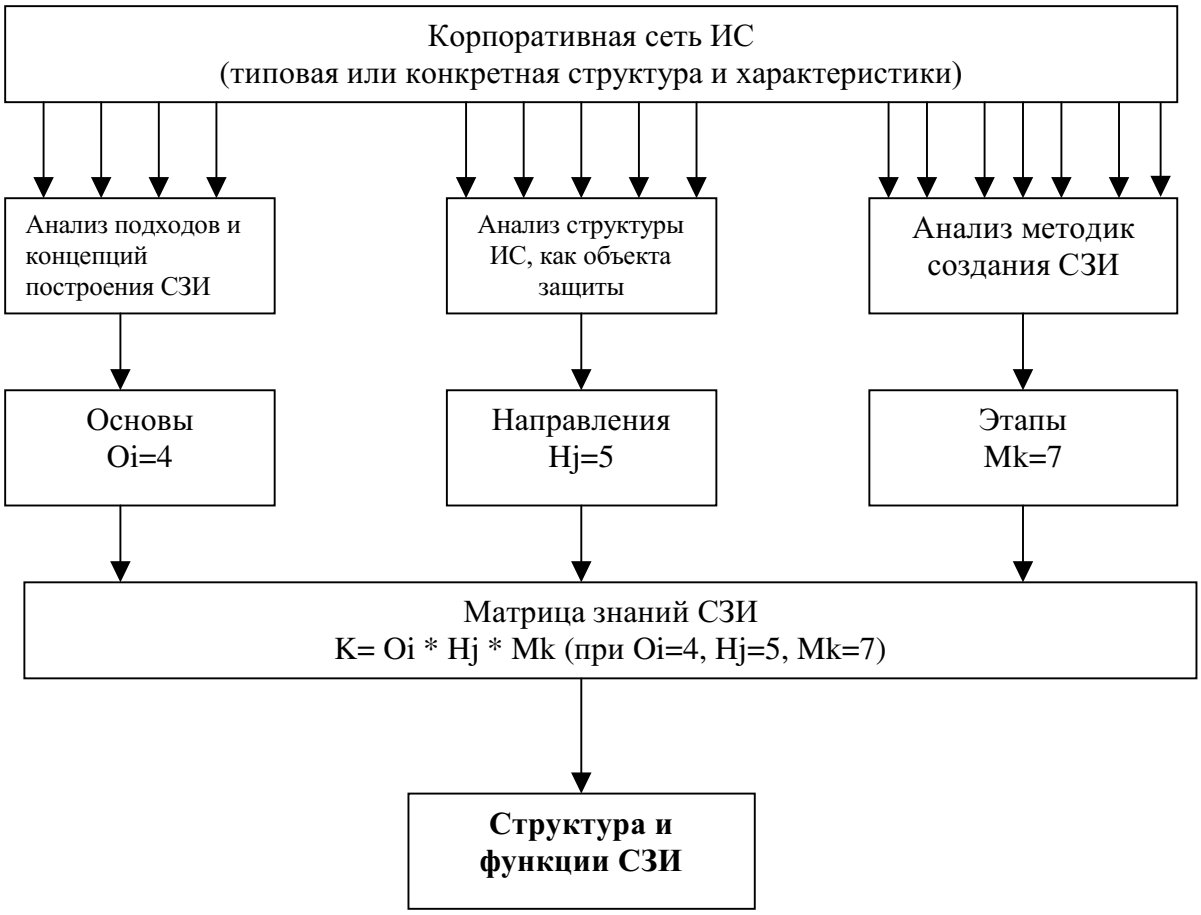


РИС. 25.1 *Структура модели оценки СЗИ*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИС. 25.2. *Пример МАТРИЦЫ ЗНАНИЙ (ОЦЕНОК)*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИС. 25.3. *Пример элемента матрицы 321*

1. "Матрица" полноты и качества состояний элементов СЗИ;

2. "Матрица" требований к СЗИ;

3. "Матрица" оценок эффективности функционирования элементов СЗИ.

Могут рассматриваться и другие функции этой же "матрицы", главное чтобы содержание каждого из элементов "матрицы" описывало взаимосвязь составляющих создаваемой СЗИ.

Оценки могут формироваться по различным группам элементов матрицы, в зависимости от целей проверки.

Например отдельно можно оценить качество документации, защищенность каналов связи, качество мероприятий по выявлению угроз и каналов утечки информации. Некоторые варианты частных оценок показаны на Рис.25.4. и Рис.25.5.

Основным содержанием "Матрицы полноты и качества" является вопрос "Какие из мероприятий по защите информации и в каком объеме уже выполнены?"

"Матрица требований" содержит вопрос "Какой должна быть создаваемая СЗИ?" и позволяет представить облик создаваемой СЗИ, а также сформулировать требования к ней.

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИС.25.4. *Вариант частных оценок защищенности каналов связи*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИС.25.5. *Вариант частных оценок качества выявления угроз*

"Матрица оценок" позволяет определить эффективность проводимых мероприятий по защите информации, задавая вопрос "Правильно ли строится СЗИ?" При этом используются все существующие методики оценки эффективности функционирования СЗИ.

На Рис.25.6. приведены вопросы "Матрицы полноты и качества" для элементов № 321, 322, 323, 324, которые объединяют показатель № 3 блока "ЭТАПЫ", показатель № 2 блока "НАПРАВЛЕНИЯ" и показатели № 1, 2, 3, 4 блока "ОСНОВЫ":

Элемент № 3.2.1 Насколько полно отражены в законодательных, нормативных и методических документах вопросы, определяющие порядок проведения оценки уязвимости и рисков для информации используемой в процессах и программах конкретной ИС?

Элемент № 3.2.2 Имеется ли структура органов (сотрудники), ответственная за проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?

Элемент № 3.2.3 Определены ли режимные меры, обеспечивающие своевременное и качественное проведение оценки уязвимости и рисков для информации используемой в процессах и программах ИС?

Элемент № 3.2.4 Применяются ли технические, программные или другие средства, для обеспечения оперативности и качества проведение оценки уязвимо-

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

РИС.25.6. *"Матрица полноты и качества" для элементов № 321, 322, 323, 324.*

сти и рисков для информации используемой в процессах и программах ИС?

В общем случае для "Матрицы экспертных оценок" формируется 140 вопросов (по числу ее элементов). Ответы на эти вопросы позволяют составить полное представление о СЗИ и оценить достигнутый уровень защиты.

Полный перечень 140 вопросов изложен в Приложение А.

Показатель уровня защиты СЗИ предлагается определять методом экспертных оценок, используя положения теории нечеткой логики и нечетких утверждений.

Напомним, что структура модели оценки представлена на Рис.25.1, а логическое дерево для расчета обобщенного и частных показателей уровня защиты СЗИ представлено на Рис 25.7.

Величина обобщенного показателя уровня защиты определяется на основе частных показателей путем сравнения заданных профилей безопасности с достигнутыми. Заданный профиль, услуги и механизмы безопасности определяются заказчиком или выбираются в соответствии с принятыми “Критериями безопасности” (например Федеральные, Канадские, Общие Критерии, НД ТЗИ 2.5-004-99 или другие) в зависимости от требований, которые устанавливаются к создаваемой СЗИ.

