# Введение

Лабораторные работы преследуют цель ознакомления с комплексом показателей для оценки защищенности систем информационных технологий (ИТ) и программной средой «Эксперт», используемой для моделирования процессов оптимизации системы информационной безопасности (СИБ) путем определения положения механизмов защиты, включение которых в иерархию СИБ повышает уровень защищенности ИТ-системы. Программная среда «Эксперт» разработана при участии студентов Хоан Зянга и Лазарева А.С.

# 1. Теоретическая часть

Мониторинг защищенности корпоративной сети (КС) базируется на решении оптимизационных задач на основе рейтинговых показателей, учитывающих разноплановые экспертные оценки, включая экономические [1]. Решению этих задач сопутствует проблема оценки эффективности инвестиционных проектов. Задача инвестиционного анализа систем информационной безопасности (ИБ) представляется актуальной и связана с определением экономической эффективности систем ИБ исходя из затрат на создание и эксплуатацию СИБ и предотвращенного ущерба от реализации угроз [2].

## 1.1. Модель адаптивной СИБ

Эволюция информационных технологий связана с *интеллектуальными системами*, в которых присутствуют процессы *зарождения*, *адаптации* и *развития*. В ИТ эти процессы реализуют, используя метод аналогии с биосистемами (рис. 1), которым свойственны высокая защищенность [3, 4].

**Системный подход** определяет *методологию* и *принципы построения* систем ИТ. Принцип м*оделируемости* позволяет предотвратить ошибки проектирования кибернетических систем. Принцип *связности* при разработке эффективной системы ИБ рассматривает объект защиты комплексно [5], объединяя объект защиты, внешнюю среду, средства защиты и угрозы злоумышленника и учитывая взаимосвязи: источник угрозы – фактор (уязвимость) – угроза (действие) – последствия (атака).

**Динамичный характер поля угроз** требует оперативно устранять новые уязвимости, выявляемые в процессе эксплуатации системы ИТ, и исключать возможность для реализации новых угроз. Динамичность поля угроз выдвигает в разряд первоочередных качеств СИБ свойства *адаптивности* и *наследования* ранее накопленного *опыта*, который отражается в многоуровневой системе ме-

ханизмов защиты. Свойство адаптивности позволяет при ограниченных затратах на СИБ обеспечить заданный уровень безопасности систем ИТ за счет реакции на изменение поля угроз, а наследование – передачу опыта ИБ в последующие реализации СИБ.

**Иерархия уровней в модели адаптивной СИБ.** Информация о жизненном опыте СИБ может хранится и передаваться в поколениях (тиражирование и модификация систем ИТ) в виде *адаптивных информационных полей* нейронных систем: (1) *поля известных угроз* на нижнем, иммунном уровне и (2) поля *жизненного опыта* на верхнем, рецепторном уровне СИБ (рис. 2). Процесс адаптации первых связан с решением задачи кластеризации - расширение информационного поля известных угроз. Изменение перечня известных угроз отражается на верхнем уровне СИБ в модификации информационного поля жизненного опыта НС - специализированной структуры НС, которая описывается системой нечетких правил логического вывода. Процесс адаптации вторых связан с алгоритмами обучения нечеткой НС и видоизменяет систему нечетких правил логического вывода, ставящую в соответствие известным угрозам механизмы защиты.

Анализ взаимосвязанных пар «угроза-уязвимость» позволяет поставить в соответствие каждой угрозе, оговоренной в спецификации, - *заданной угрозе* из множества *известных угроз*, уязвимости, которые назовем *выявленными уязвимостями* системы. Остальные уязвимости в системе ИТ обозначим термином *потенциальные уязвимости*.

Экономически целесообразно закрыть механизмами защиты все *выявленные уязвимости*, а изменение поля угроз, повлекшее перевод ряда потенциальных уязвимостей в разряд выявленных, сопровождать процессом адаптации информационных полей СИБ.

В процессе адаптации информационных полей вначале задействуют имеющиеся в системе механизмы защиты для нейтрализации выявленной уязвимости, и только в случае неудовлетворительного результата производят расширение состава механизмов защиты и обучение верхнего уровня СИБ.

Для представления защищенности систем ИТ используют модели многоуровневой СИБ [6]. Вначале модель содержит минимальное количество механизмов, достаточных для защиты выявленных уязвимостей, которые будут пополняться при расширении поля угроз и переводе отдельных потенциальных уязвимостей в статус выявленных.

**Модель адаптивной СИБ**. Связующим звеном модели адаптивной СИБ (рис. 3) является методика оценки защищенности ИТ-системы [7].

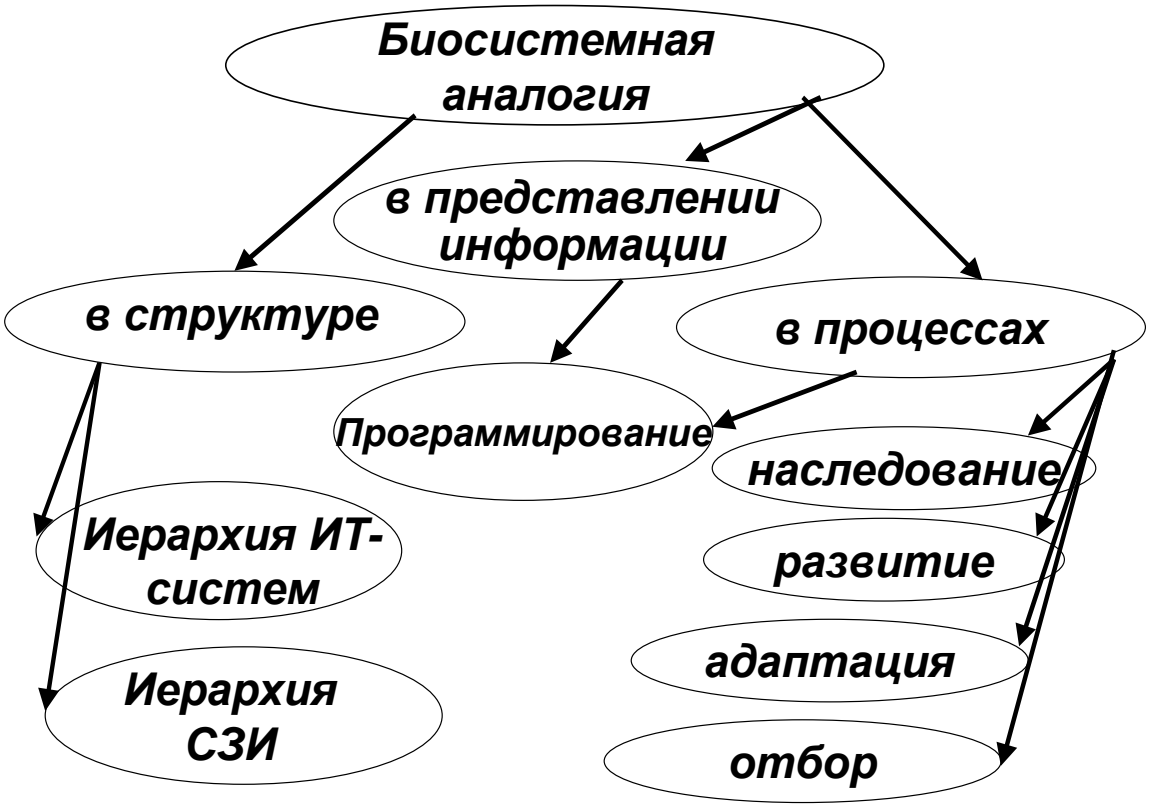
Биосистемная аналогия
в представлении информации
в структуре
в процессах
Программирование
наследование
развитие
адаптация
отбор
Иерархия ИТ-систем
Иерархия СЗИ

*Рис. 1*

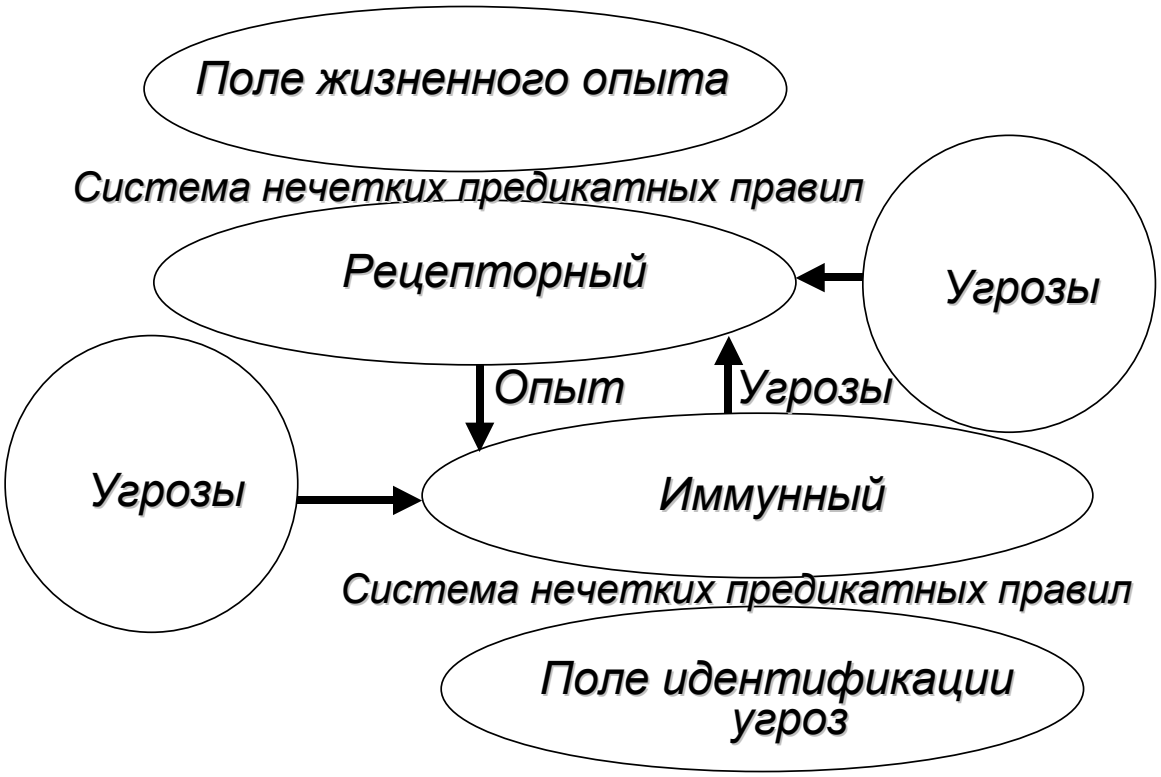
Поле жизненного опыта
Система нечетких предикатных правил
Рецепторный
Угрозы
Опыт
Угрозы
Угрозы
Иммунный
Система нечетких предикатных правил
Поле идентификации угроз

*Рис. 2.*

Методика оценки защищенности координирует взаимосвязь классификаторов угроз и механизмов защиты (в виде нейронных сетей - НС, нечетких НС, систем нечетких предикатных правил), структурной модели системы информационной безопасности (СИБ), инструментальных средств расчета показателей защищенности и рейтинга ИТ-системы [8 – 10].

