менение» SSA'2004, 26-28 октября 2004 г., Минск, – Минск.: ОИПИ НАН Беларуси, 2004, – С. 238-243.

5. *Анищенко В.В., Криштофик А. М.* Базовая модель системы защиты активов объекта информационных технологий // Материалы докладов и краткие сообщения II Белорусско-российской научно-техн. конф. «Технические средства защиты информации», 17 мая-21 мая 2004, Минск-Нарочь. Доклады БГУИР. –2004. № 5. – С. 9.

6. *Анищенко В.В., Криштофик А. М.* Влияние уязвимостей средств защиты на безопасность объектов информационных технологий // Материалы IX Международной конференции «Комплексная защита информации», 1-3 марта 2005 г., Раубичи (Беларусь). – Минск: ОИПИ НАН Беларуси, 2005, – С.52-54.

7. *Анищенко В.В., Криштофик А. М.* Методика оценки защищенности автоматизированных систем при повышенных требованиях безопасности // Тезисы докладов Международной научной конференции по военно-техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения. – Минск: БелИСА, 2005, – С. 150-151

8. *Анищенко В.В., Криштофик А.М.* Показатели защищенности информационных систем // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. – Минск: Академия управления, 2004, – С. 30-33

9. *Анищенко В.В., Криштофик А.М.* Комплексный подход к ранжированию уязвимостей информационных систем // Материалы конференции «Обеспечение безопасности информации в информационных системах», Минск, 11 ноября 2004 г. – Минск: Академия управления, 2004, –С. 36-39.

10. *Анищенко В.В., Криштофик А.М.* Этапы проведения оценки защищенности объектов информационных технологий // Материалы IX Международной конференции «Комплексная защита информации», 1-3 марта 2005 г., Раубичи (Беларусь). – Минск: ОИПИ НАН Беларуси, 2005, – С55-57.

11. *Криштофик А.М., Анищенко В.В.* Управление информационной безопасностью на основе системного анализа рисков//Доклады пятой междун. конференции «Обработка информации и управление в чрезвычайных и экстремальных ситуациях». – Минск: ОИПИ НАН Беларуси, 2006, – С.117-122.

12. *Криштофик А.М.* Модель комплексной оценки потенциала атаки // Материалы X междун. конференции «Комплексная защита информации». – Мн.: Амалфея, 2006, – С.111-113

13. *Криштофик А.М.* Модель оценки уязвимости системы защиты информации //Материалы третьей междун. конференции «Информационные системы и технологии», IST'2006. – Минск: Академия управления при Президенте РБ, 2006. – С.109 -114.

И.В. Машкина
Россия, г. Уфа, УГАТУ

ПОДСИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОМУ УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ

Для успешного использования современных информационных технологий необходимо *эффективное управление* не только сетью, но и системой защиты информации (СЗИ). В число задач управления защитой информации (ЗИ) входит обеспечение работы проектной группы приложений: определение *модульного состава* и *точек установки* средств защиты (СрЗ) в сети предприятия [1].

Это обусловлено тем, что защита информации – это не разовое мероприятие и не совокупность средств защиты, а непрерывный *целенаправленный процесс*, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы (ИС). При этом важными аспектами обеспечения безопасности информации являются принципы комплексности, гибкости системы

защиты и разумной достаточности [2]. Принцип комплексности предполагает *согласованное применение* разнородных средств при построении целостной СЗИ, принцип гибкости – способность системы защиты соответствовать целям и задачам бизнес-процессов и не снижать производительность ИС, обеспечивать возможность *варьирования уровнем защищенности*. Принцип разумной достаточности основывается на том, что создать абсолютно непреодолимую СЗИ принципиально невозможно, важно выбрать тот достаточный уровень защищенности, при котором затраты и размер *возможного ущерба*, то есть риск, были бы *приемлемы*.

Повышение эффективности мероприятий по ЗИ возможно в интеллектуальной СЗИ, функционирование которой организовано в соответствии с принципом управления защитой информации

Целью статьи является описание результатов разработки подсистемы поддержки принятия решений интеллектуальной СЗИ. Современные СЗИ не обладают свойством интеллектуальности, что требует решения ряда научных задач, направленных на разработку практически применимых моделей и методов интеллектуального обеспечения ЗИ. В [3] отмечается, что одно из требований, которым должна удовлетворять такая система – это автоматизированная *поддержка принятия решений* о перераспределении ресурсов СЗИ.