Уровень достигнутого профиля защиты определяется экспертным путем в соответствии с теми же критериями оценки защищенности.

Методика оценки качества СЗИ на основе матрицы знаний

Качество СЗИ определяется степенью (полнотой) выполнения требований, предъявляемых к СЗИ. В основу оценки качества СЗИ положим исходные данные, представленные в виде матрицы знаний, заполняемой экспертами.

Заполнение матрицы знаний осуществляется на основе лингвинистических (интервальных) оценок отдельных элементов.

Особенностью частных показателей является то, что все они имеют качественный характер, т.е. не имеют точного количественного измерения. Поэтому при оценке одного и того же показателя несколькими экспертами могут возникать разные мнения. Кроме того эксперт не всегда способен словесно оценить частный показатель, хотя интуитивно ощущает его уровень. Для преодоления этих трудностей можно оценивать частные показатели по принципу термометра (рис. 25.a).

Удобство такого подхода состоит в том, что разные по смыслу частные показатели определяются как лингвинистические переменные, заданные на едином универсальном множестве $U = \left[\underline{u}, \overline{u}\right]$ которым является шкала термометра.

Оценка частных показатели по принципу термометра дает возможность использовать в качестве показателя оценки СЗИ аддитивный показатель, который для количественной оценки качества СЗИ позволяет определить количество выполненных частных показателей. В этом случае показатель качества имеет вид

$$Q = \frac{\sum_{k=1}^{5}\sum_{j=1}^{4}\sum_{i=1}^{7} z_{kji}}{140}, \qquad (25.\text{А})$$

где $z_{kji} = \begin{cases} 1, \text{если } q_{kji} > q_{kji}^{T}, \\ 0, \text{если } q_{kji} < q_{kji}^{T}. \end{cases}$, q_{kji} и q_{kji}^{T} – действительное и заданное значение частных показателей соответственно.

Оценка качества СЗИ имеет вид

$$Q = \sum_{i=1}^{m} \omega_i q_i \ . \qquad (25.\text{Б})$$

Однако большое количество элементов матрицы знаний (m = 140) может привести к потере объективности определения весовых коэфициентов. Поэтому более перспективным путем является задание весовых коэфициентов столбцов, строк и направлений матрицы знаний

$$Q = \sum_{k=1}^{5} \omega_k \sum_{j=1}^{4} \omega_j \sum_{i=1}^{7} \omega_i q_{kji} \ , \qquad (25.\text{В})$$

где $\sum_{k=1}^{5} \omega_k = 1$, $\sum_{j=1}^{4} \omega_j = 1$, $\sum_{i=1}^{7} \omega_i = 1$.

Графическое представление степени выполнения требований приведено на рисунке 25.b.

Определение принадлежности СЗИ к конкретному классу проводится на основе функции принадлежности, заданной нечеткими термами классов. Результатом оценки будет вероятность принадлежности СЗИ к конкретному классу.

Рассмотрим возможные варианты представления экспертных знаний и соответствующие им методики расчета показателя качества СЗИ.

Вариант 1.а. Степень выполнения каждого требования определяется как:

- требование выполнено $X_j = 1$;
- требование не выполнено $X_j = 0$, $j = 1, m$.