В соответствии с заданием на проектирование системы защиты информации выбирается *структурная модель СИБ* в виде иерархии уровней механизмов защиты (МЗ). Как правило, ограничиваются минимальным комплектом МЗ, достаточным для отражения угроз информационным ресурсам (ИР), оговоренных в спецификации на проектирование ИТ-системы.

Опыт экспертов представляется матрицами экспертных оценок, на базе которых формируются *системы нечетких предикатных правил* для классификации 1) угроз по признакам атак и 2) МЗ на поле угроз.

Системы нечетких предикатных правил для возможности автоматической адаптации отображают в структуре *нейро-нечетких классификаторов*, которые обучают на подмножестве векторов признаков атаки. Аналогично *обучают четкие нейросетевые классификаторы* таким образом, чтобы число формируемых кластеров равнялось числу правил в системе нечетких предикатных правил.

Для исходных матриц экспертных оценок производят расчет *показателей защищенности и рейтинга ИТ-системы* [7, 8], которые используются методикой оценки защищенности ИТ-системы для анализа и коррекции матриц экспертных оценок и функциональных параметров нейросетевых и нейро-нечетких классификаторов (систем нечетких предикатных правил логического вывода).

## 1.2. Комплекс показателей защищенности систем ИТ

Применение модели адаптивной защиты, основанной на принципе биологической аналогии позволяет:

- обеспечить близкое к оптимальному соотношение "стоимость/ эффективность" СИБ за счет постепенного наполнения многоуровневой модели ИБ только необходимыми механизмами защиты,
- в динамике отслеживать наиболее задействованные механизмы защиты при изменении поля угроз,
- формировать спецификацию требований на отсутствующие механизмы защиты,
- оценивать защищенность системы ИТ через величины относительного ущерба и интегральные показатели активности распределенных по структуре СИБ механизмов защиты.

## Показатели защищенности системы ИТ

Решение о расширении классификаций атак и механизмов защиты производится в соответствии с системой *оценок достоверности* нейтрализации угроз в разрезе отдельных механизмов защиты или отдельных эшелонов СИБ и аналогичных *оценок потенциального ущерба*, также соотносимых с отдельными механизмами защиты или отдельными эшелонами СИБ. Далее по тексту потенциальный ущерб будем рассматривать в относительных величинах, к примеру, по отношению к значению максимально допустимого ущерба в информационной системе хозяйствующего субъекта.

Можно использовать распределение используемого в системе ИТ подмножества механизмов защиты по эшелонам многоуровневой модели СИБ, аналогичное изображенному на рис. 4 [11].

Результаты экспертных оценок, а также последующего обучения нечетких НС могут быть представлены в виде матрицы достоверности «угрозы – механизмы защиты» *ME* размерностью *m*x*n*

$$ME_{m\times n} = \begin{pmatrix} me_{11} & me_{12} & \vdots & me_{1\ n} \\ me_{21} & me_{22} & \vdots & me_{2\ n} \\ \cdots & \cdots & \cdots & \cdots \\ me_{m\,1} & me_{m\,2} & \vdots & me_{m\ n} \end{pmatrix},$$

где $i = m$ – число механизмов защиты, $j = n$ - число эшелонов СИБ.

*Активность эшелона* СИБ по нейтрализации угроз, входящих в систему предикатных правил в качестве посылок, определяется строкой интегральных показателей, представленных строкой показателей *значимости эшелона* в многоуровневой СИБ

$$x_j = \sqrt[m]{\sum_{i=1}^{m} me_{ij}}\ ,\ \ j = 1,...,n\ , \qquad (1)$$

нормированных, например, по значению максимального из $x_j,\ j = 1,...,n$ или по значению суммы элементов строки показателей значимости $\sum_{j=1}^{m} x_j$, $j = 1,...,n$.

Сопоставление интегральных показателей в пределах строки позволяет выявить наиболее задействованные эшелоны в многоуровневой модели СИБ по нейтрализации поля действующих на систему ИТ угроз.

Аналогично по матрице достоверности использования механизмов защиты для нейтрализации угроз можно получить столбец интегральных показателей *активности* использования отдельного *механизма защиты* во всех эшелонах СИБ для нейтрализации последствий действующего поля угроз

$$x_i = \sqrt[n]{\sum_{i=1}^{n} me_{ij}}\ ,\ i = \ 1,..., m\ . \qquad (2)$$

Сопоставление интегральных показателей в пределах столбца позволяет выявить наиболее задействованные механизмы защиты в многоуровневой СИБ.

Анализ интегральных показателей матрицы достоверности «угрозы – МЗ» дает возможность обосновать целесообразность использования механизма защиты в составе соответствующего эшелона многоуровневой СИБ.

Использование экспертных оценок и отражение в структуре нейронечеткой сети априорного опыта экспертов ИБ сопровождается проверкой на непротиворечивость результатов опроса экспертов. Непротиворечивость оценок экспертов ИБ м.б. обеспечена применением, например, метода на основе расчета максимального собственного значения матрицы парных сравнений [12].

Приведенные выше показатели будут более информативными, если учитывать не только достоверность использования механизмов защиты в структуре СИБ, но и показатели *потенциального ущерба*, возникающего в результате реализации атак на систему ИТ и который может быть предотвращен системой информационной безопасности. С этой целью *оценку защищенности* можно косвенно связать с *предотвращением ущерба* системе ИТ, и, кроме того, использовать экспертные оценки для сопоставления, с одной стороны, поля угроз ИБ с потенциальным ущербом от их реализации, с другой стороны, размера потенциального ущерба с местом реализации угрозы в структуре ИТ.

## Методика оценки защищенности системы ИТ

Для каждого эшелона многоуровневой СИБ формируется экспертная оценка *достоверности нейтрализации* поля известных угроз известными механизмами защиты и *потенциального ущерба*, исходя из опыта экспертов ИБ. Ущерб от реализации угроз в системе ИТ следует оценивать в относительных величинах, например, по отношению к максимально допустимой для данного хозяйствующего субъекта величине. Расчет потенциального ущерба производится за определенный промежуток времени с учетом частоты активации угроз.

1. Исходные данные (*экспертные оценки)* представляют в матричной форме.

Для каждого эшелона многоуровневой СИБ оценивается достоверность нейтрализации угроз механизмами защиты с последующим формированием матрицы достоверности «МЗ-угрозы» *MT* размерностью *m*x*p*

$$MT_{m\times p} = \begin{pmatrix} mt_{11} & mt_{12} & \vdots & mt_{1p} \\ mt_{21} & mt_{22} & \vdots & mt_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ mt_{m1} & mt_{m2} & \vdots & mt_{mp} \end{pmatrix},$$

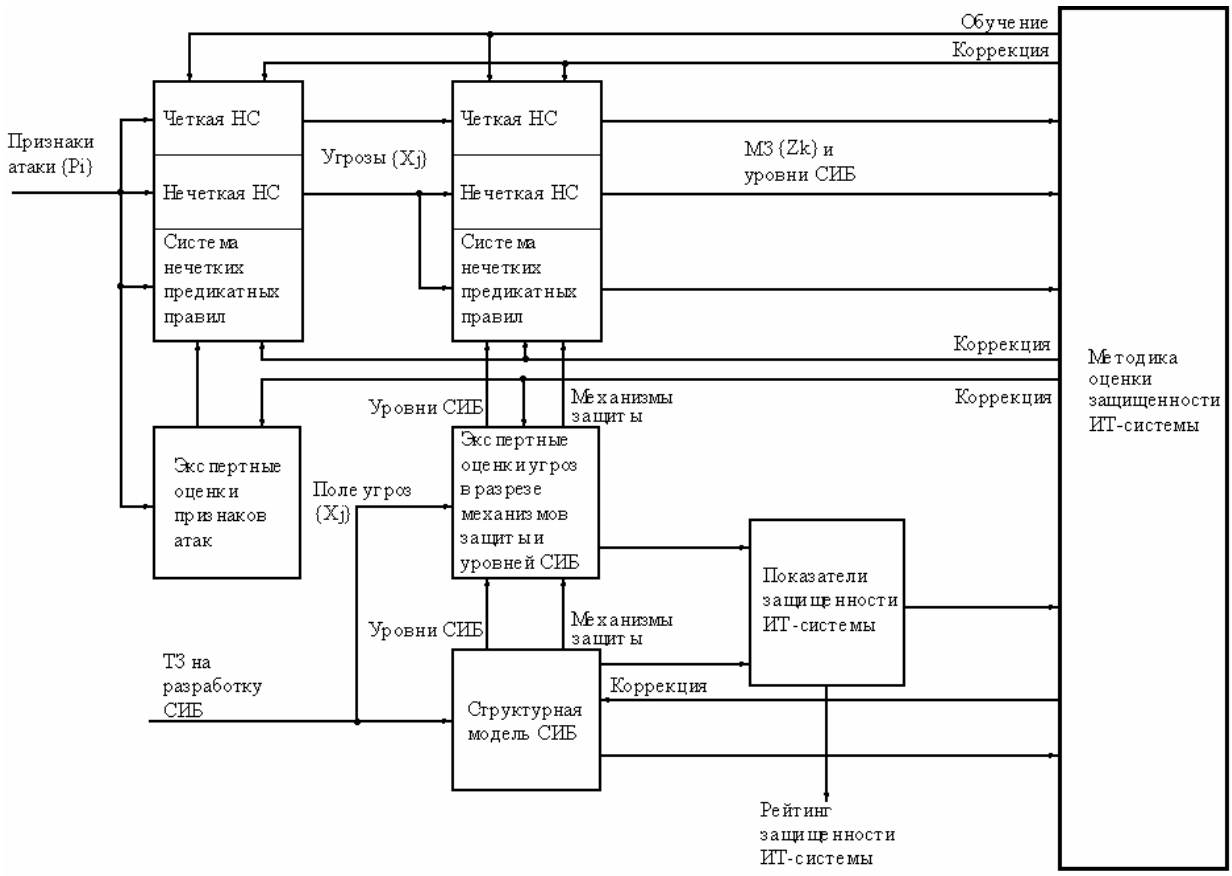
Обучение
Коррекция
Признаки атаки (Pi)
Четкая НС
Нечеткая НС
Система нечетких предикатных правил
Угрозы (Xj)
Четкая НС
Нечеткая НС
Система нечетких предикатных правил
МЗ (Zk) и уровни СИБ
Коррекция
Коррекция
Методика оценки защищенности ИТ-системы
Уровни СИБ
Механизмы защиты
Экспертные оценки признаков атак
Поле угроз (Xj)
Экспертные оценки угроз в разрезе механизмов защиты и уровней СИБ
Показатели защищенности ИТ-системы
Уровни СИБ
Механизмы защиты
ТЗ на разработку СИБ
Структурная модель СИБ
Коррекция
Рейтинг защищенности ИТ-системы