Назовем подсистемой поддержки принятия решений по организационно-техническому управлению (ППРР ОТУ) автоматизированную систему, в которой в течение всего периода функционирования объекта информатизации (ОИ) при активном использовании экспертной информации осуществляется принятие решений по выбору рационального варианта системы защиты в зависимости от требуемого уровня защищенности информации.

В настоящее время при выборе комплексов средств защиты предлагается руководствоваться принятыми международными стандартами, которые представляют собой библиотеку функциональных требований. Такому подходу присущи принципиальные недостатки [4]: сложность получения системных решений, адекватных стратегии и тактике защиты, и отсутствие расчетных соотношений и количественных показателей эффективности системы защиты.

В ППРР ОТУ в виде *специального программного обеспечения* (ПО) реализуется методика выбора рациональных наборов средств защиты и точек их установки при обработке на ОИ информации с различными уровнями ограничения доступа.

ПО позволяет производить поиск рациональных вариантов системы защиты в зависимости от условий поиска, создать и корректировать базы данных средств защиты и базы знаний каналов несанкционированного доступа, утечки и деструктивных воздействий на информацию, организовать работу экспертов для получения экспертных оценок СрЗ.

Управляющее воздействие – *плановая командная информация* – доводится до объекта управления администратором безопасности или сотрудниками отдела информационной безопасности. Формирование управляющих воздействий имеет плановый характер и зависит от изменения планов обработки информации на ОИ.

Практическая реализация ППРР ОТУ возможна при условии создания базы декларативных и процедурных знаний, а также методической базы для ее разработки.

Основанием для разработки базы знаний ППРР ОТУ послужила разработанная (на основе комбинаторно-морфологического метода синтеза) методика выбора рациональных наборов средств защиты [5]. В работе [5] предложен методический подход: принцип построения СЗИ на основе трехрубежной модели защиты и *расчетные соотношения*, позволяющие на научной основе синтезировать систему

защиты информации от внешних и внутренних преднамеренных угроз. Этот подход целесообразно использовать, поскольку он позволяет осуществлять многокритериальный и многоальтернативный выбор, когда наборы СрЗ синтезируются из некоторого множества функциональных подсистем, и каждая подсистема имеет более одной элементарной альтернативы для ее реализации.

Совокупность знаний, необходимых для синтеза рационального варианта СЗИ, записывается в форме, понятной эксперту и лицу, принимающему решение (ЛПР). Содержимое базы знаний формируется заранее, а также в процессе функционирования системы.

В ППРР ОТУ реализуется механизм приобретения знаний. Приобретение знаний в интеллектуальной системе – процесс взаимодействия эксперта с автоматизированной системой, которая обеспечивает ввод данных и знаний, их расширение, модификацию, корректировку, тестирование. Предполагается разработка инженером по знаниям структуры знаний (поля знаний). Происходит физическое наполнение базы знаний экспертом и настройка всех механизмов в рамках выбранного инструментального средства. Структура исходных данных подлежит интерпретации и обработке.