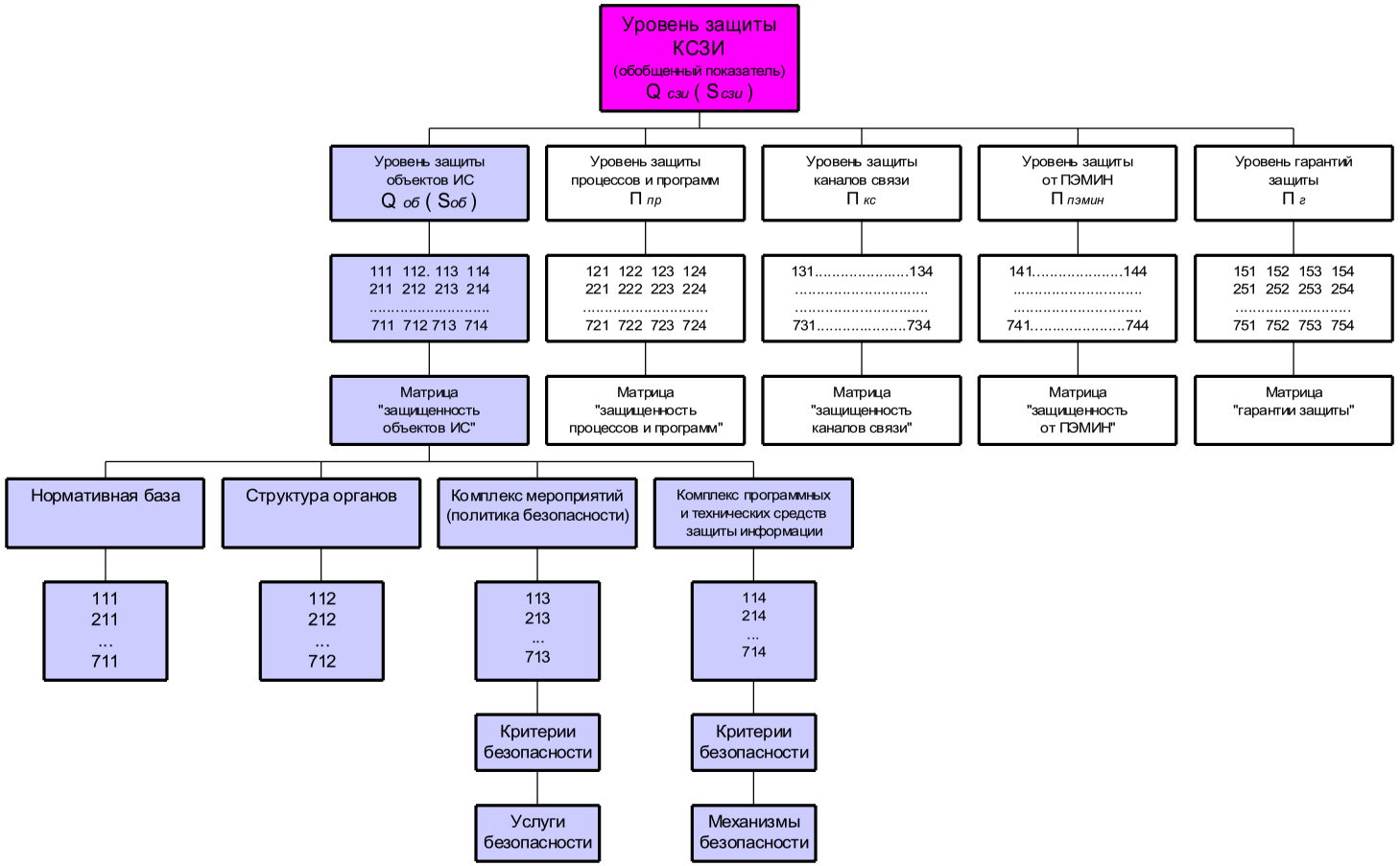


РИС. 25.7. *Логическое дерево вывода оценки уровня защищенности ИС*

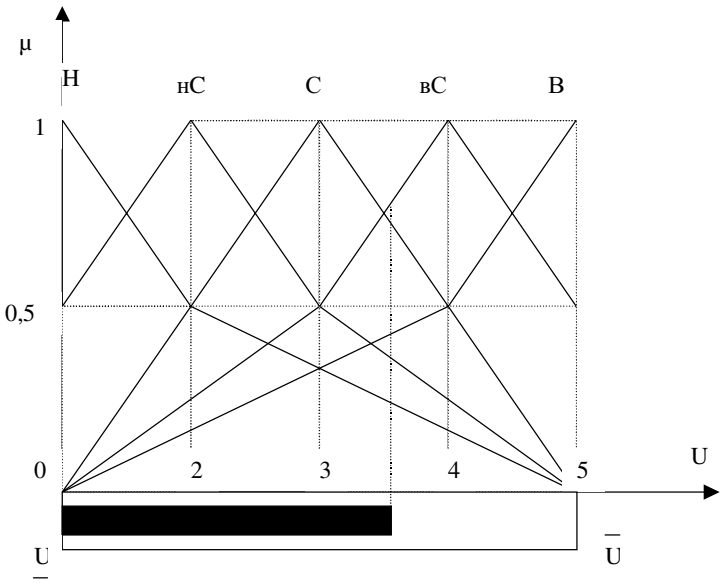


РИС. 25.a.
Оценка частных показателей по принципу термометра

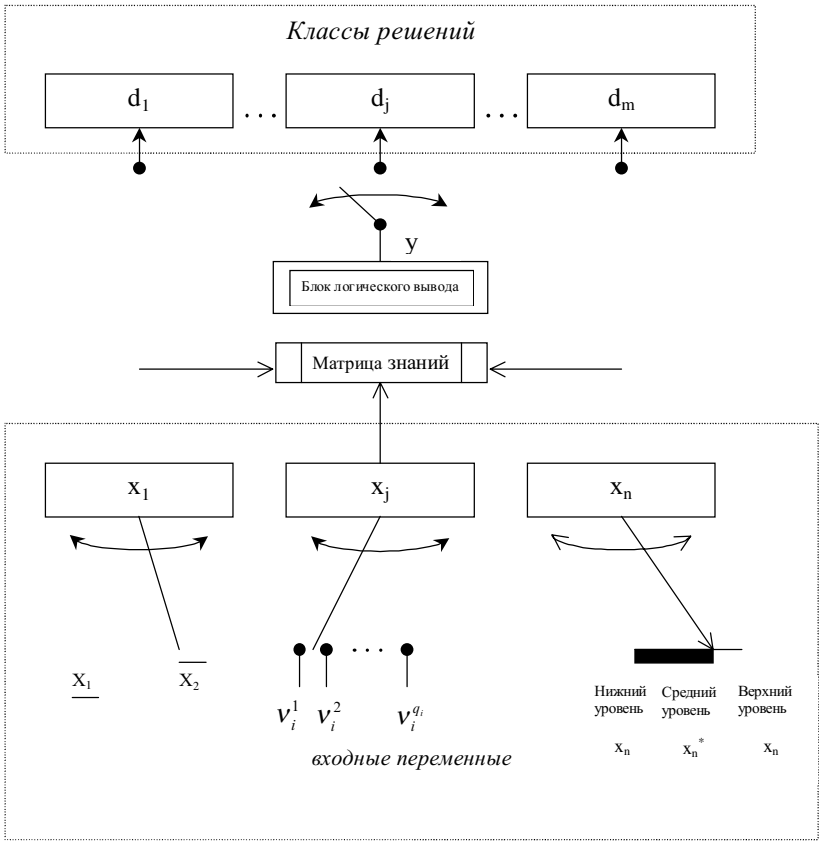


РИС. 25.b.
Схема апроксимации для объекта с дискретным выходом

Важность выполняемых требований не учитывается.

Тогда качество СЗИ оценивается соотношением:

$$W = \frac{\sum_{j=1}^{m} X_j}{m};\ 0 \le W \le 1 \qquad (25.1.)$$

Вариант 1.б. Степень выполнения с учетом важности требований

Важность выполнения каждого требования, определяемое экспертным путем, учитывается. Тогда качество СЗИ оценивается соотношением:

$$W = \sum_{j=1}^{m} a_j x_j;\ 0 \le W \le 1 \qquad (25.2.)$$

где $0 \le a \le 1;\ \sum_{j=1}^{m} a_j = 1$.

Вариант 2.а. Степень выполнения требований оценивается по бальной шкале.

Например, в наиболее распространенной 5-ти бальной шкале:

B_j = 5 − отлично

B_j = 4 — хорошо

B_j = 3 — удовлетворительно

B_j = 2 − не удовлетворительно

B_j = 1 − весьма не удовлетворительно

С точки зрения степени удовлетворения требований бальную оценку можно интерпретировать следующим образом:

Отлично − СЗИ полностью удовлетворяет требованиям;

Хорошо − почти удовлетворяет;

Удовлетворительно — удовлетворяет в основном;

Не удовлетворительно − не удовлетворяет;

Весьма не удовлетворительно − полностью не удовлетворяет.

Качество СЗИ оценивается средним баллом.

$$\overline{B} = \frac{\sum_{j=1}^{m} b_j}{m};\ 1 \le \overline{B} \le 5,\ j = 1,\overline{m} \qquad (25.3)$$

Вариант 2.б. Степень выполнения требований оценивается по бальной шкале, дополнительно определяется важность каждого требования

Тогда качество СЗИ определяется из выражения:

$$\overline{B} = \sum_{j=1}^{m} a_j b_j;\ 1 \le \overline{B} \le 5 \qquad (25.4)$$

где $0 \le a \le 1;\ \sum_{j=1}^{m} a_j = 1$.

Шкала соответсвия

Очень часто при бальной оценке степени выполнения требований удобно итоговую оценку иметь в шкале от 0 до 1 ($0 < Q < 1$).

Тогда надо сформировать шкалу соответствия $B \sim Q$;

$B_j \sim Q_j$

$J = 1,m.$

$b_j \sim q_j;\ j = 1,\overline{m}.$ (25.4.а)

Образец такой шкалы соответствия приведен в Таблице 25.3.

Оценка качества СЗИ производится по формулам аналогичным (25.3) и (25.4).

$$Q = \frac{\sum_{j=1}^{m} q_j}{m}; \qquad (25.5)$$

$$Q = \frac{\sum_{j=1}^{m} a_j q_j}{m} \qquad (25.6)$$

Таблица 25.3.

Бальная оценка	*Лингвистическая оценка*	*Интервальная оценка*
5 − отлично	(В) Полностью удовлетворяет требованиям	0,9 — 1
4 — хорошо	(ВС) Почти удовлетворяет	0,7 − 0,9
3 — удовлетворительно	(С) Удовлетворяет в основном	0,5 − 0,7
2 − не удовлетворительно	(НС) Не удовлетворяет	0,3 − 0,5
1 − весьма не удовлетворительно	(Н) Полностью не удовлетворяет	0 − 0,3

Лингвистическая переменная

Пусть лингвистическая переменная “Качество СЗИ” определена на универсальном множестве вариантов СЗИ

$$u_i;\ i=1,\overline{n} \qquad (*1)$$

Уровень качества СЗИ будем оценивать термами (В, ВС, С, НС, Н), приведенными в табл. 25.3.

