Ученые записки Таврического национального университета им. В.И. Вернадского
Серия "Филология". Том 19 (58). 2006 г. №5. С.86-98.

УДК 070

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Стариш А.Г.

«Из анализа содержания современных угроз национальной безопасности Украины вытекает, что механизмы обеспечения национальных интересов по своей сущности носят преимущественно информационный характер... Главная информационная угроза национальной безопасности – это угроза влияния другой стороны на информационную инфраструктуру страны, информационные ресурсы, на общество, сознание и подсознание личности, с целью навязать государству желательную (для другой стороны) систему ценностей, взглядов, интересов и решений в жизненно важных сферах общественной и государственной деятельности, руководить их поведением и развитием в желательном для другой стороны направлении» [1]. Соответственно: «Государственная политика должна предусматривать согласованность решений, принимаемых органами власти и местного самоуправления для обеспечения информационной безопасности в рамках единого национального информационного пространства» [2, с. 211].

Отсюда следует, что при исследовании и разработке систем защиты информационной системы понятие *системности* заключается не только в создании соответствующих механизмов и технологий, но включает непрерывный процесс их контроля и коррекции. Контроля и коррекции, осуществляемых на всех этапах жизненного цикла информационной системы, при которых средства, методы и мероприятия, используемые для защиты, формируют целостный комплекс – систему защиты информационной системы (СЗИС).

Актуальность. Проблемой обеспечения информационной безопасности сегодня вынуждены заниматься специалисты из самых разных областей знаний. Очевидно, это обусловлено тем, что в ближайшей перспективе цивилизации придется жить в среде информационных технологий, куда, вероятно, будет перенесено решение основных социальных проблемы человечества и, как следствие, проблемы информационной безопасности. Однако даже в среде специалистов-естественников, работающих с материально-технической базой информационных технологий, необходимость *системности* в решении проблем обеспечения информационной безопасности не находит должного понимания. Тем более что:

– во-первых, под «информационной безопасностью» понимают защиту не информации, что по определению не представляется возможным, и, как следствие, сама постановка проблемы в таком формате является принципиально некорректной, но данных;

– во-вторых, практически не рассматривается вопрос защиты от информации – от произвольного информационного воздействия.

Постановка проблемы. Исходя из ноосферной парадигмы информации [3], информация – это системо- и структурообразующий феномен. В контексте данного исследования необходимо принципиально выделить тот факт, что информация по сути своей есть социальный феномен, так как «формально на человечество можно смотреть как на информационную самообучающуюся систему, состоящую из элементов-людей, между которыми существует информационное взаимодействие... на мозг отдельно

взятого человека можно смотреть как на информационную самообучающуюся систему, состоящую из элементов-нейронов, между которыми существует информационное взаимодействие... При этом элементы систем иногда гибнут, иногда рождаются, и то, и другое приводит к изменению информационных связей...» [4, с. 23]. Отсюда следует, что «человек – информационная система как форма существования информации, обусловленной способностью человека накапливать и хранить в своей памяти и обрабатывать данные, а при необходимости выдавать их другому человеку или техническому устройству» [4, с. 137].

Соответственно, на повестке дня стоит вопрос не только безопасности (защиты) данных, но в контексте тотального вхождения во все сферы бытия как отдельного человека, так и социумов, информационных технологий, вопрос защиты *от информации*. То есть вопрос об *информационной уязвимости* цивилизации.

При этом проблемность обеспечения безопасности ИС усугубляется еще и высокой неопределенностью условий функционирования информационных систем. Соответственно, постановка задачи обеспечения защиты ИС, как правило, оказывается некорректной, поскольку зачастую формулируется в условиях непредсказуемости поведения системы в нестандартных и особенно экстремальных ситуациях. Влияние неопределенности особенно сильно проявляется в радикально трансформируемых и/или нестабильных ИС из-за неполноты, несвоевременности, ненормированности и низкой достоверности исходных данных.

Следствием указанных особенностей является неоднозначность и неединственность решения, эффективность и оптимальность которого зависят от степени учета ограничений, характерных для конкретной ситуации. То есть для повышения степени корректности постановки задачи по формированию СЗИС необходимо континуально повышать знания об ИС в непрерывно изменяющихся условиях ее функционирования как внешней, так и внутренней сред. В связи с этим получение и использование знаний должны осуществляться непосредственно в процессе функционирования ИС путем накопления необходимых данных, их анализа и использования для эффективного выполнения системой заданной целевой функции.