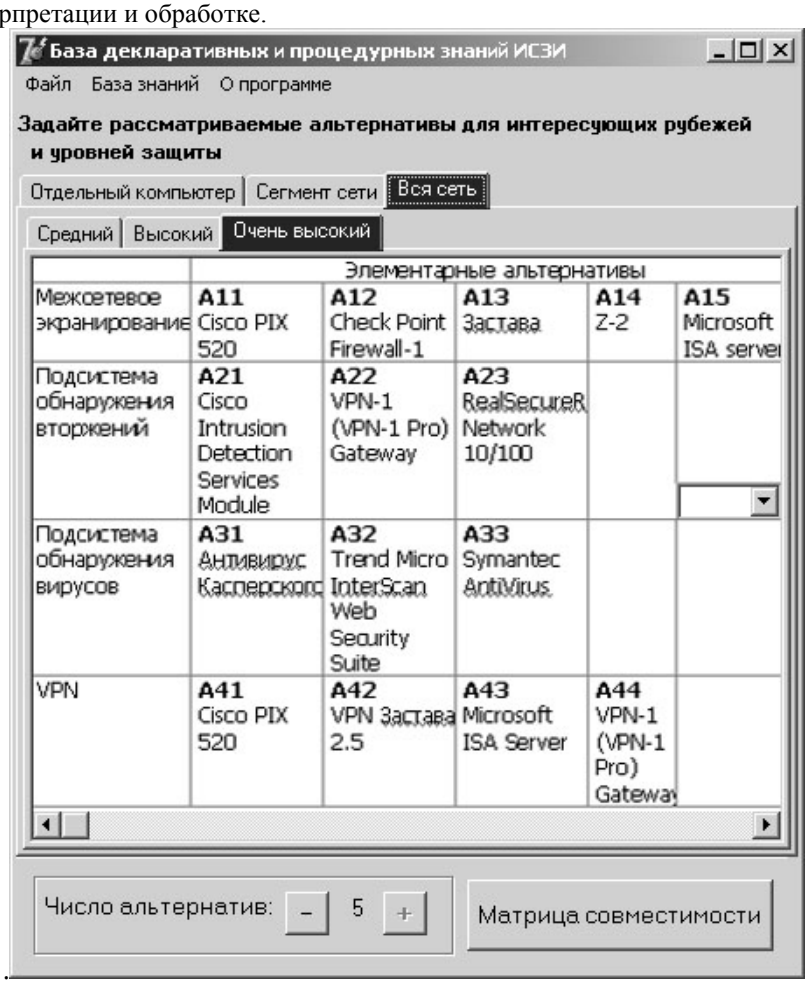


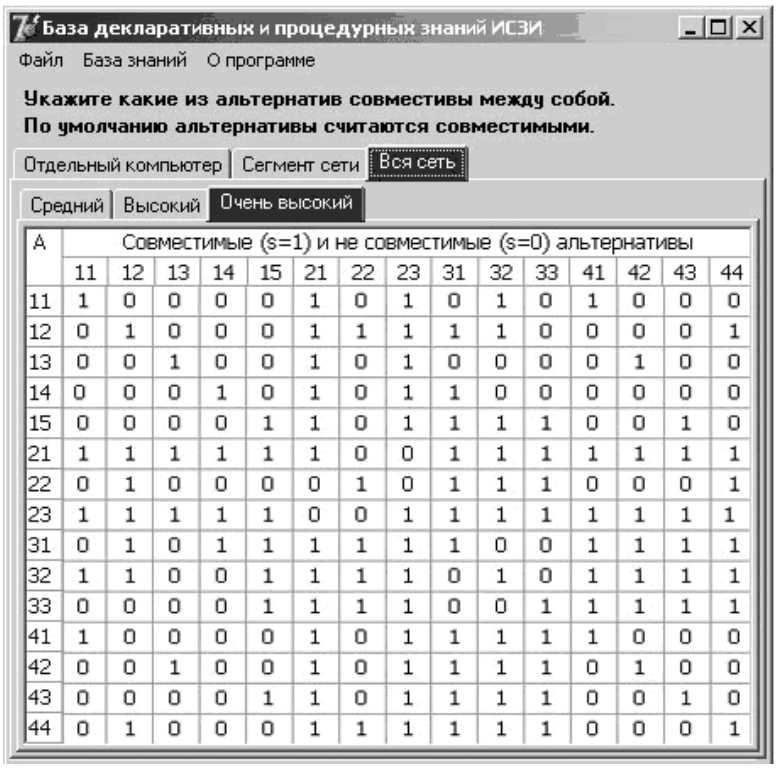
Рис.1. Комбинаторно-морфологическая матрица альтернатив для формирования набора средств защиты периметра ОИ

Разработанная ППППР ОТУ использует при функционировании следующие *знания эксперта*:

- в соответствии с созданными на основе существующих стандартов профилями безопасности эксперт формирует девять комбинаторно-морфологических матриц для трех рубежей защиты (периметр ОИ, сегмент, рабочая станция или сервер) и трех уровней ограничения доступа; каждая матрица представляет собой многовариантную объектную модель рубежа защиты;
- эксперт заполняет поле знаний – вспомогательные матрицы, в которых он отмечает совместимые друг с другом программно-аппаратные средства;
- экспертом разрабатывается система иерархических критериев качества для сравнения альтернатив каждой функциональной подсистемы по двум глобальным критериям: «защищенность» и «издержки»;
- на основе предложенных инженером по знаниям шкал относительной важности критериев и альтернатив для получения численных оценок альтернатив по группе критериев, отражающих свойство «защищенность», и группе критериев, отражающих свойство «издержки», эксперт заполняет матрицы попарных сравнений альтернатив по нижнему иерархическому уровню и матрицы попарных сравнений критериев по всем уровням иерархии.