Пусть далее экспертным путем одним из методов, описанных в главе 6, получены функции принадлежности

$$\mu(u_{ij}) \qquad (*2),$$

Тогда, используя функции принадлежности с помощью табл. 25.3. Можно получить оценку качества СЗИ либо в виде оценки:

$$B_i = \frac{\sum_{j=1}^{m} B_{ij}}{m} = \frac{\sum_{j=1}^{m}\sum_{b_j=1}^{5} b_j \mu(u_i b_j)}{m}; \qquad (25.7)$$

$$B_i = \sum_{j=1}^{m} \alpha_j \sum_{b_j=1}^{5} b_j \mu(u_i b_j). \qquad (25.8)$$

Оценка качества СЗИ на основе анализа профиля безопасности

Под профилем безопасности в дальнейшем будем понимать графическое представление степени выполнения требований в системе координат:

по горизонтали – перечень требований, предъявляемых к СЗИ;

по вертикали – степень выполнения каждого требования.

Степень выполнения каждого требования рассчитывается в соответствии с формулами (25.1)...(25.10).

Рассмотрим частный (наиболее удобный с нашей точки зрения) случай, когда степень выполнения требований задается в шкале $0 < Q < 1$; $J = 1,m$.

При этом целесообразно рассматривать два профиля безопасности: требуемый и реально достигнутый.

Для построения требуемого профиля безопасности используются предварительно заданные экспертами значения

$$0 \le Q_j^{TP} \le 1;\ j=1,m. \qquad (*3).$$

Исходные данные для построения требуемого профиля безопасности представлены в виде уже знакомой матрицы знаний.

Пример оценки качества СЗИ

Как указывалось ранее, качество СЗИ определяется степенью (полнотой) выполнения требований к СЗИ. Исходные данные, представлены в виде частных матриц знаний, заполненных экспертами по соответствующим направлениям защиты (рис. 25.8–25.12).

На рис. 25.8 представлены данные для оценки ***защищенности объектов ИС*** (первое направление защиты). Поясним используемые обозначения:

- Номер этапа с 1 по 7 (см. блок показателей “Этапы”).
- Перечень показателей (*m)* для соответствующих элементов матрицы (от 1 до 28*)*.
- Коэффициенты важности (a_j), которые определяются для показателей каждого из этапов.
- Показатели требуемого профиля безопасности (*Qmp*). Для всех показателей установлено значение 0,65. Графически требуемый профиль изображен на диаграмме "Сравнение профилей защиты" (рис. 25.8) в виде прямой линии на уровне 0,65.
- Показатели достигнутого профиля безопасности ($Q_д$). Их значения определены экспертами и графически изображены на диаграмме "Сравнение профилей защиты" в виде ломанной линии.
- Показатели достигнутого профиля безопасности с учетом коэффициентов важности ($Q_{даj}$).

Сравнение профилей ($S_{пр}$), которое производится следующим образом:

- ($S_{пр}$) = 1 — если значение показателя достигнутого профиля безопасности равно или превышает значение показателя заданного;
- ($S_{пр}$) = 0 — если значение показателя достигнутого профиля безопасности ниже значение показателя заданного.

Графически этот процесс представлен на диаграмме "Оценка достигнутого профиля безопасности" (рис. 25.8).

Степень выполнения групп требований ($Q_{груп}$) в данном примере определяется с учетом коэффициентов важности ($Q_{даj}$) для каждого из этапов: 1 – 0,68, 2 – 0,65, 3 – 0,60, 4 – 0,80, 5 – 0,80, 6 – 0,65, 7 – 0,80. Графически эти значения изображены на диаграмме "Оценка этапов" (рис. 25.8).

Качественная оценка (Q) определяется исходя из значений показателей ($Q_{груп}$), вычисленных для соответствующих этапов. В нашем случае

$$Q = 0{,}71;$$

Количественная оценка (S) определятся путем подсчета значений ($S_{пр}$), а именно нулей и единиц полученных при сравнении профилей. Это более грубая оценка, определяющая количество выполненных (достигнутых) требований.

$$S = 0{,}68$$

Другими словами в рассматриваемой ИС выполнено 68% требований по защите информации. Правда не известно насколько эти требования важны.

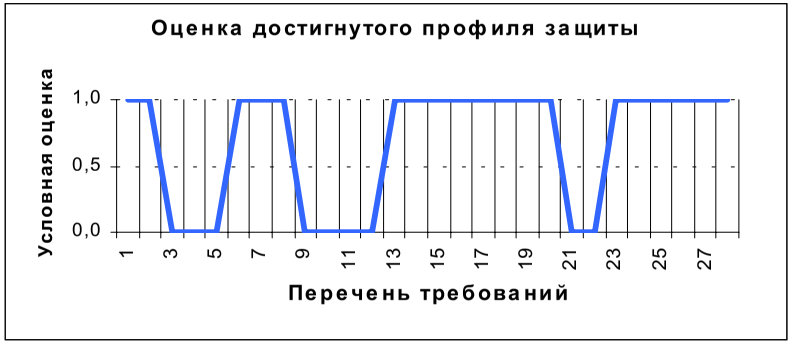
Аналогичным образом производится оценка для других направлений защиты. Результаты представлены на рисунках 25.9−25.12.

Далее, объединив частные показатели (по направлениям) в обобщенный показатель, получаем результирующий профиль безопасности и его графическое изображение (рис. 25.13). Обратите внимание на то, что требования 11, 12, 21 и 22 не выполнены вообще ни в одном из направлений защиты. Требования 1, 3,4,5,9,10 и др. выполнены не по всем направлениям. Определить какие группы требований по каким направлениям выполнены можно с помощью диаграммы (рис. 25.14)

Обобщенные показатели уровня защищенности (качественный и количественный) представлены на рис. 25.15. Превышение величины качественного показателя над количественным, свидетельствует о том, что выполненные требования более важны по своему значению чем невыполненные.

На рисунках 25.16 и 25.17 представлены матрицы количественных и качественных оценок уровня защищенности, позволяющие наглядно оценить степень выполнения требований по защите информации. Это дает возможность определить сильные и слабые места в СЗИ.