*Рис. 3.*

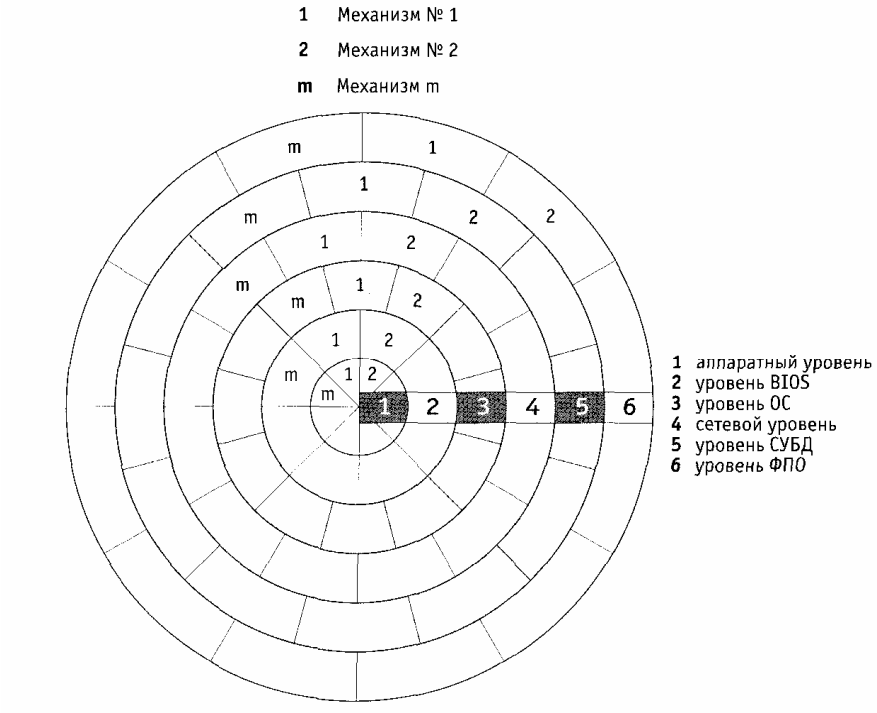
1 Механизм № 1
2 Механизм № 2
m Механизм m
1 аппаратный уровень
2 уровень BIOS
3 уровень ОС
4 сетевой уровень
5 уровень СУБД
6 уровень ФПО

*Рис. 4.*

$m$ – число механизмов защиты, $p$ - число известных угроз, и матрицы достоверности «угрозы-эшелоны» *TE*

$$TE_{p\times n} = \left(\begin{array}{cc:c} te_{11} & te_{12} & te_{1n} \\ te_{21} & te_{22} & te_{2n} \\ \hdashline te_{p1} & te_{p2} & te_{pn} \end{array}\right),$$

$p$ - число известных угроз, $n$ - число эшелонов СИБ.

Для каждого эшелона многоуровневой СИБ оценивается уровень потенциального ущерба и формируются матрицы «эшелоны-ущерб» *ET*

$$ET_{n\times p} = \left(\begin{array}{cc:c} et_{11} & et_{12} & et_{1p} \\ et_{21} & et_{22} & et_{2p} \\ \hdashline et_{n1} & et_{n2} & et_{np} \end{array}\right),$$

$n$ - число эшелонов СИБ, $p$ - число угроз, и матрицы «ущерб-МЗ» *TM*

$$TM_{p\times m} = \left(\begin{array}{cc:c} tm_{11} & tm_{12} & tm_{1m} \\ tm_{21} & tm_{22} & tm_{2m} \\ \hdashline tm_{p1} & tm_{p2} & tm_{pm} \end{array}\right),$$

$p$ - число известных угроз, $m$ – число механизмов защиты.

2. Для каждого эшелона многоуровневой СИБ экспертные оценки в виде системы нечетких предикатных правил отображают в структуре нейро-нечетких сетей. В процессе последующей адаптации нечетких НС в составе иерархических СИБ на обучающей выборке, соответствующей некоторому подмножеству поля известных угроз производится *автоматическая коррекция* системы нечетких предикатных правил, а также показателей потенциального ущерба и достоверности (истинности) нейтрализации набора угроз соответствующим эшелоном или МЗ многоуровневой СИБ. Корректность исходных экспертных оценок может быть проверена сопоставлением элементов вышеперечисленных матриц либо сопоставлением интегральных оценок защищенности до и после процесса обучения нейро-нечетких СИБ.

3. *Интегральные оценки защищенности* получают в результате операций над матрицами. В частности умножение матриц достоверности «МЗ-угрозы» *MT* и «угрозы-эшелоны» *TE* позволяет получить матрицу «МЗ-эшелоны» *ME* – матрицу достоверности активации известных механизмов защиты, распределенных по эшелонам многоуровневой СИБ, для нейтрализации известных угроз

$$ME_{m\times n} = \begin{pmatrix} me_{11} & me_{12} & \vdots & me_{1\,n} \\ me_{21} & me_{22} & \vdots & me_{2\,n} \\ \cdots & \cdots & \cdots & \cdots \\ me_{m\,1} & me_{m\,2} & \vdots & me_{m\,n} \end{pmatrix},$$

$m$ – число механизмов защиты, $n$ - число эшелонов СИБ, а умножение матриц потенциального ущерба «эшелоны-ущерб» *ET* и «ущерб-МЗ» *TM* - матрицу потенциального ущерба «эшелоны-МЗ» *EM,* отражающую распределение потенциального ущерба от реализации известных угроз по МЗ и эшелонами СИБ

$$EM_{n\times m} = \begin{pmatrix} em_{\,11} & em_{\,12} & \vdots & em_{\,1\,m} \\ em_{\,21} & em_{\,22} & \vdots & em_{\,2\,m} \\ \cdots & \cdots & \cdots & \cdots \\ em_{\,n\,1} & em_{\,n\,2} & \vdots & em_{\,n\,m} \end{pmatrix},$$

$n$ - число эшелонов СИБ, $m$ – число механизмов защиты.

Промежуточные оценки в виде строки (1) и столбца (2) интегральных показателей характеризуют *активность* использования отдельного *механизма защиты* либо отдельного *эшелона* в рамках многоуровневой СИБ, а также позволяют оценить потенциальный *ущерб* в разрезе МЗ и эшелонов СИБ.

4. Дальнейшие операции над матрицами *ME* и *EM* дают возможность обобщить в диагональных элементах *итоговой матрицы* как показатель достоверности активации механизма защиты в результате атаки, так и потенциального ущерба от ее реализации.

Умножением матрицы достоверности *ME* и матрицы потенциального ущерба *EM* получают квадратную *матрицу достоверности потенциального ущерба* «МЗ-МЗ» *MM*

$$MM_{m\times m} = \begin{pmatrix} mm_{\,11} & mm_{\,12} & \vdots & mm_{\,1\,m} \\ mm_{\,21} & mm_{\,22} & \vdots & mm_{\,2\,m} \\ \cdots & \cdots & \cdots & \cdots \\ mm_{\,m\,1} & mm_{\,m\,2} & \vdots & mm_{\,m\,m} \end{pmatrix},$$

$m$ – число МЗ, а умножением матрицы *EM* и матрицы *ME* получают квадратную матрицу достоверности потенциального ущерба «эшелоны-эшелоны» *EE*

$$EE_{n\times n} = \begin{pmatrix} ee_{\,11} & ee_{\,12} & \vdots & ee_{1n} \\ ee_{\,21} & ee_{\,22} & \vdots & ee_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ ee_{n\,1} & ee_{\,n\,2} & \vdots & ee_{nn} \end{pmatrix},$$

$n$ - число эшелонов СИБ.

Для матрицы *MM* в качестве обобщающего показателя можно рассматривать вектор, образованный диагональными элементами $mm_{ij} = p_i$, $i = j = 1,\ldots, m$,

матрицы - *вектор распределения потенциального ущерба по механизмам защиты* СИБ $P_{1xm} = (p_1, p_2, ..., p_m)$,

а для матрицы *EE* – вектор из диагональных элементов $ee_{ij} = d_i$, $i = j = 1,\ldots, n$, - *вектор распределения ущерба по эшелонам СИБ* $D_{1xn} = (d_1, d_2, ..., d_n)$.

5. В качестве интегральных оценок защищенности системы ИТ в разрезе МЗ можно использовать рейтинговый показатель $R_M$ - длину вектора $P_{1xm}$

$$R_M = |P_{1xm}| = \sqrt{\sum_{i=1}^{m} p_i^2}, \; i = 1,..., m, \tag{3}$$

а в разрезе эшелонов СИБ - рейтинговый показатель $R_E$ - длину вектора $D_{1xn}$

$$R_E = |D_{1xn}| = \sqrt{\sum_{i=1}^{n} d_i^2}, \; i = 1,..., n. \tag{4}$$

## 2. Практическая часть

Практическая часть работы связана с формированием структуры СИБ, путем задания иерархии эшелонов и перечня МЗ для нейтрализации требуемого поля угроз, заполнением матриц экспертными оценками достоверности активации МЗ, предотвращенного ущерба и частоты активации угроз, расчета рейтинговых показателей защищенности и оптимизации СИБ в составе ИТ-системы.

### 2.1. Моделирование системы защиты информации

Инструментальные средства «Эксперт» (далее программа) реализуют комплекс показателей для оценки информационной защищенности систем информационных технологий, которые как элемент динамической модели адаптивной защиты используются в системах ИТ для осуществления механизмов развития и адаптации к изменению поля угроз, а также определения (путем моделирования последствий атак на множестве известных угроз) положения механизмов защиты, включение которых в иерархию системы защиты информации предотвратит появление ущерба, превышающего допустимый для данного хозяйствующего субъекта уровень.

#### Описание программы моделирования СИБ

Программа активируются запуском файла Expert.exe, для работы которого необходим размещенный в том же каталоге файл default.dic, содержащий списки известных угроз, МЗ и перечень уровней СИБ.

При первом запуске программы открывается окно (рис. 5), предназначенное для формирования или корректировки списков известных угроз, механизмов защиты и уровней иерархической СИБ.