Пример декларативных знаний – комбинаторно-морфологическая матрица альтернатив, которая заполняется экспертом для выбора рационального набора средств защиты периметра, приведена на рис.1

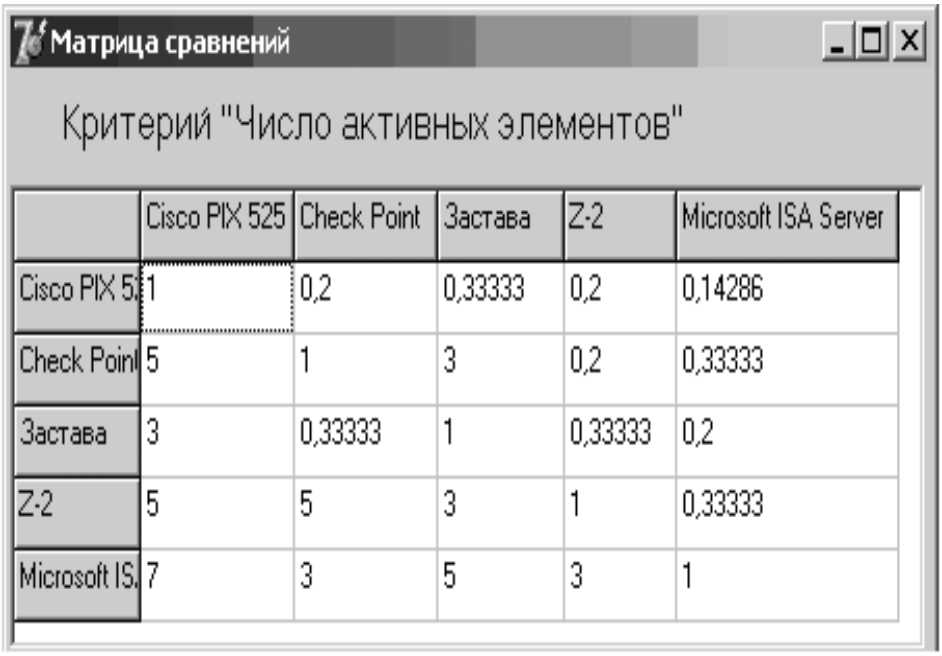
Пример декларативных знаний – вспомогательная матрица, в которой экспертом отмечены совместимые друг с другом средства защиты, приведена на рис.2.



A	Совместимые (s=1) и не совместимые (s=0) альтернативы														
	11	12	13	14	15	21	22	23	31	32	33	41	42	43	44
11	1	0	0	0	0	1	0	1	0	1	0	1	0	0	0
12	0	1	0	0	0	1	1	1	1	1	0	0	0	0	1
13	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0
14	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0
15	0	0	0	0	1	1	0	1	1	1	1	0	0	1	0
21	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1
22	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1
23	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1
31	0	1	0	1	1	1	1	1	1	0	0	1	1	1	1
32	1	1	0	0	1	1	1	1	0	1	0	1	1	1	1
33	0	0	0	0	1	1	1	1	0	0	1	1	1	1	1
41	1	0	0	0	0	1	0	1	1	1	1	1	0	0	0
42	0	0	1	0	0	1	0	1	1	1	1	0	1	0	0
43	0	0	0	0	1	1	0	1	1	1	1	0	0	1	0
44	0	1	0	0	0	1	1	1	1	1	1	0	0	0	1

Рис.2. Вспомогательная матрица совместимости

Пример декларативных знаний – матрица попарных сравнений альтернатив по одному из критериев приведена на рис.3.



	Cisco PIX 525	Check Point	Застава	Z-2	Microsoft ISA Server
Cisco PIX 5	1	0,2	0,33333	0,2	0,14286
Check Poin	5	1	3	0,2	0,33333
Застава	3	0,33333	1	0,33333	0,2
Z-2	5	5	3	1	0,33333
Microsoft IS	7	3	5	3	1

Рис.3. Матрица попарных сравнений альтернатив

Таким образом формируются декларативные знания. Далее для получения результатов, которых ожидает от ПППР ОТУ пользователь или ЛПР, выполняется совокупность процедур над проблемной областью с использованием процедурных знаний.