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qд x aj	Сравнение профилей	Степень выполнения групп требований	Качественная оценка	Количественная оценка
	m	№	a_j	$Q_{тр}$	Qд	$Q_{даj}$	$S_{пр}$	$Q_{груп}$	Q	S
1	1	111	0,5	0,65	0,7	0,35	1	0,68		
	2	112	0,2	0,65	0,8	0,16	1			
	3	113	0,15	0,65	0,5	0,075	0			
	4	114	0,15	0,65	0,6	0,09	0			
2	5	211	0,5	0,65	0,5	0,25	0	0,65		
	6	212	0,2	0,65	0,8	0,16	1			
	7	213	0,15	0,65	0,8	0,12	1			
	8	214	0,15	0,65	0,8	0,12	1			
3	9	311	0,25	0,65	0,6	0,15	0	0,60		
	10	312	0,25	0,65	0,6	0,15	0			
	11	313	0,25	0,65	0,6	0,15	0			
	12	314	0,25	0,65	0,6	0,15	0			
4	13	411	0,5	0,65	0,8	0,4	1	0,80	**0,71**	**0,68**
	14	412	0,2	0,65	0,8	0,16	1			
	15	413	0,15	0,65	0,8	0,12	1			
	16	414	0,15	0,65	0,8	0,12	1			
5	17	511	0,25	0,65	0,8	0,2	1	0,80		
	18	512	0,25	0,65	0,8	0,2	1			
	19	513	0,25	0,65	0,8	0,2	1			
	20	514	0,25	0,65	0,8	0,2	1			
6	21	611	0,25	0,65	0,5	0,125	0	0,65		
	22	612	0,25	0,65	0,5	0,125	0			
	23	613	0,25	0,65	0,8	0,2	1			
	24	614	0,25	0,65	0,8	0,2	1			
7	25	711	0,5	0,65	0,8	0,4	1	0,80		
	26	712	0,2	0,65	0,8	0,16	1			
	27	713	0,15	0,65	0,8	0,12	1			
	28	714	0,15	0,65	0,8	0,12	1			



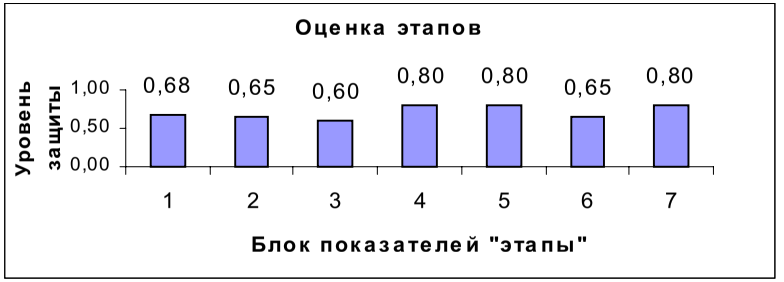
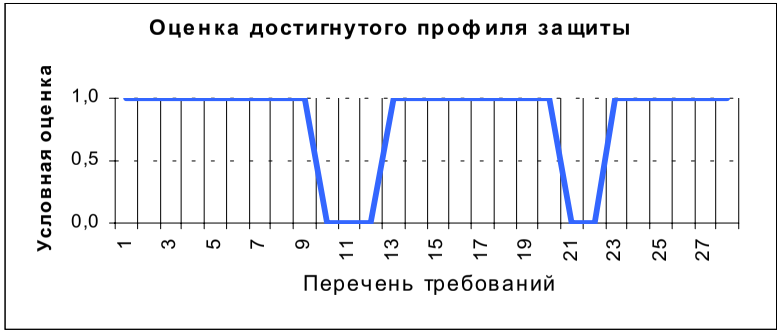


РИС. 25.8. *Оценка защищенности объектов ИС*

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qд x aj	Сравнение профилей	Степень выполнения групп требований	Качественная оценка	Количественная оценка
	m	№	a_j	$Q_{тр}$	Qд	$Q_{даj}$	$S_{пр}$	$Q_{груп}$	*Q*	*S*
1	1	121	0,5	0,7	0,9	0,45	1	0,90		
	2	122	0,2	0,7	0,9	0,18	1			
	3	123	0,15	0,7	0,9	0,135	1			
	4	124	0,15	0,7	0,9	0,135	1			
2	5	221	0,25	0,7	0,9	0,225	1	0,90		
	6	222	0,25	0,7	0,9	0,225	1			
	7	223	0,25	0,7	0,9	0,225	1			
	8	224	0,25	0,7	0,9	0,225	1			
3	9	321	0,25	0,7	0,9	0,225	1	0,68		
	10	322	0,25	0,7	0,6	0,15	0			
	11	323	0,25	0,7	0,6	0,15	0			
	12	324	0,25	0,7	0,6	0,15	0			
4	13	421	0,25	0,7	0,8	0,2	1	0,80	**0,79**	**0,82**
	14	422	0,25	0,7	0,8	0,2	1			
	15	423	0,25	0,7	0,8	0,2	1			
	16	424	0,25	0,7	0,8	0,2	1			
5	17	521	0,25	0,7	0,8	0,2	1	0,80		
	18	522	0,25	0,7	0,8	0,2	1			
	19	523	0,25	0,7	0,8	0,2	1			
	20	524	0,25	0,7	0,8	0,2	1			
6	21	621	0,25	0,7	0,5	0,125	0	0,65		
	22	622	0,25	0,7	0,5	0,125	0			
	23	623	0,25	0,7	0,8	0,2	1			
	24	624	0,25	0,7	0,8	0,2	1			
7	25	721	0,25	0,7	0,8	0,2	1	0,80		
	26	722	0,25	0,7	0,8	0,2	1			
	27	723	0,25	0,7	0,8	0,2	1			
	28	724	0,25	0,7	0,8	0,2	1			



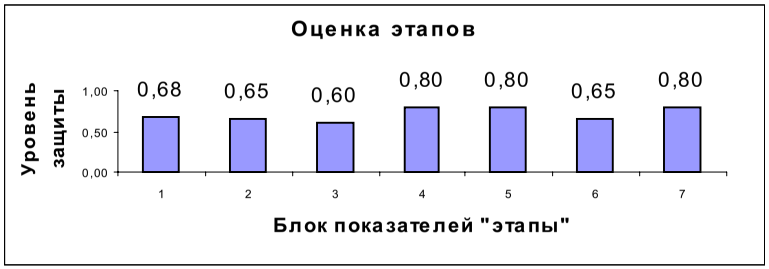


РИС. 25.9. *Оценка защищенности процессов и программ ИС*

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qд x aj	Сравнение профилей	Степень выполнения групп требований	Качественная оценка	Количественная оценка
	m	№	a_j	Q тр	Qд	Q даj	$S_{пр}$	$Q_{груп}$	Q	S
1	1	131	0,5	0,8	0,7	0,35	0	0,68		
	2	132	0,2	0,8	0,8	0,16	1			
	3	133	0,15	0,8	0,5	0,075	0			
	4	134	0,15	0,8	0,6	0,09	0			
2	5	231	0,25	0,8	0,5	0,125	0	0,73		
	6	232	0,25	0,8	0,8	0,2	1			
	7	233	0,25	0,8	0,8	0,2	1			
	8	234	0,25	0,8	0,8	0,2	1			
3	9	331	0,25	0,8	0,6	0,15	0	0,60		
	10	332	0,25	0,8	0,6	0,15	0			
	11	333	0,25	0,8	0,6	0,15	0			
	12	334	0,25	0,8	0,6	0,15	0			
4	13	431	0,25	0,8	0,8	0,2	1	0,70	**0,67**	**0,39**
	14	432	0,25	0,8	0,8	0,2	1			
	15	433	0,25	0,8	0,6	0,15	0			
	16	434	0,25	0,8	0,6	0,15	0			
5	17	531	0,25	0,8	0,6	0,15	0	0,65		
	18	532	0,25	0,8	0,6	0,15	0			
	19	533	0,25	0,8	0,6	0,15	0			
	20	534	0,25	0,8	0,8	0,2	1			
6	21	631	0,25	0,8	0,5	0,125	0	0,65		
	22	632	0,25	0,8	0,5	0,125	0			
	23	633	0,25	0,8	0,8	0,2	1			
	24	634	0,25	0,8	0,8	0,2	1			
7	25	731	0,25	0,8	0,8	0,2	1	0,68		
	26	732	0,25	0,8	0,6	0,15	0			
	27	733	0,25	0,8	0,5	0,125	0			
	28	734	0,25	0,8	0,8	0,2	1			