Однако используемые математические модели для описания структуры, поведения и управления СЗИС в условиях некорректной постановки задачи не дают желаемого результата [5]. Собственно, математические методы и НЕ могут дать *абсолютный* результат, но они позволяют, пусть только и приближенно к реальному, дать оценку состоянию системы и способствовать выработке прогнозов потенциального состояния системы [6].

Соответственно, необходима разработка принципиально новых, ориентированных на специфику процессов защиты данных методов и средств контроля, моделирования и прогнозирования. То есть для получения данных о состоянии и поведении СЗИС необходимо выделить особо значимые и важные с точки зрения достижения целей функционирования системы параметры и определить времена проверки их значений. Контроль и анализ значений параметров необходимы для повышения знаний о системе, должны осуществляться таким образом, чтобы обеспечить принятие оптимальных решений и корректировку поведения ИС в процессе функционирования. Таким образом, в СЗИС обязательно должно быть предусмотрено выполнение процедур диагностирования ее состояний и контроля работоспособности.

Отметим при этом, что в некоторых ситуациях принятие решений может базироваться на методе экспертных оценках, но в условиях неопределенности исходных данных и

некорректности постановки задач управления эти оценки могут внести дополнительную некорректность в принимаемое решение, увеличив тем самым исходную неопределенность [7].

Соответственно, решение проблем анализа и/или моделирования СЗИС требует поэтапного выполнения следующих действий:

1. Разработки принципов, методов и средств сокращения размерности описания СЗИС, включающей:

– анализ структуры системы и взаимосвязей между решаемыми в ней задачами;

– анализ динамических характеристик решения задач;

– анализ корреляционных зависимостей между параметрами системы, являющимися результатами решения отдельных задач;

– выделение совокупностей задач, результат решения каждой из которых позволяет определить один из контролируемых параметров системы.

В результате разработки должны быть сформулированы требования и рекомендации по организации структуры СЗИС, декомпозированной по уровням контроля и управления. Это позволит проводить дальнейшие исследования в условиях минимизированной размерности описания системы [8].

2. Разработки методологии, методов и средств решения задач обеспечения информационной безопасности в условиях неопределенности, включающей:

– исследование вопросов корректности постановки задач при недостаточном понимании конечных результатов и целей решения в резко меняющихся условиях;

– исследование вопросов использования неопределенности исходных данных при решении задач обеспечения информационной безопасности.

3. Разработки принципов, методов и средств самоорганизации СЗИС, включающей:

– конструирование адаптивных моделей для описания структуры и поведения системы, прогнозирование значений ее параметров;

– конструирование адаптивных моделей для формирования подмножеств контролируемых параметров и диапазонов значений зон их контроля на основе заданных требований к устойчивости функционирования системы;

– конструирования адаптивных моделей контроля работоспособности и диагностирования нарушений работоспособности системы;

– самоорганизацию и саморазвитие семейств моделей для описания структуры, поведения, прогнозирования, контроля и диагностирования с учетом обеспечения необходимой устойчивости системы в условиях влияния факторов внутренней и внешней среды.

4. Разработки методов и средств поддержки принятия решений, включающей:

– разработку методов и средств выбора решений из всего множества вариантов на основании анализа состояния и поведения ИС с учетом требований управления, реального ресурса, удовлетворяющего этим требованиям, квантифицированных оценок близких и отдаленных последствий выполнения принятых решений;

– разработку методов и средств декомпозиции решений по уровням управления системы;

– разработку методов и средств поддержки принятия решений по самоорганизации системы в процессе ее функционирования для совершенствования всех видов моделей и их семейств.

Вероятно, для решения перечисленных проблем необходима целенаправленная *государственная* программа, выполняемая на единой концептуальной и методологической

основе. В результате предложенных исследований должна быть создана универсальная унифицированная модель СЗИС. Очевидно, что при существенной неопределенности условий функционирования ИС, когда необходимо установить логические связи между всеми ее элементами, для решения вопросов взаимодействия нужно перейти с механистического на логический уровень представления процессов создания и функционирования СЗИС.