Приобретенные в процессе взаимодействия ПППР ОТУ с экспертом знания о его предпочтениях позволяют упорядочить сравниваемые альтернативы с помощью многокритериального сравнительного анализа и выявить, используя процедурные знания, в заданном экспертом множестве реализаций набора СрЗ подмножество наилучших по критериям предпочтения вариантов набора.

Стратегия принятия решений придает активность знаниям, она заключается в поиске путей от входных данных (задание рубежа защиты, уровня ограниченного доступа к информации) к выходным (описание рационального варианта набора средств защиты) в плановом *решателе* ПППР ОТУ.

Поиск рационального варианта набора СрЗ для каждого рубежа защиты осуществляется следующим образом:

- на основе перечня требований к набору в соответствии с необходимым классом защищенности генерируется множество решений по синтезу целостных вариантов набора СрЗ с усечением этого множества до подмножества вариантов набора из совместимых между собой программно-аппаратных продуктов;

- дальнейшее усечение подмножества осуществляется методом полного перебора по заданной целевой функции, максимизирующей отношение суммарного показателя «защищенность» варианта набора к суммарному показателю «издержки».

В качестве целевой функции для синтезируемого варианта набора $S_r=\{A_{1i}, A_{2j} \dots A_{lm}, A_{Ln}\}$ применяется функция

$$J = \max_{r} \frac{W_{K^1_{зщ}}^{A_{li}} + \dots + W_{K^1_{зщ}}^{A_{lm}} + \dots + W_{K^1_{зщ}}^{A_{Ln}}}{W_{K^1_{и}}^{A_{li}} + \dots + W_{K^1_{и}}^{A_{lm}} + \dots + W_{K^1_{и}}^{A_{Ln}}},$$

где $W_{K^1_{зщ}}^{A_{lm}}$ - значение показателя «защищенность», $W_{K^1_{и}}^{A_{lm}}$ - значение показателя «издержки» для альтернативы A_{lm}, которые находятся с использованием метода анализа иерархии.

Методика позволяет осуществить выбор наиболее рациональных наборов средств защиты для точек установки при обработке на объекте информатизации в разные периоды времени информации с разными уровнями ограничения доступа.

ППРР ОТУ представляет собой сложный программный комплекс, аккумулирующий знания эксперта в области защиты информации и специалиста по теории принятия решений.

Модель ППРР ОТУ и метод принятия решений по выбору рациональных наборов СрЗ реализованы программно и апробированы [6,7].

Выводы:

- рассмотрены прикладные аспекты формализации и приобретения автоматизированной системой знаний эксперта в области защиты информации при разработке ППРР ОТУ, сформированы необходимые для поддержки принятия решений декларативные и процедурные знания для ввода и обработки на ЭВМ;
- создано алгоритмическое и программное обеспечение для автоматизированной поддержки принятия решений в интеллектуальной СЗИ. На программные модули получены свидетельства об официальной регистрации программ для ЭВМ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Галицкий, А. В. и др.* Защита информации в сети – анализ технологий и синтез решений// А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин – М.: ДМК Пресс, 2004. – 616 с.

2. *Арефьев Ю. С., Серенков С. В.* Принципы применения механизмов и средств защиты информации при разработке автоматизированных систем на основе отечественных базовых информационных защищенных компьютерных технологий// Материалы VIII Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2006. – 244 с. С. 135 – 138.

3. *Бородакий, Ю. В., Куликов Г. В.* Интеллектуальные системы обеспечения информационной безопасности// Информационная безопасность: сб. статей VII Международной научно-практической конференции. – 2005. – С. 32.

4. *Мельников В. В.* Безопасность информации в автоматизированных системах. Альтернативный подход// Защита информации. INSIDE. – 2005. – №6. – С. 40-45.

5. *Машкина И. В., Васильев В. И., Рахимов Е. А.* Проектирование системы защиты информации объекта информатизации// Информационные технологии. – 2006. – №10. – С. 17-26.

6. Выбор целостных вариантов системы защиты информации, состоящих из совместимых между собой программно-аппаратных средств. *Машкина И. В., Рахимов Е. А., Дивель. А. В.*//Свидетельство об официальной регистрации программ для ЭВМ №2006611352 от 20.04.2006.

7. Блок расчета показателя защищенности и издержек средств защиты методом анализа иерархии / *Машкина И. В., Рахимов Е. А., Дивель. А. В.*//Свидетельство об официальной регистрации программ для ЭВМ №2006611782 от 25.05.2006.