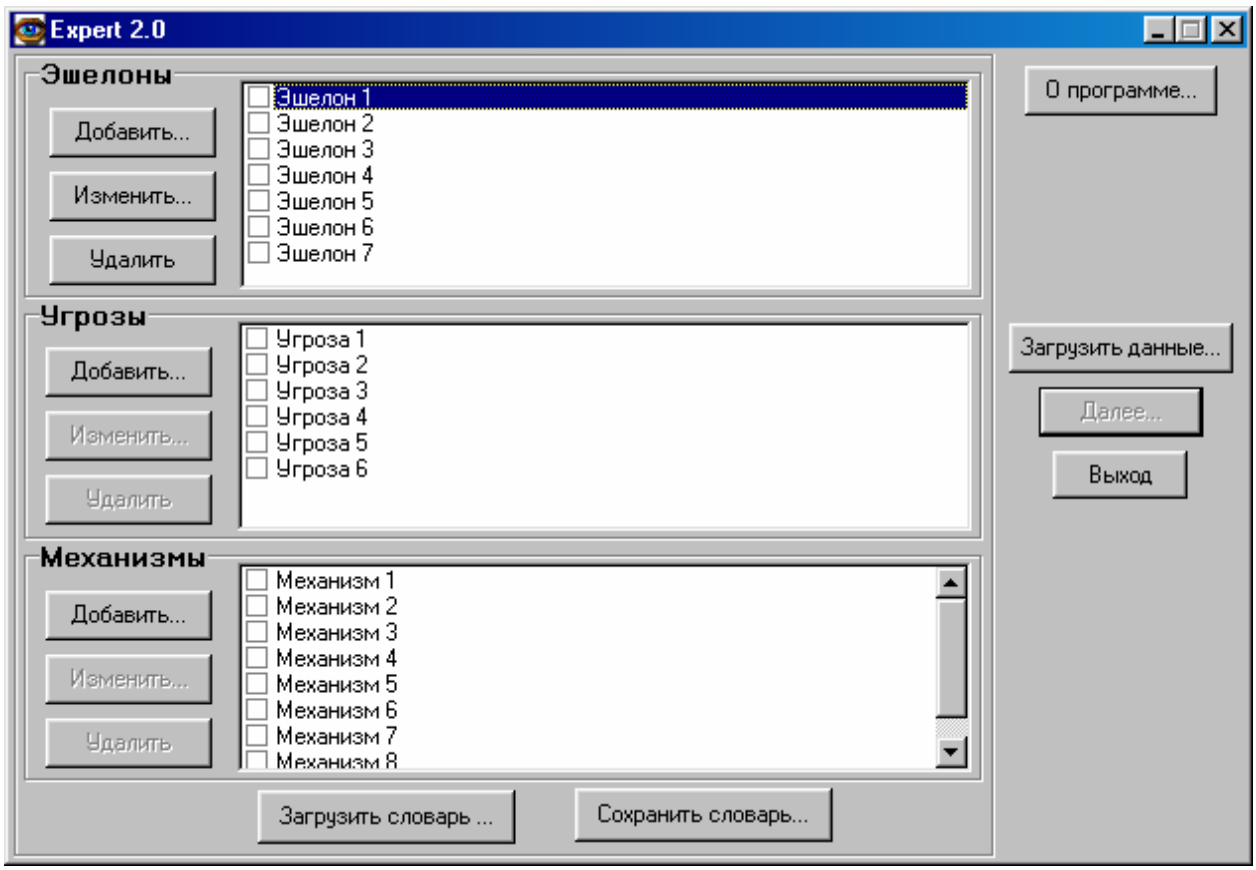
Expert 2.0
Эшелоны
Добавить...
Изменить...
Удалить
Эшелон 1
Эшелон 2
Эшелон 3
Эшелон 4
Эшелон 5
Эшелон 6
Эшелон 7
Угрозы
Добавить...
Изменить...
Удалить
Угроза 1
Угроза 2
Угроза 3
Угроза 4
Угроза 5
Угроза 6
Механизмы
Добавить...
Изменить...
Удалить
Механизм 1
Механизм 2
Механизм 3
Механизм 4
Механизм 5
Механизм 6
Механизм 7
Механизм 8
Загрузить словарь ...
Сохранить словарь...
О программе...
Загрузить данные...
Далее...
Выход

*Рис. 5.*

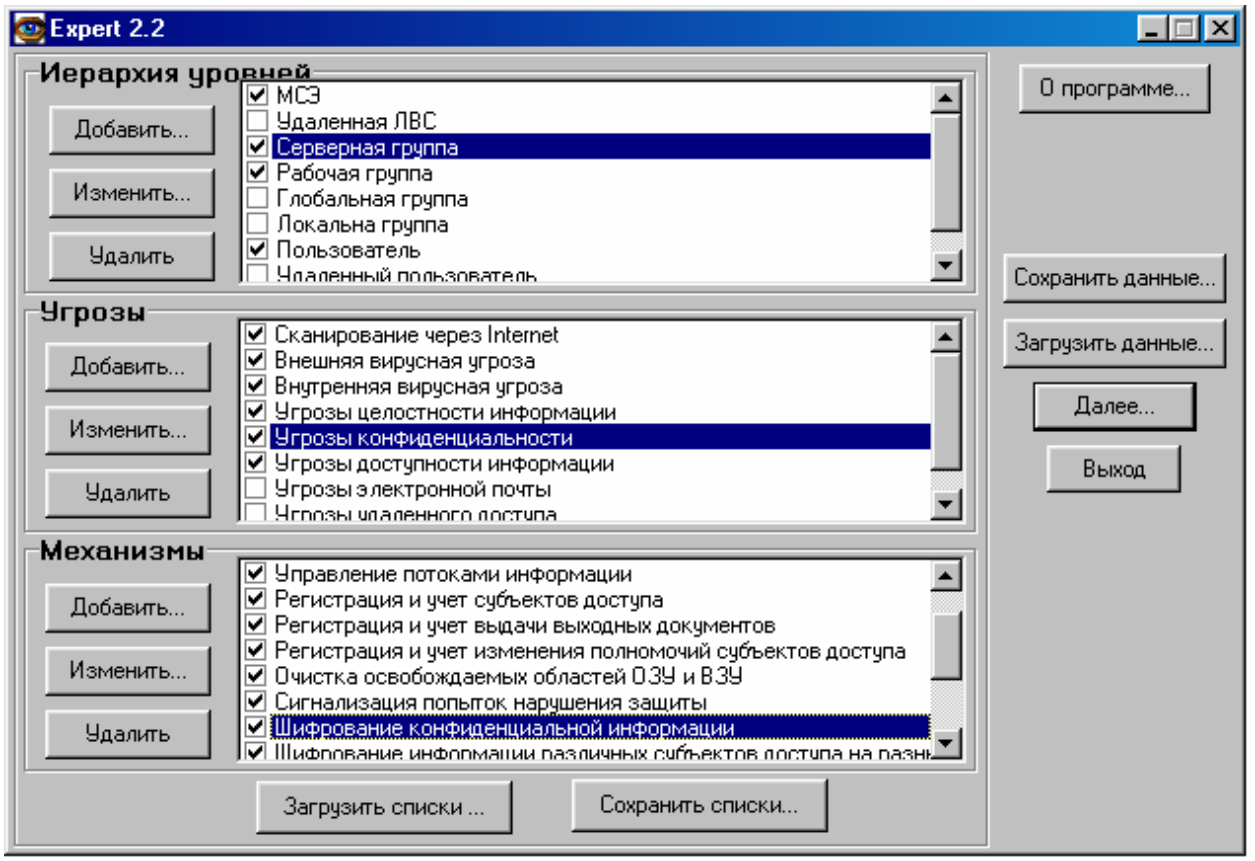
Expert 2.2
Иерархия уровней
Добавить...
Изменить...
Удалить
МСЭ
Удаленная ЛВС
Серверная группа
Рабочая группа
Глобальная группа
Локальна группа
Пользователь
Удаленный пользователь
Угрозы
Добавить...
Изменить...
Удалить
Сканирование через Internet
Внешняя вирусная угроза
Внутренняя вирусная угроза
Угрозы целостности информации
Угрозы конфиденциальности
Угрозы доступности информации
Угрозы электронной почты
Угрозы удаленного доступа
Механизмы
Добавить...
Изменить...
Удалить
Управление потоками информации
Регистрация и учет субъектов доступа
Регистрация и учет выдачи выходных документов
Регистрация и учет изменения полномочий субъектов доступа
Очистка освобождаемых областей ОЗУ и ВЗУ
Сигнализация попыток нарушения защиты
Шифрование конфиденциальной информации
Шифрование информации различных субъектов доступа на разны
Загрузить списки ...
Сохранить списки...
О программе...
Сохранить данные...
Загрузить данные...
Далее...
Выход

*Рис. 6.*

Выбор одного из списков **Эшелоны**, **Угрозы** или **Механизмы** активирует кнопки **Добавить**, **Изменить** и **Удалить,** после чего можно редактировать пункты соответствующего списка (рис. 6) и сохранять их (**Сохранить списки**) для последующего использования (**Загрузить списки**).

Если сформированный перечень списков сохранить с именем default.dic, то последующие запуски программы приведут к отображению в окне программы последней сохраненной редакции списков.

Для дальнейших расчетов (для активации кнопки **Далее**) необходимо во всех списках отметить конкретные угрозы, активированные МЗ и те эшелоны многоуровневой СИБ, в которых использованы активированные МЗ.

Подобная отметка определяет размерность матриц экспертных оценок, заполняемых в последующих окнах программы. Кнопка **Далее** открывает последовательность диалоговых окон для формирования матриц экспертных оценок по достоверности активации (ДА), относительному потенциальному ущербу (ОПУ) и частоте активации угроз (ЧАУ) в разрезе «угрозы-МЗ» и «угрозы-эшелоны».

Возможно использование ранее введенных экспертами баз данных (выбор кнопки (**Загрузить данные**) из файла с расширением *.sav.

Для формирования исходных матриц экспертных оценок необходимо в списке **Исходные матрицы** выбрать соответствующую из **матриц достоверности активации** «МЗ-угрозы», «угрозы-эшелоны» и осуществить ввод значений, сопровождаемый контекстными пояснениями вида: **Столбец *j***: Угроза; **Строка *i*** : Механизм защиты.

В верхней правой части окна (рис. 7) следует также ввести экспертные оценки граничных значений для лингвистической переменной «Достоверность активации МЗ» в поля **Пороговые значения для малой величины** и **Пороговые значения для средней величины**, задающие нечеткие значения «малая величина» (в окне окрашена в зеленый цвет), «средняя величина» - коричневый цвет и «большая величина» - красный цвет.