Отметим при этом, что многообразие существующих и создаваемых человеком ИС рождает необходимость создания различных СЗИС, учитывающих особенности каждой из ИС. И, соответственно, возникает вопрос: возможно ли сформировать некий унифицированный подход к созданию СЗИС, при этом желательно, чтобы он был универсальным, понятным и позволял бы в одинаковой степени удовлетворить произвольные требования, предъявляемые к СЗИС. Фактически задача обеспечения информационной безопасности ИС состоит в разработке *модели представления комплекса информационной уязвимости системы*, которая бы позволяла решать задачи формирования, применения и оценки эффективности СЗИС. Модель системы защиты информационной системы представлена на рисунке 1:

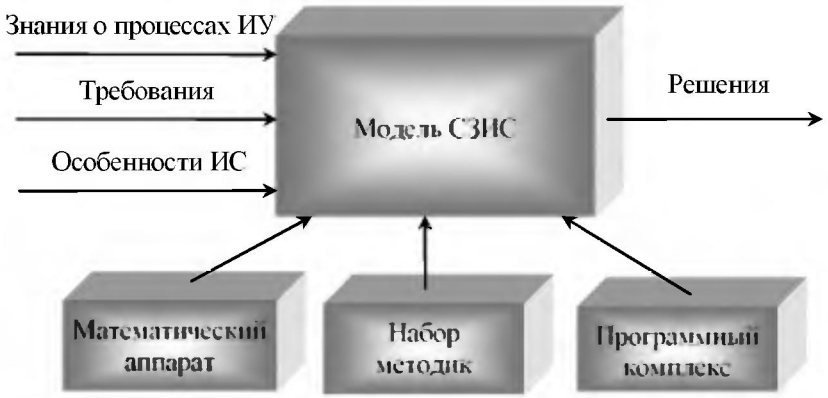

Рис.1. Модель системы защиты информационной системы

Основной задачей модели является научное обеспечение процесса создания СЗИС за счет объективной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации. Отметим при этом, что специфическими особенностями решения задачи создания СЗИС являются:

– неполнота и неопределенность исходных данных о составе ИС и характерных угрозах;

– многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей СЗИС;

– наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИС;

– невозможность применения классических методов оптимизации.

Соответственно, предлагаемая модель должна отвечать следующим требованиям:

Использоваться в качестве:

– выявления формата СЗИС;

– методики формирования показателей и требований к СЗИС;

– инструментария оценки СЗИС;
– матрицы состояния СЗИС – модели для проведения исследований.

Обладать свойствами:

– универсальности;
– простоты использования;
– наглядности;
– самообучаемости – возможностью наращивания знаний;
– функционирования в условиях неопределенности данных [9].

Позволять:

– задавать разные уровни защиты ИС;
– контролировать состояние СЗИС;
– применять различные методики оценок;
– оперативно реагировать на изменения условий функционирования.

Соответственно, встает вопрос о том, как составить такое представление о СЗИС, чтобы охватить все аспекты проблемы? Человек получает наиболее полное представление об интересующем его явлении, когда ему удается рассмотреть это нечто неизвестное со всех сторон, в трехмерном измерении (рис.2).

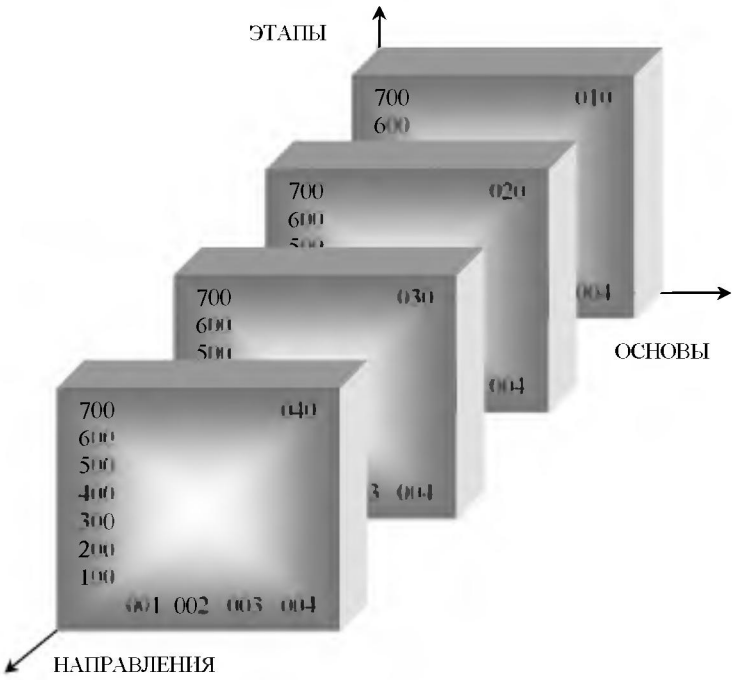

Рис.2. Координаты измерений модели СЗИС

Применим этот принцип и рассмотрим координаты измерений – триаду компонентов модели СЗИС:

1. ОСНОВЫ – элементная база СЗИС;
2. НАПРАВЛЕНИЯ – назначение СЗИС;

3. ЭТАПЫ – функционирование СЗИС.