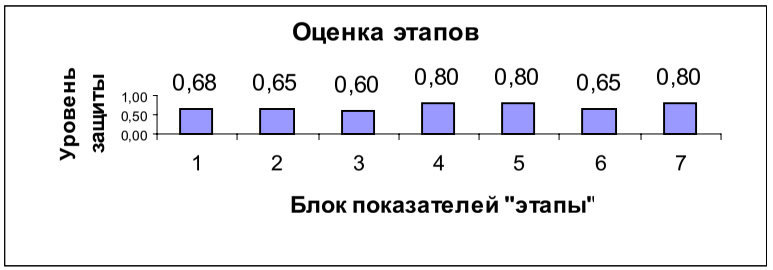


РИС. 25.10. *Оценка защищенности каналов связи ИС*

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qд x aj	Сравнение профилей	Степень выполнения групп требований	Качественная оценка	Количественная оценка
	m	№	a_j	Q_{mp}	$Q_д$	$Q_{даj}$	$S_{пр}$	$Q_{груп}$	*Q*	*S*
1	1	141	0,5	0,75	0,7	0,35	0	0,68	**0,72**	**0,64**
	2	142	0,2	0,75	0,8	0,16	1			
	3	143	0,15	0,75	0,5	0,075	0			
	4	144	0,15	0,75	0,6	0,09	0			
2	5	241	0,25	0,75	0,5	0,125	0	0,73		
	6	242	0,25	0,75	0,8	0,2	1			
	7	243	0,25	0,75	0,8	0,2	1			
	8	244	0,25	0,75	0,8	0,2	1			
3	9	341	0,25	0,75	0,6	0,15	0	0,60		
	10	342	0,25	0,75	0,6	0,15	0			
	11	343	0,25	0,75	0,6	0,15	0			
	12	344	0,25	0,75	0,6	0,15	0			
4	13	441	0,25	0,75	0,8	0,2	1	0,80		
	14	442	0,25	0,75	0,8	0,2	1			
	15	443	0,25	0,75	0,8	0,2	1			
	16	444	0,25	0,75	0,8	0,2	1			
5	17	541	0,25	0,75	0,8	0,2	1	0,80		
	18	542	0,25	0,75	0,8	0,2	1			
	19	543	0,25	0,75	0,8	0,2	1			
	20	544	0,25	0,75	0,8	0,2	1			
6	21	641	0,25	0,75	0,5	0,125	0	0,65		
	22	642	0,25	0,75	0,5	0,125	0			
	23	643	0,25	0,75	0,8	0,2	1			
	24	644	0,25	0,75	0,8	0,2	1			
7	25	741	0,25	0,75	0,8	0,2	1	0,80		
	26	742	0,25	0,75	0,8	0,2	1			
	27	743	0,25	0,75	0,8	0,2	1			
	28	744	0,25	0,75	0,8	0,2	1			

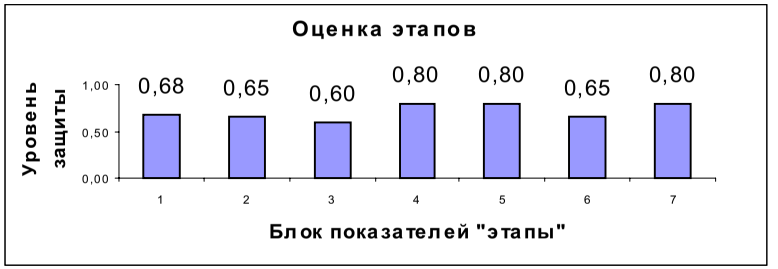
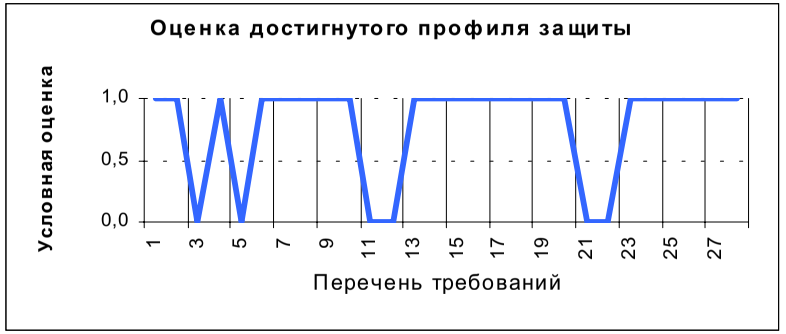
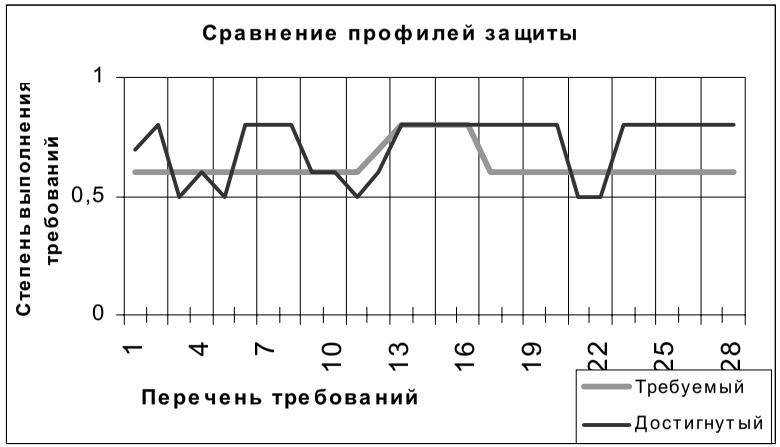


РИС. 25.11. *Оценка защищенности от утечки по техническим каналам (ПЭМИН)*

№ этапа	Перечень показателей	№ элемента матрицы	Коэффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qд x aj	Сравнение профилей	Степень выполнения групп требований	Качественная оценка	Количественная оценка
	m	№	a_j	Q_{mp}	$Q_д$	$Q_{дaj}$	$S_{пр}$	$Q_{груп}$	*Q*	*S*
1	1	151	0,5	0,6	0,7	0,35	1	0,68		
	2	152	0,2	0,6	0,8	0,16	1			
	3	153	0,15	0,6	0,5	0,075	0			
	4	154	0,15	0,6	0,6	0,09	1			
2	5	251	0,25	0,6	0,5	0,125	0	0,73		
	6	252	0,25	0,6	0,8	0,2	1			
	7	253	0,25	0,6	0,8	0,2	1			
	8	254	0,25	0,6	0,8	0,2	1			
3	9	351	0,5	0,6	0,6	0,3	1	0,59		
	10	352	0,2	0,6	0,6	0,12	1			
	11	353	0,15	0,6	0,5	0,075	0			
	12	354	0,15	0,7	0,6	0,09	0			
4	13	451	0,25	0,8	0,8	0,2	1	0,80	**0,72**	**0,79**
	14	452	0,25	0,8	0,8	0,2	1			
	15	453	0,25	0,8	0,8	0,2	1			
	16	454	0,25	0,8	0,8	0,2	1			
5	17	551	0,5	0,6	0,8	0,4	1	0,80		
	18	552	0,2	0,6	0,8	0,16	1			
	19	553	0,15	0,6	0,8	0,12	1			
	20	554	0,15	0,6	0,8	0,12	1			
6	21	651	0,25	0,6	0,5	0,125	0	0,65		
	22	652	0,25	0,6	0,5	0,125	0			
	23	653	0,25	0,6	0,8	0,2	1			
	24	654	0,25	0,6	0,8	0,2	1			
7	25	751	0,5	0,6	0,8	0,4	1	0,80		
	26	752	0,2	0,6	0,8	0,16	1			
	27	753	0,15	0,6	0,8	0,12	1			
	28	754	0,15	0,6	0,8	0,12	1			