Выбор кнопки **Расчет** после завершения ввода результатов экспертных оценок приводит к умножению матриц «МЗ-угрозы», «угрозы-эшелоны». Подобное преобразование позволяет сформировать матрицы «МЗ-эшелоны» (рис. 7), описывающие распределение ДА, ОУП, ЧАУ по механизмам защиты и эшелонам СИБ на поле известных угроз. Результаты расчетов матрицы «МЗ-эшелоны» сопровождаются выводом столбца и строки **показателей значимости** (в окне выделены синим цветом). Показатели значимости отражают распределение достоверности активации конкретного МЗ во всех эшелонах СИБ или достоверности активации конкретного эшелона со всеми его МЗ.

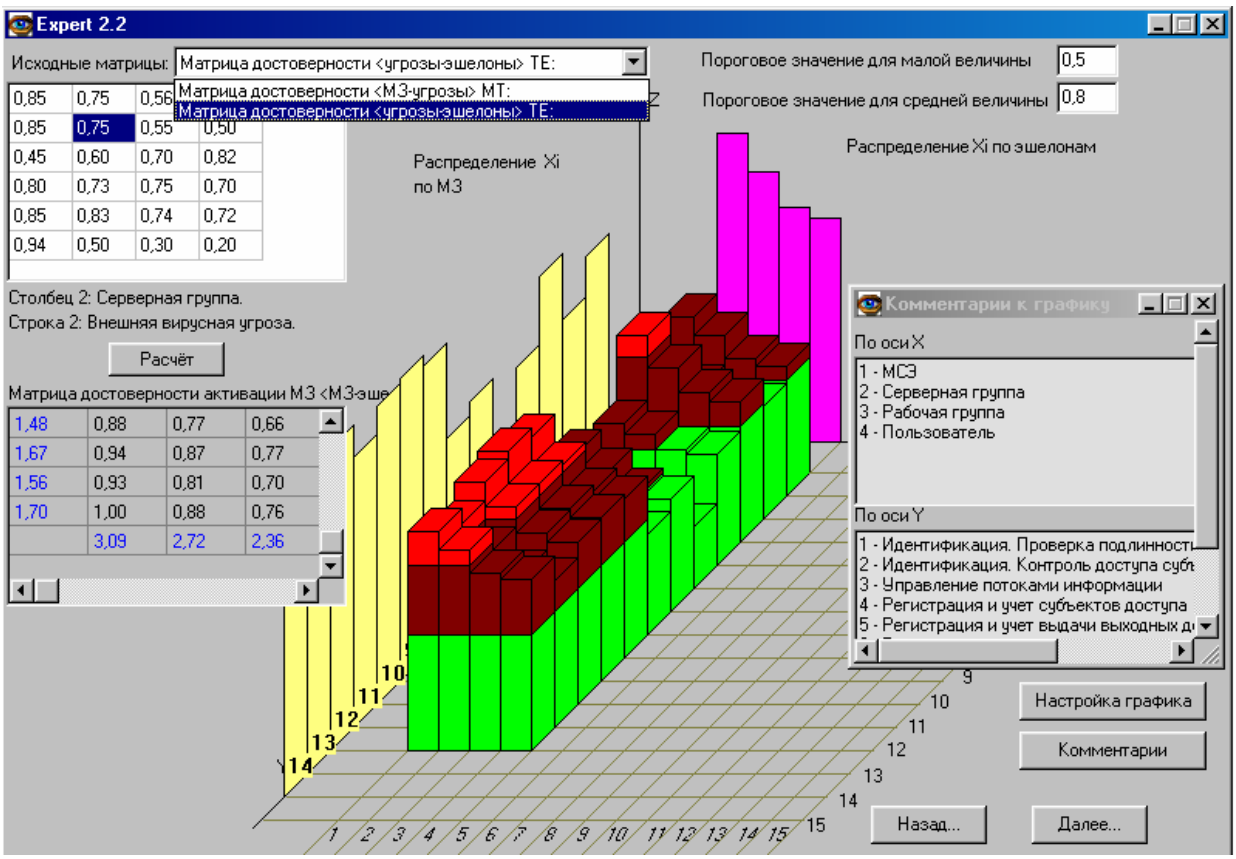
Expert 2.2
Исходные матрицы:
Матрица достоверности <угрозы-эшелоны> TE:
Матрица достоверности <МЗ-угрозы> MT:
Матрица достоверности <угрозы-эшелоны> TE:
Пороговое значение для малой величины
0,5
Пороговое значение для средней величины
0,8
Распределение Xi по МЗ
Распределение Xi по эшелонам
Столбец 2: Серверная группа.
Строка 2: Внешняя вирусная угроза.
Расчёт
Матрица достоверности активации МЗ <МЗ-эше
Комментарии к графику
По оси X
1 - МСЭ
2 - Серверная группа
3 - Рабочая группа
4 - Пользователь
По оси Y
Настройка графика
Комментарии
Назад...
Далее...

*Рис. 7.*

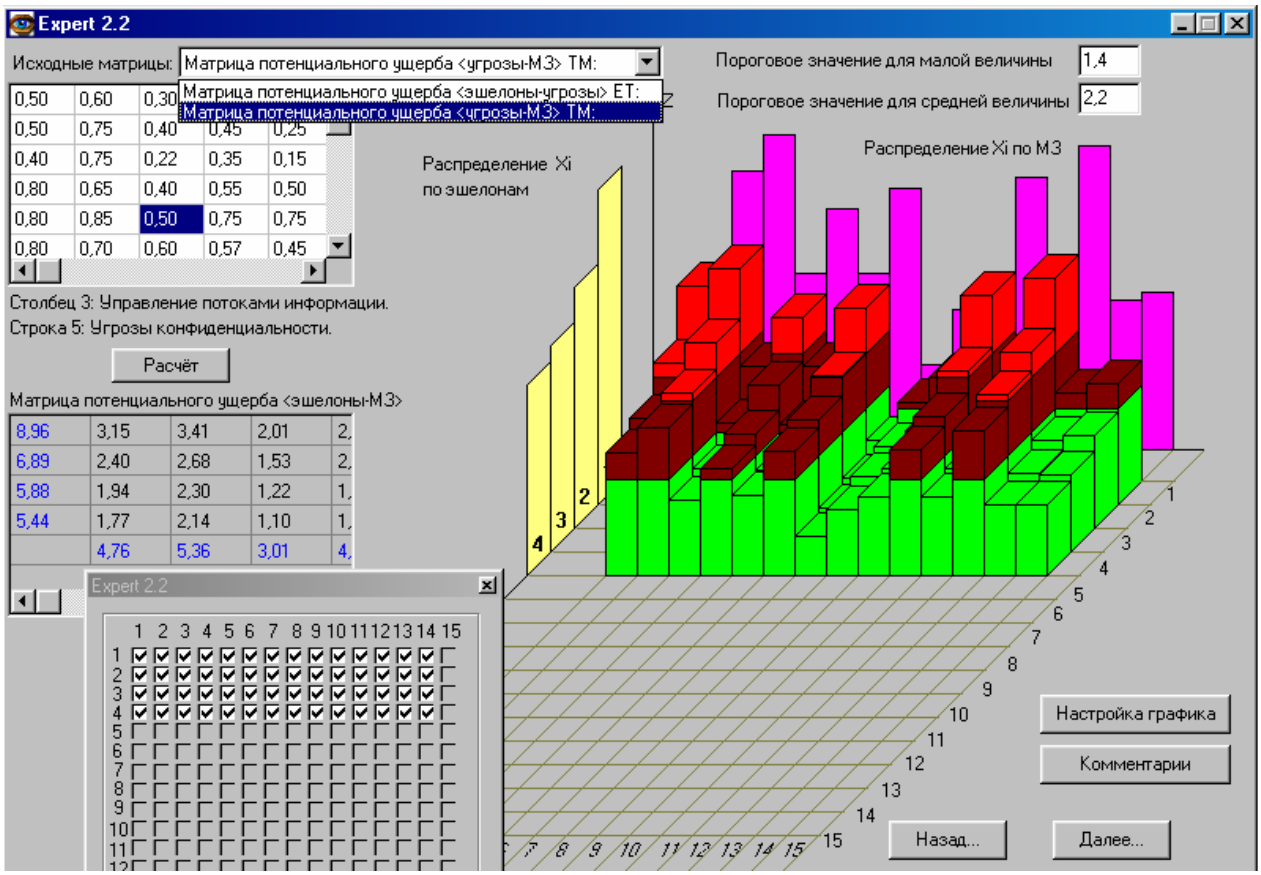
Expert 2.2
Исходные матрицы:
Матрица потенциального ущерба <угрозы-МЗ> TM:
Матрица потенциального ущерба <эшелоны-угрозы> ET:
Матрица потенциального ущерба <угрозы-МЗ> TM:
Пороговое значение для малой величины
1,4
Пороговое значение для средней величины
2,2
Распределение Xi по эшелонам
Распределение Xi по МЗ
Столбец 3: Управление потоками информации.
Строка 5: Угрозы конфиденциальности.
Расчёт
Матрица потенциального ущерба <эшелоны-МЗ>
Expert 2.2
Настройка графика
Комментарии
Назад...
Далее...

*Рис. 8.*

Для наглядности результаты расчетов матрицы «МЗ-эшелоны» представляются в виде трехмерной диаграммы распределения нечетких значений лингвистической переменной «Достоверность активации МЗ» в разрезе МЗ и эшелонов СИБ.

Диаграмма сопровождается распределением показателей значимости по механизмам защиты (плоскость *Y*0*Z* - выделена в окне желтым цветом) и эшелонам многоуровневой СИБ (плоскость *X*0*Z* - выделена сиреневым цветом). Двумерное поле в левом нижнем углу рис. 7 позволяет выборочно (путем отметки соответствующих элементов поля) просмотреть распределение нечетких значений лингвистической переменной «Достоверность активации МЗ» по строкам ил столбцам путем соответствующей отметки элементов поля.

Кнопка **Комментарии** позволяет с помощью одноименного окна установить соответствие нумерации по осям *X* и *Y* с активированными МЗ и эшелонами СИБ (рис. 7), кнопка **Назад** – вернуться к предыдущему окну, а кнопка **Далее** - перейти к последующим окнам (рис. 8 и 9), где аналогично рассмотренному производится ввод экспертных оценок и расчет матрицы «МЗ-эшелоны» для относительного потенциального ущерба от однократной активизации угроз и матрицы «МЗ-эшелоны» для частоты активации угроз.

Поэлементное умножение матриц относительного потенциального ущерба от однократной активизации угроз и матрицы «МЗ-эшелоны» для частоты активации угроз позволяет оценить ОПУ с учетом ЧАУ (рис. 10) и выполняется автоматически после завершения расчетов матриц «МЗ-эшелоны» для ДА, ОПУ и ЧАУ.Так как дальнейшие операции над матрицами *ME* и *EM* не требуют ввода дополнительных данных, то в следующем окне программы (рис. 11) отражены итоговые квадратные матрицы, обобщающие в элементах главной диагонали как показатель достоверности активации механизма защиты, так и потенциального ущерба от реализации атаки.

В частности умножением матрицы достоверности «МЗ-эшелоны» *ME* и матрицы относительного потенциального ущерба «эшелоны-МЗ» *EM* формируется квадратная *матрица достоверного потенциального ущерба* «МЗ-МЗ» *MM*. Аналогично умножением матрицы ОПУ «эшелоны-МЗ» *EM* и матрицы ДА «МЗ-эшелоны» *ME* получается квадратная матрица достоверного потенциального ущерба «эшелоны-эшелоны» *EE*.

Здесь же приведено распределение достоверного потенциального ущерба по механизмам защиты и эшелонам СИБ, а также интегральные оценки защищенности системы ИТ в разрезе механизмов защиты - рейтинговый показатель $R_M$ и эшелонов - рейтинговый показатель $R_E$.

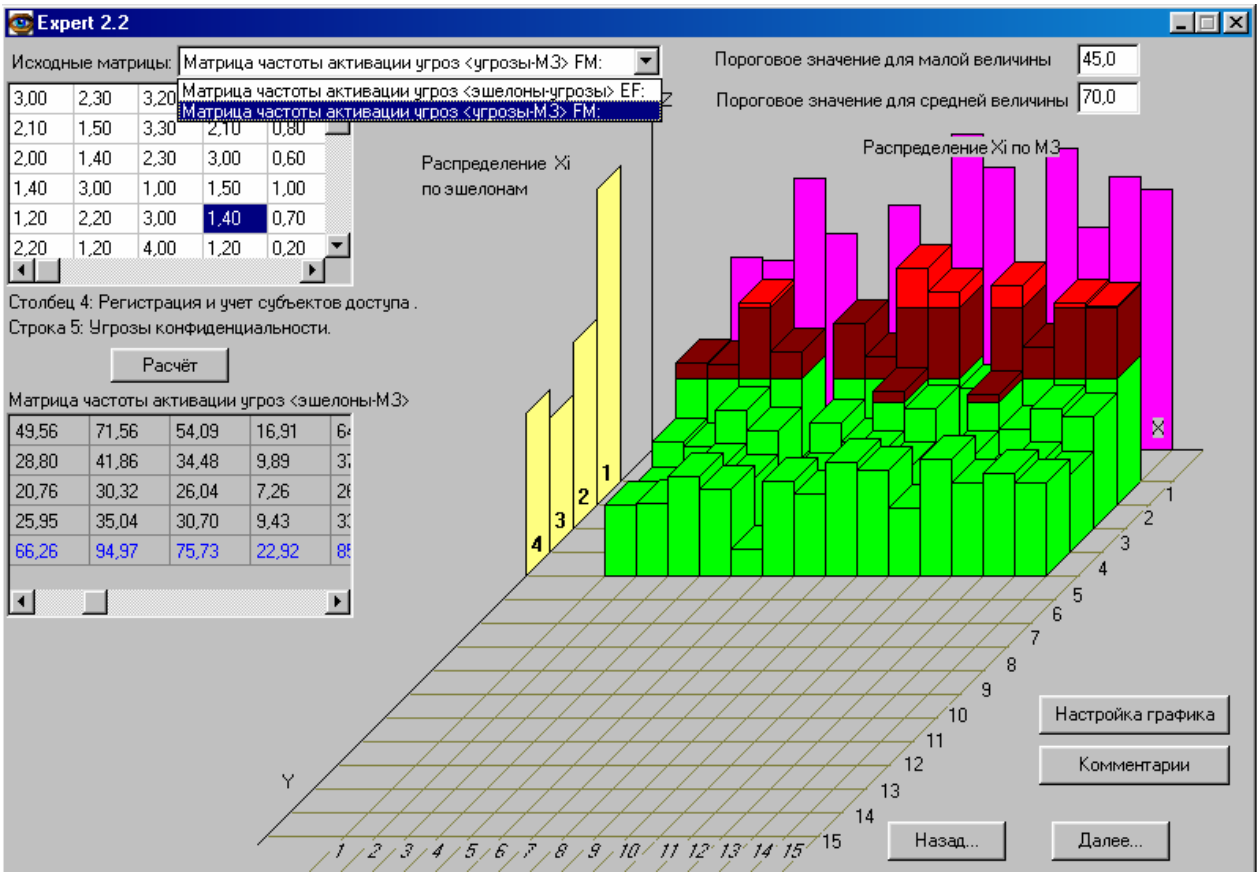
Expert 2.2
Исходные матрицы:
Матрица частоты активации угроз <угрозы-МЗ> FM:
Матрица частоты активации угроз <эшелоны-угрозы> EF:
Матрица частоты активации угроз <угрозы-МЗ> FM:
Пороговое значение для малой величины
45,0
Пороговое значение для средней величины
70,0
Распределение Xi по эшелонам
Распределение Xi по МЗ
Столбец 4: Регистрация и учет субъектов доступа .
Строка 5: Угрозы конфиденциальности.
Расчёт
Матрица частоты активации угроз <эшелоны-МЗ>
Настройка графика
Комментарии
Назад...
Далее...

*Рис. 9.*

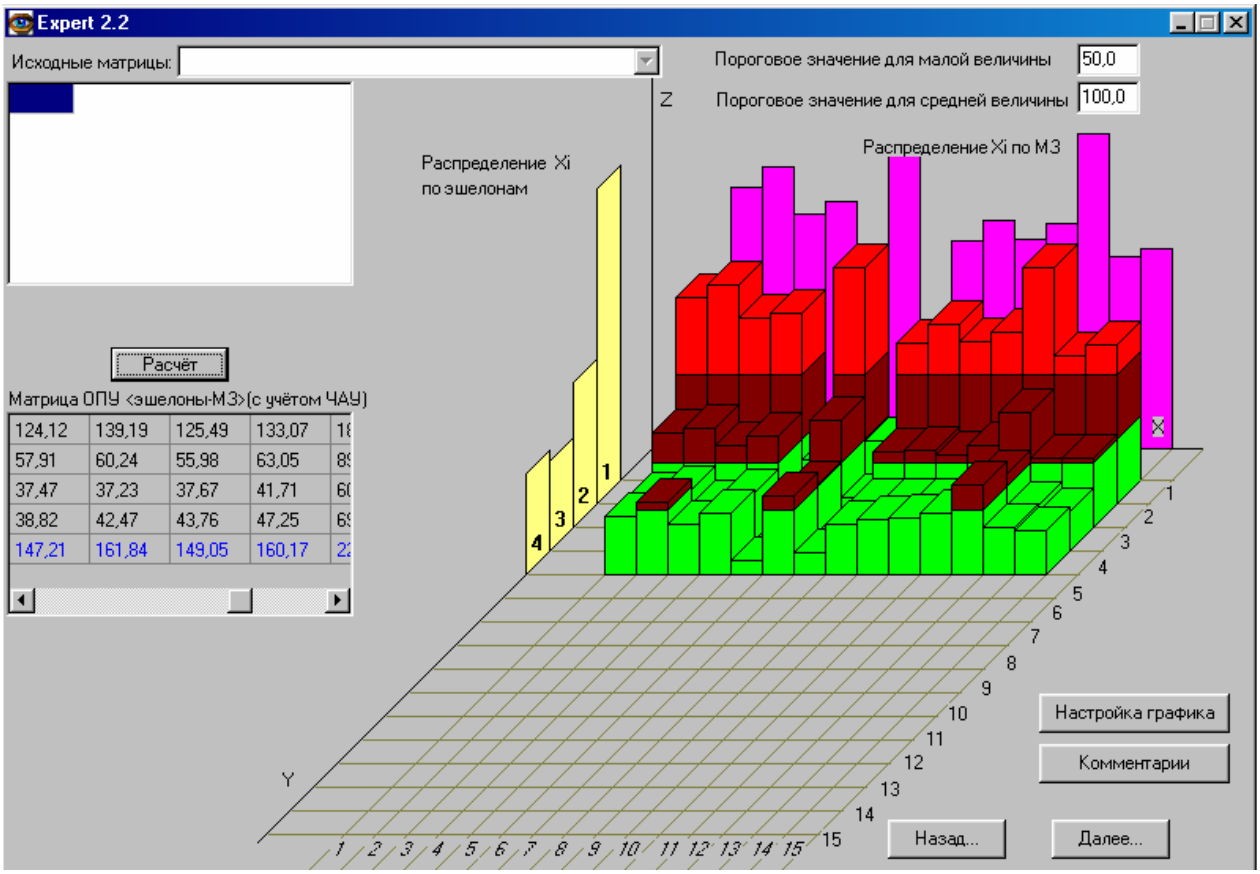
Expert 2.2
Исходные матрицы:
Пороговое значение для малой величины
50,0
Пороговое значение для средней величины
100,0
Распределение Xi по эшелонам
Распределение Xi по МЗ
Расчёт
Матрица ОПУ <эшелоны-МЗ>(с учётом ЧАУ)
Настройка графика
Комментарии
Назад...
Далее...

*Рис. 10.*

## Методика применения инструментальных средств для анализа системы защиты информации

Программа используется в динамической модели адаптивной защиты для анализа последствий реализации угрозы, приведшей к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение (*постактивация* МЗ) либо моделирования возможных последствий атак из множества *известных угроз* для определения положения в многоуровневой СИБ механизмов защиты, включение которых в иерархию СИБ предотвратит появление ущерба, превышающего пороговый уровень (*предактивация* МЗ).

Предактивация МЗ позволяет в результате моделирования активности угроз, путем целенаправленного или эволюционного изменения экспертных оценок (исходных матриц) выявить механизмы защиты, активация которых целесообразна, если величина ОПУ превышает допустимые значения. Постактивация МЗ является следствием расширения поля угроз за счет реализации (в результате атаки) ранее неизвестной угрозы в системе ИТ.

Для проведения анализа влияния угроз из числа специфицированных (отмечены в списке **Угрозы** в первом окне программы) на показатели защищенности системы ИТ следует в окне программы, представленном на рис. 11, выбрать кнопку **Далее** для перехода к окну выбора угрозы, подлежащей анализу (рис. 12).