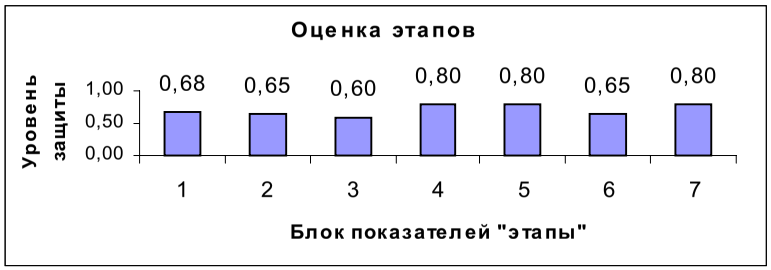


РИС. 25.12. *Оценка защищенности элементов системы защиты (управление и контроль)*

Табличное представление обобщенных количественных оценок						
	Направления защиты					$Q_{СЗИ}$
	1	2	3	4	5	
1	1,00	1,00	0,00	0,00	1,00	0,60
2	1,00	1,00	1,00	1,00	1,00	1,00
3	0,00	1,00	0,00	0,00	0,00	0,20
4	0,00	1,00	0,00	0,00	1,00	0,40
5	0,00	1,00	0,00	0,00	0,00	0,20
6	1,00	1,00	1,00	1,00	1,00	1,00
7	1,00	1,00	1,00	1,00	1,00	1,00
8	1,00	1,00	1,00	1,00	1,00	1,00
9	0,00	1,00	0,00	0,00	1,00	0,40
10	0,00	0,00	0,00	0,00	1,00	0,20
11	0,00	0,00	0,00	0,00	0,00	0,00
12	0,00	0,00	0,00	0,00	0,00	0,00
13	1,00	1,00	1,00	1,00	1,00	1,00
14	1,00	1,00	1,00	1,00	1,00	1,00
15	1,00	1,00	0,00	1,00	1,00	0,80
16	1,00	1,00	0,00	1,00	1,00	0,80
17	1,00	1,00	0,00	1,00	1,00	0,80
18	1,00	1,00	0,00	1,00	1,00	0,80
19	1,00	1,00	0,00	1,00	1,00	0,80
20	1,00	1,00	1,00	1,00	1,00	1,00
21	0,00	0,00	0,00	0,00	0,00	0,00
22	0,00	0,00	0,00	0,00	0,00	0,00
23	1,00	1,00	1,00	1,00	1,00	1,00
24	1,00	1,00	1,00	1,00	1,00	1,00
25	1,00	1,00	1,00	1,00	1,00	1,00
26	1,00	1,00	0,00	1,00	1,00	0,80
27	1,00	1,00	0,00	1,00	1,00	0,80
28	1,00	1,00	1,00	1,00	1,00	1,00

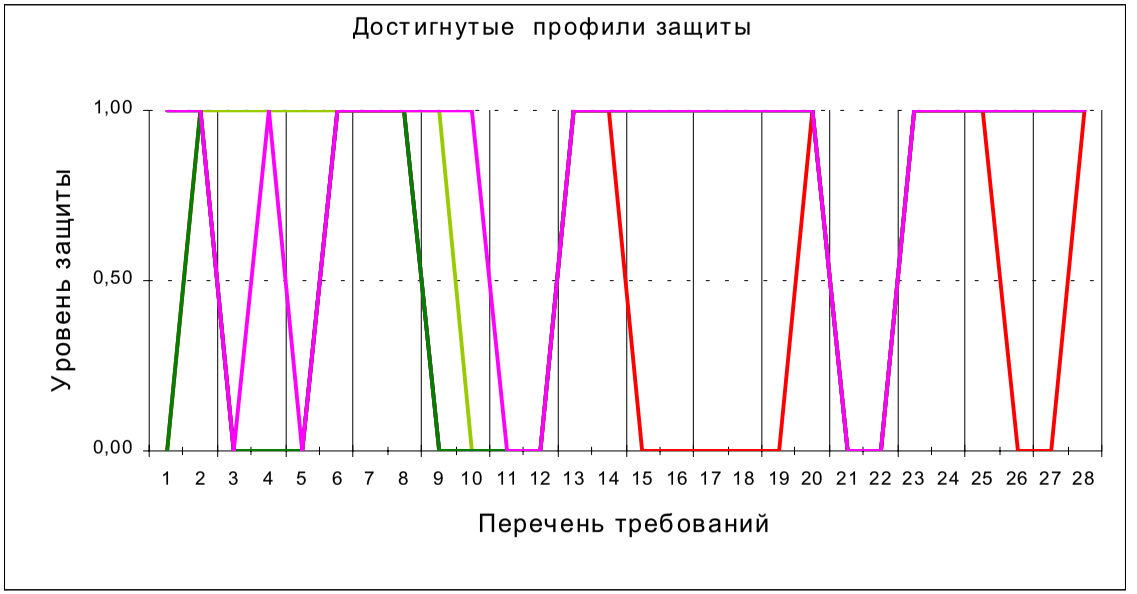


РИС. 25.13. *Достигнутый суммарный профиль безопасности (количественная оценка)*

Требования	Направления защиты					Qсзи
	1	2	3	4	5	
1	1,00	1,00	0,00	0,00	1,00	0,60
2	1,00	1,00	1,00	1,00	1,00	1,00
3	0,00	1,00	0,00	0,00	0,00	0,20
4	0,00	1,00	0,00	0,00	1,00	0,40
5	0,00	1,00	0,00	0,00	0,00	0,20
6	1,00	1,00	1,00	1,00	1,00	1,00
7	1,00	1,00	1,00	1,00	1,00	1,00
8	1,00	1,00	1,00	1,00	1,00	1,00
9	0,00	1,00	0,00	0,00	1,00	0,40
10	0,00	0,00	0,00	0,00	1,00	0,20
11	0,00	0,00	0,00	0,00	0,00	0,00
12	0,00	0,00	0,00	0,00	0,00	0,00
13	1,00	1,00	1,00	1,00	1,00	1,00
14	1,00	1,00	1,00	1,00	1,00	1,00
15	1,00	1,00	0,00	1,00	1,00	0,80
16	1,00	1,00	0,00	1,00	1,00	0,80
17	1,00	1,00	0,00	1,00	1,00	0,80
18	1,00	1,00	0,00	1,00	1,00	0,80
19	1,00	1,00	0,00	1,00	1,00	0,80
20	1,00	1,00	1,00	1,00	1,00	1,00
21	0,00	0,00	0,00	0,00	0,00	0,00
22	0,00	0,00	0,00	0,00	0,00	0,00
23	1,00	1,00	1,00	1,00	1,00	1,00
24	1,00	1,00	1,00	1,00	1,00	1,00
25	1,00	1,00	1,00	1,00	1,00	1,00
26	1,00	1,00	0,00	1,00	1,00	0,80
27	1,00	1,00	0,00	1,00	1,00	0,80
28	1,00	1,00	1,00	1,00	1,00	1,00

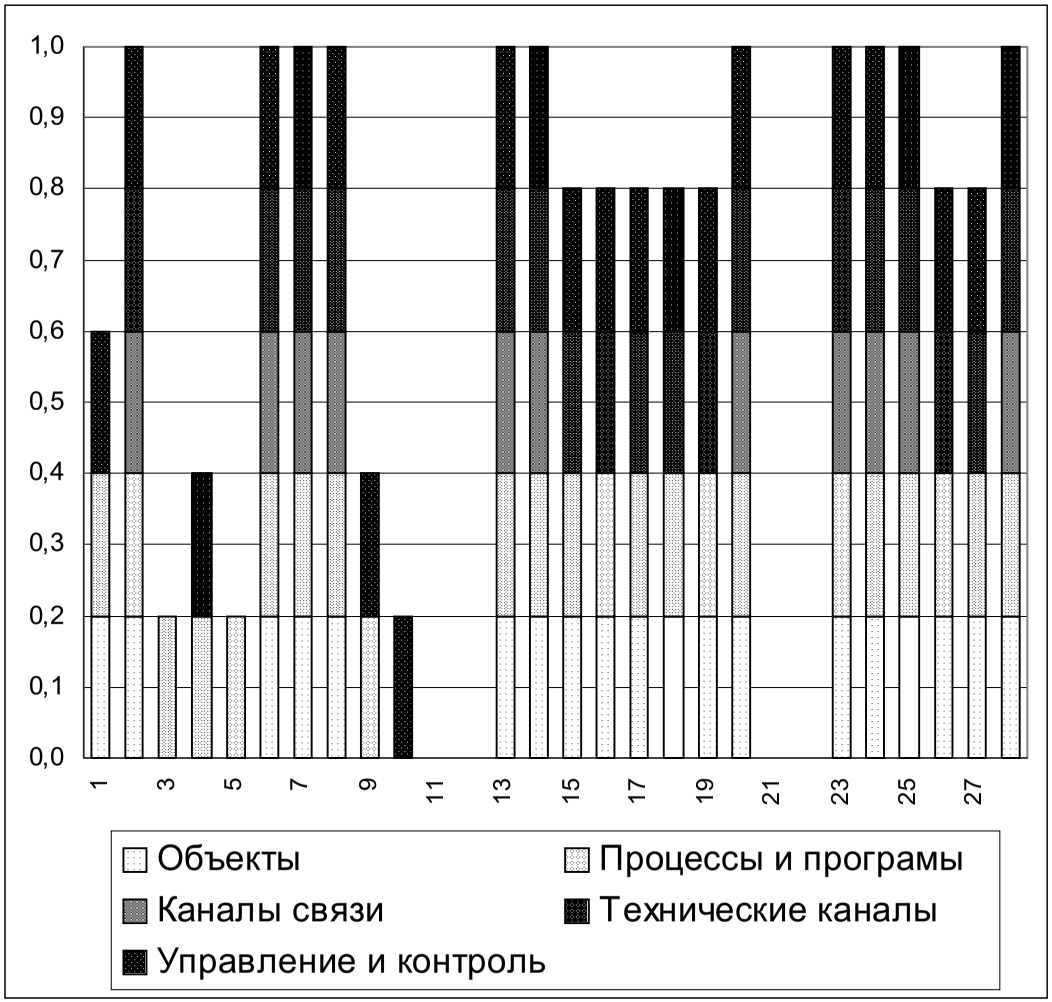


РИС. 25.14. *Количественные показатели степени выполнения требований по защите информации*

РИС. 25.15. *Обобщенные показатели уровня защищенности ИС*

Показатели	Направления защиты					$Q_{СЗИ}$
	1	2	3	4	5	
	Коэффициенты важности по направлениям					
	0,3	0,1	0,2	0,1	0,3	
Количественный	0,68	0,82	0,39	0,64	0,79	**0,66**
Качественный	0,71	0,79	0,67	0,72	0,72	**0,71**

РИС. 25.16. *Матрица количественных оценок*

<<< Этапы	Направления >>>	010				020				030				040				050				<<<Оценки
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты				
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054	
100	Определение информации, подлежащей защите	1	1	0	0	1	1	1	1	0	1	0	0	0	1	0	0	1	1	0	1	0,55
200	Выявление потенциальных каналов утечки информации	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0,85
300	Проведение оценки уязвимости и рисков	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0,15
400	Определение требований к СЗИ	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	0,90
500	Осуществление выбора средств защиты	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1	1	1	0,85
600	Внедрение и использование выбранных мер и средств	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0,50
700	Контроль целостности и управление защитой	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	0,90
	Оценки >>>	0,71	0,71	0,71	0,71	0,86	0,71	0,86	0,86	0,29	0,43	0,29	0,57	0,43	0,71	0,71	0,71	0,71	0,86	0,71	0,86	

РИС. 25.17. *Матрица качественных оценок*

<<< Этапы	Направления >>>	010				020				030				040				050				<<< Оценки
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				Управление системой защиты				
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054	
100	Определение информации, подлежащей защите	0,35	0,16	0,08	0,09	0,45	0,18	0,14	0,14	0,35	0,16	0,08	0,09	0,35	0,16	0,08	0,09	0,35	0,16	0,08	0,09	0,18
200	Выявление потенциальных каналов утечки информации	0,16	0,16	0,12	0,12	0,23	0,23	0,23	0,23	0,13	0,20	0,20	0,20	0,13	0,20	0,20	0,20	0,13	0,20	0,20	0,20	0,18
300	Проведение оценки уязвимости и рисков	0,15	0,15	0,15	0,15	0,23	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,30	0,12	0,08	0,09	0,15
400	Определение требований к СЗИ	0,40	0,16	0,12	0,12	0,20	0,20	0,20	0,20	0,20	0,20	0,15	0,15	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20
500	Осуществление выбора средств защиты	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,20	0,15	0,15	0,15	0,20	0,20	0,20	0,20	0,20	0,40	0,16	0,12	0,12	0,19
600	Внедрение и использование выбранных мер и средств	0,13	0,13	0,20	0,20	0,13	0,13	0,20	0,20	0,13	0,13	0,20	0,20	0,13	0,13	0,20	0,20	0,13	0,13	0,20	0,20	0,16
700	Контроль целостности и управление защитой	0,40	0,16	0,12	0,12	0,20	0,20	0,20	0,20	0,20	0,15	0,13	0,20	0,20	0,20	0,20	0,20	0,40	0,16	0,12	0,12	0,19
	Оценки >>>	0,26	0,16	0,14	0,14	0,23	0,18	0,19	0,19	0,19	0,16	0,15	0,17	0,19	0,18	0,18	0,18	0,27	0,16	0,14	0,15	