1. В каждом из списков: **Анализируемые угрозы**, **Анализируемые механизмы** и **Анализируемые эшелоны** необходимо отметить подлежащую анализу угрозу в разрезе конкретного механизм защиты и эшелона СИБ.
2. Задаются величины допустимого относительного потенциального ущерба (низкое и высокое) относительно текущего значения, используемые в качестве параметров.
3. Кнопкой **Графики** инициируется отображение динамики изменения рейтинговых показателей защищенности в зависимости от ЧАУ, где в качестве параметров выступает допустимая величина ОПУ.
4. Анализ динамики изменения рейтинговых показателей позволяет выбрать наиболее критичные МЗ и эшелоны СИБ для обеспечения информационной безопасности системы ИТ.
5. Для предактивации МЗ необходим анализ потенциального ущерба от возможной реализации в системе ИТ ранее не активированных угроз. С этой целью следует выполнить следующую последовательность шагов:

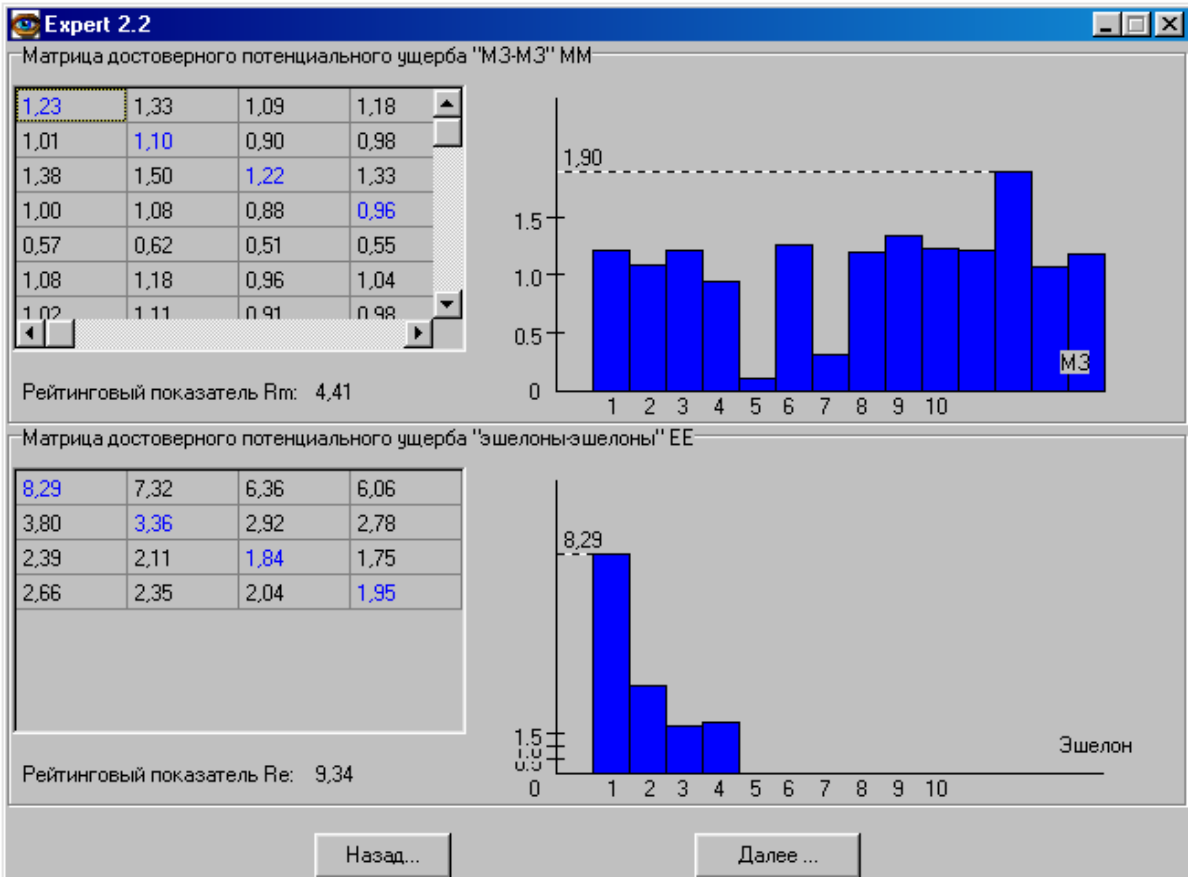
Expert 2.2
Матрица достоверного потенциального ущерба "МЗ-МЗ" ММ
1,23 1,33 1,09 1,18
1,01 1,10 0,90 0,98
1,38 1,50 1,22 1,33
1,00 1,08 0,88 0,96
0,57 0,62 0,51 0,55
1,08 1,18 0,96 1,04
Рейтинговый показатель Rm: 4,41
1,90
1.5
1.0
0.5
0
1 2 3 4 5 6 7 8 9 10
МЗ
Матрица достоверного потенциального ущерба "эшелоны-эшелоны" ЕЕ
8,29 7,32 6,36 6,06
3,80 3,36 2,92 2,78
2,39 2,11 1,84 1,75
2,66 2,35 2,04 1,95
Рейтинговый показатель Re: 9,34
8,29
1.5
0
1 2 3 4 5 6 7 8 9 10
Эшелон
Назад...
Далее ...

*Рис. 11.*

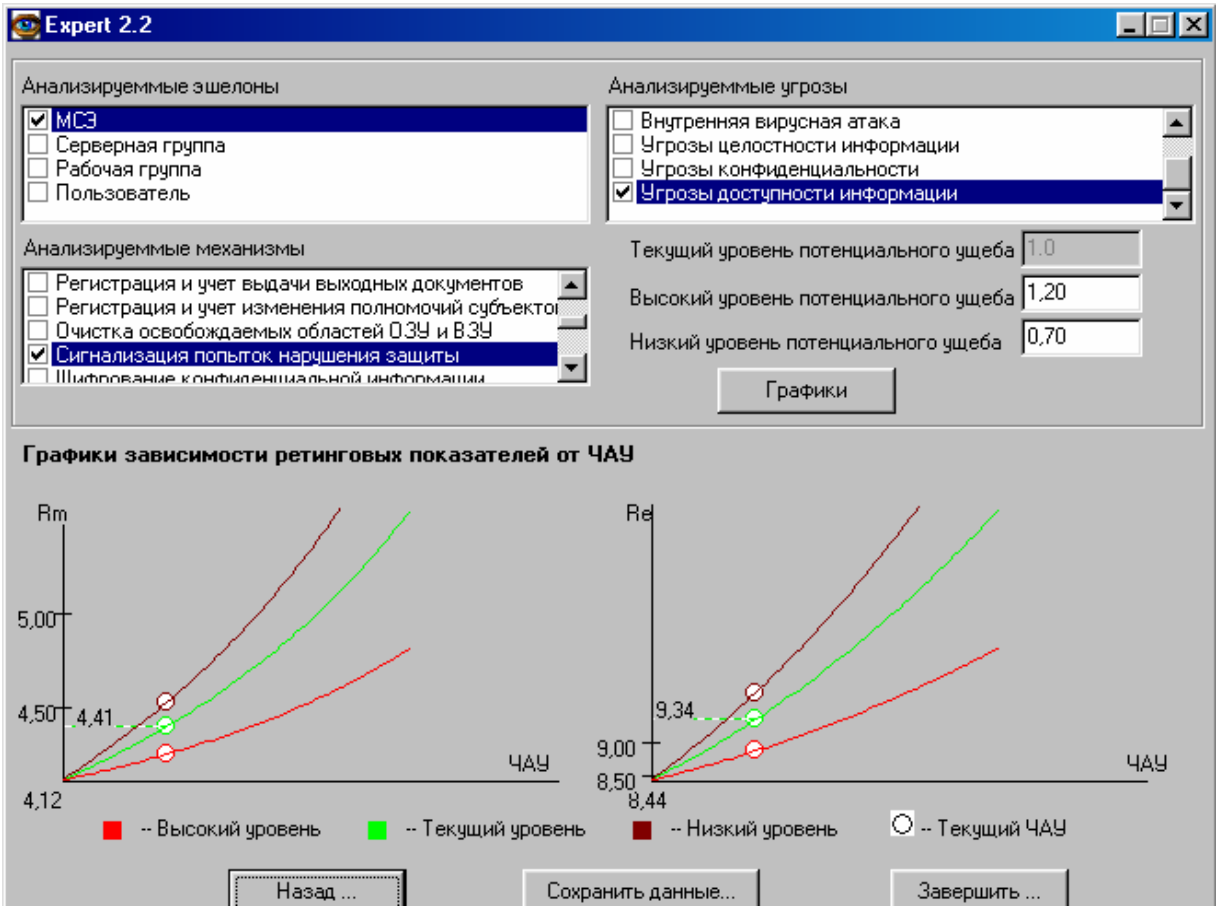
Expert 2.2
Анализируемые эшелоны
МСЭ
Серверная группа
Рабочая группа
Пользователь
Анализируемые угрозы
Внутренняя вирусная атака
Угрозы целостности информации
Угрозы конфиденциальности
Угрозы доступности информации
Анализируемые механизмы
Регистрация и учет выдачи выходных документов
Очистка освобождаемых областей ОЗУ и ВЗУ
Сигнализация попыток нарушения защиты
Текущий уровень потенциального ущеба 1.0
Высокий уровень потенциального ущеба 1,20
Низкий уровень потенциального ущеба 0,70
Графики
Графики зависимости ретинговых показателей от ЧАУ
Rm
5,00
4,50
4,41
4,12
ЧАУ
Re
9,34
9,00
8,50
8,44
ЧАУ
-- Высокий уровень
-- Текущий уровень
-- Низкий уровень
-- Текущий ЧАУ
Назад ...
Сохранить данные...
Завершить ...

*Рис. 12.*

а. в первом окне программы в списке **Угрозы** с помощью кнопки **Добавить** и соответствующего окна ввести в список наименование угрозы, подлежащей анализу, и отметить в соответствующем поле признак активности вновь введенной угрозы;

б. в связи с приращением измерения «угрозы» в окнах 2 - 4 провести коррекцию исходных матриц путем формирования и ввода экспертных оценок по вновь введенной угрозе по ДА, ОПУ и ЧАУ;

в. коррекция исходных матриц сопровождается проведением расчетов (кнопка **Расчет**), в результате которых изменения претерпевают все производные матрицы, показатели значимости, рейтинговые показатели;

г. придать введенной угрозе на время анализа статус специфицированной. Далее повторить П. 1 - 4 настоящего параграфа.

6. Если для введенной угрозы динамика рейтинговых показателей при увеличении ЧАУ недостаточно высока, то необходимо расширить перечень активированных механизмов защиты. С этой целью следует выполнить следующую последовательность шагов:

   а. в первом окне программы в списке **Механизмы** отметить в соответствующем поле признак активности неактивного до настоящего момента МЗ, который по мнению экспертов должен с максимальной достоверностью нейтрализовать угрозу, подлежащей анализу;

   б. в связи с приращением измерения «МЗ» в окнах со 2 по 4 провести коррекцию исходных матриц путем формирования и ввода экспертных оценок по активированному механизму защиты по ДА, ОПУ и ЧАУ;

   в. коррекция исходных матриц сопровождается проведением расчетов (кнопка **Расчет**), в результате которых формируются все производные матрицы, показатели значимости, рейтинговые показатели. Далее - П. 1 – 4 настоящего параграфа.

7. Если для введенной угрозы вновь активированный МЗ (1) улучшил динамику рейтинговых показателей при увеличении ЧАУ и (2) расчетное значение ОПУ для активированного МЗ превысило допустимое для лингвистической переменной «ОПУ с учетом ЧАУ» значение - «большая величина» (красный цвет элемента трехмерной диаграммы, представленной на рис. 10), то дается рекомендация расширить перечень активированных механизмов защиты для системы ИТ данного хозяйствующего субъекта. Иначе с п. 6 для иного МЗ, предварительно сняв отметку с неудовлетворившего условиям п. 7 механизма защиты, до тех пор пока не завершится перебор всех неактивированных МЗ.

8. Действия П. 5 - 7 повторить для каждой из неспецифицированной угроз, оставляя активными только те из них, которые привели к повышению рейтинговых показателей СИБ за счет активного использования (предотвращения потенциального ущерба) имеющегося набора МЗ или вновь введенного механизма защиты.
9. Постактивация МЗ – следствие предотвращения повторения уже реализованной в системе ИТ угрозы, приведшей к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение, вызывает выполнение действий в соответствии с П. 5.а – 7.
10. Если для всех эшелонов СИБ выполнены П. 5 – 9, то анализ системы ИТ завершен. Иначе следует выполнить следующую последовательность шагов:
    а. в первом окне программы в списке **Эшелоны** отметить в соответствующем поле признак активности неактивного до настоящего момента эшелона СИБ, который по мнению экспертов должен улучшить рейтинговые показатели СИБ;
    б. в связи с приращением измерения «эшелоны» в окнах программы со 2 по 4 провести коррекцию исходных матриц путем формирования и ввода экспертных оценок по активированному эшелону СИБ по ДА, ОПУ и ЧАУ;
    в. коррекция исходных матриц сопровождается проведением расчетов (кнопка **Расчет**), в результате которых формируются все производные матрицы, показатели значимости, рейтинговые показатели. Далее - П. 1 – 4 настоящего параграфа.
11. Выполнить П. 5 – 9 для анализа поля известных угроз и механизмов защиты.
12. Если отметка эшелона улучшила рейтинговые показатели СИБ за счет активации МЗ, то дается рекомендация расширить перечень эшелонов защиты в системе ИТ данного хозяйствующего субъекта. Иначе с п. 10 для иного эшелона СИБ, предварительно сняв отметку с неудовлетворившего условию п. 12 эшелона.

Рассмотренная выше методика на основе анализа системы показателей применима для оценки защищенности системы ИТ как по всему полю известных угроз, так и по заданному подмножеству поля угроз. В последнем случае СИБ обретает специализацию по типу потенциальных угроз, а процесс анализа упрощается за счет снижения размерности исходных матриц.

# 3. Задания

## 3.1. Задание на лаб. раб № 1

## «Знакомство с показателями информационной защищенности ИТ-системы и инструментальными средствами «Эксперт»

1. Ознакомиться с системой показателей для оценки информационной защищенности ИТ-системы.
2. Запустить программу **Expert.exe** и в первом окне программы в интерактивном режиме сформировать перечень известных угроз, механизмов защиты и иерархии эшелонов защиты ИТ-системы, сохранив его в файле **default1.dic**.
3. Отметить в списках первого окна программы заданный преподавателем набор угроз, используемых механизмов защиты и перечень эшелонов системы защиты, т. е. определить распределение конкретных механизмов защиты по эшелонам ИТ-системы.
4. В соответствии с п. 3 сформировать матрицы экспертных оценок «МЗ-угрозы» и «Угрозы-эшелоны» для достоверности активации - ДА механизмов защиты.
5. Провести расчет матрицы «МЗ-эшелоны», определяющей распределение ДА по механизмам защиты и эшелонам на заданном множестве известных угроз. Проанализировать активность СИБ в разрезе использования конкретных механизмов защиты и эшелонов ИТ-системы. Обратить внимание на интегральные показатели активности МЗ и эшелонов ИТ-системы.
6. Действия, аналогичные П. 4 и 5, повторить в окнах программы для относительного потенциального ущерба (ОПУ) и частоты активации угроз (ЧАУ).
7. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов для ИТ-системы в целом, а также показатели активности отдельных эшелонов и МЗ.
8. Сохранить в файле **save0.sav** текущее состояние адаптивной СИБ для дальнейших исследований.
9. Показать преподавателю полученные результаты расчетов и результаты вашего анализа адаптивной СИБ.

### 3.2. Задание на лаб. раб № 2

### «Анализ системы адаптивной защиты»

1. Запустить программу ***Expert*** и загрузить данные из файла **save0.sav**, содержащего результаты предыдущей лабораторной работы.
2. Получить от преподавателя вариант многоуровневой СИБ, т. е. индивидуальное распределение конкретных механизмов защиты по эшелонам ИТ-системы
3. В соответствии с п. 2 сформировать матрицы экспертных оценок «МЗ-угрозы» и «Угрозы-эшелоны» для достоверности активации механизмов защиты.
4. Провести расчет матрицы «МЗ-эшелоны», определяющей распределение ДА по механизмам защиты и уровням адаптивной СИБ на заданном множестве известных угроз. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов ИТ-системы. Обратить внимание на интегральные показатели активности МЗ и эшелонов СИБ.
5. Действия, аналогичные П. 3 и 4, повторить в окнах программы для относительного потенциального ущерба (ОПУ) и частоты активации угроз (ЧАУ).
6. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов для ИТ-системы в целом, а также показатели активности отдельных эшелонов и МЗ.
7. Сохранить в файле **save1.sav** текущее состояние адаптивной СИБ для дальнейших исследований.
8. Показать преподавателю полученные результаты расчетов и результаты вашего анализа адаптивной системы защиты информации.
9. Сформулировать предложения по улучшения рейтинга ИТ-системы.

### 3.3. Задание на лаб. раб № 3

### «Исследование системы адаптивной защиты»

1. Запустить программу ***Expert*** и загрузить данные из файла **save1.sav**, содержащего результаты предыдущей лабораторной работы.
2. На основании результатов, полученных в П. 8 и 9 предыдущей лабораторной работы, внести коррективы в многостраничную структуру ИТ-системы, т. е. изменения в исходное распределение конкретных механизмов защиты по эшелонам СИБ.

3. В соответствии с п. 2 откорректировать матрицы экспертных оценок «МЗ-угрозы» и «Угрозы-эшелоны» для достоверности активации механизмов защиты, т. к. изменение, внесенные в п. 2, приведут к увеличению размерности матриц «МЗ-угрозы» и «Угрозы-эшелоны» (по умолчанию дополнительные строки и столбцы матриц заполняются нулями, а вам необходимо ввести конкретные значения экспертных оценок).
4. Провести расчет матрицы «МЗ-Эшелоны», определяющей распределение ДА по механизмам защиты и эшелонам СИБ на заданном множестве известных угроз. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов СИБ. Обратить внимание на интегральные показатели активности МЗР и эшелонов СИБ.
5. Действия, аналогичные П.3 и 4, повторить в окнах программы для относительного потенциального ущерба (ОПУ) и частоты активации угроз (ЧАУ).
6. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов для ИТ-системы в целом, а также показатели активности отдельных эшелонов и МЗ.
7. Воспользовавшись методикой применения программы «Эксперт» для анализа информационной защищенности ИТ-системы, определить конкретные механизмы защиты, обеспечивающие наибольшую динамику рейтинговых показателей.
8. Сохранить в файле **save2.sav** текущее состояние адаптивной СИБ для дальнейших исследований.
9. Повторить действия П. 2 – 7 и сохранить полученный вариант адаптивной СИБ в файле **save3.sav**
10. Сравнить многоуровневую структуру СИБ и рейтинговые показатели для вариантов адаптивной защиты, соответствующих файлам **save1.sav – save3.sav.**
11. Показать преподавателю результаты исследования адаптивной системы защиты информации.

## Литературные источники

1. Нестерук Г. Ф., Фахрутдинов Р. Ш., Нестерук Ф. Г. К разработке инструментальных средств для мониторинга защищенности корпоративной сети // Сб. докл. VIII Междунар. конф. SCM'2005. – СПб.: СПГЭТУ, 2005.

2. Минаев В. А. Перспективы развития IT-security в России // Межотраслевой тематический каталог "Системы безопасности-2003". 2003, С. 218 – 221.

3. Осовецкий Л. Г. Научно-технические предпосылки роста роли защиты информации в современных информационных технологиях // Изв. вузов. Приборостроение. 2003. Т.46, № 7. С. 5-18

4. Осовецкий Л. Г., Нестерук Г. Ф., Бормотов В. М. К вопросу иммунологии сложных информационных систем // Изв. вузов. Приборостроение. 2003. Т.46, № 7. С. 34-40

5. Вихорев С. В., Кобцев Р. Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент. 2002. № 2.

6. Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. Адаптивная модель нейросетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные системы. 2003, №3.

7. Нестерук Г.Ф., Куприянов М.С., Нестерук Ф. Г., Нестерук Л. Г. Методика оценки защищенности информационных систем с применением НС и нечеткой логики // SCM'2004: Сборник докладов VI Международной конференции по мягким вычислениям и измерениям. Т.1. – СПб.: СПбГЭТУ, 2004

8. Нестерук Ф. Г., Осовецкий Л.Г., Жигулин Г. П., Нестерук Т.Н. Разработка комплекса показателей для оценки информационных ресурсов и безопасности иерархических систем // РИ-2004: Материалы IX Санкт-Петербургской международной конференции Региональная информатика - 2004 г. – СПб.: СПИИ РАН, 2004

9. Нестерук Г.Ф., Осовецкий Л. Г., Нестерук Ф. Г. К оценке защищенности систем информационных технологий // Перспективные информационные технологии и интеллектуальные системы. 2004, № 1

10.Нестерук Г.Ф., Куприянов М.С., Осовецкий Л.Г., Нестерук Ф.Г. Разработка инструментальных средств для оценки защищенности информационных систем с применением механизмов нечеткой логики и нейронных сетей // SCM'2004: Сборник докладов VII Международной конференции по мягким вычислениям и измерениям. Т.1. – СПб.: СПбГЭТУ, 2004.

11.Осовецкий Л., Шевченко В. Оценка защищенности сетей и систем // Экспресс электроника. 2002. № 2 - 3. С.20-24.

12.Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В. Базы данных. Интеллектуальная обработка информации. – М.: Нолидж, 2001.

# Содержание