Элементной базой или ОСНОВАМИ произвольной системы являются:

– законодательная, нормативно-правовая и научно-методическая база;

– структура и задачи органов, обеспечивающих безопасность ИС;

– политика информационной безопасности – организационно-режимные меры;

– программно-технические средства.

Отметим при этом, что с целью сохранения определенной универсальности матричного подхода под политикой информационной безопасности ИС имеет смысл понимать и ее национальный аспект. То есть к организационно-технологическим и режимным мерам и методам защиты национального информационного пространства целесообразно отнести и проблему политики воспитания в соответствующем духе населения государства. Соответственно, координату ОСНОВЫ можно представить в следующем виде (рис. 3).

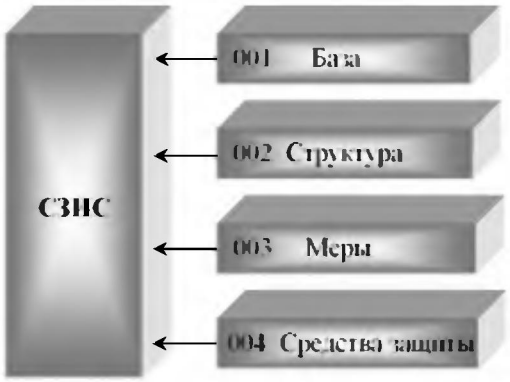

Рис.3. Координата ОСНОВЫ

Координата НАПРАВЛЕНИЯ формируется исходя из конкретных особенностей ИС как объекта защиты. В общем случае, учитывая типовую структуру ИС и исторически сложившиеся виды работ по защите ИС, целесообразно рассмотреть следующие направления:

– защита объектов информационных систем;

– защита процессов, процедур и программ обработки данных;

– защита коммуникаций;

– управление системой защиты.

Соответственно, координату НАПРАВЛЕНИЯ можно представить в следующем виде (рис. 4):

А так как каждое из НАПРАВЛЕНИЙ базируется на перечисленных выше ОСНОВАХ, то элементы ОСНОВ и НАПРАВЛЕНИЙ рассматриваются в неразрывной взаимосвязи друг с другом. Например, одну из ОСНОВ под названием «Законодательная база…» необходимо рассматривать по всем НАПРАВЛЕНИЯМ, а именно:

– законодательная база защиты объектов;

– законодательная база защиты процессов, процедур и программ;

– законодательная база защиты коммуникаций;

– законодательная база по управлению и контролю самой системы защиты.

Аналогично следует рассматривать остальные грани ОСНОВ – база, структура, меры, средства – по всем НАПРАВЛЕНИЯМ.

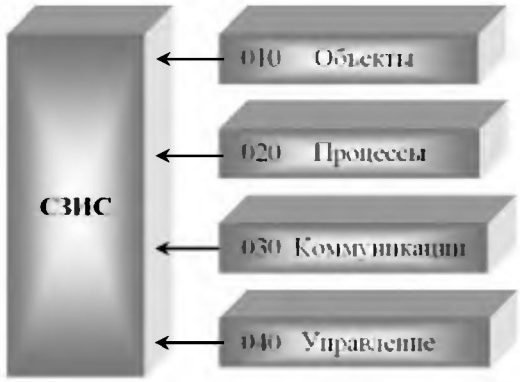

Рис.4. Координата НАПРАВЛЕНИЯ

Соответственно, для формирования наиболее общего представления о рассматриваемой СЗИС необходимо ответить минимум на 16 вопросов. Однако для более полного представления о СЗИС обязательно рассмотреть последовательность шагов – ЭТАПЫ – создания СЗИС, которые необходимо реализовать в равной степени для каждого из НАПРАВЛЕНИЙ с учетом указанных выше ОСНОВ. Соответственно, координату ЭТАПЫ можно представить в следующем виде (рис. 5), который включает:

– определение объектов и ресурсов ИС, подлежащих защите;
– выявление полного множества потенциальных угроз;
– проведение оценки уязвимости ресурсов ИС;
– определение требований к системе защиты данных;
– осуществление выбор средств защиты данных и их характеристик;
– внедрение и организация использования выбранных мер, способов и средств защиты;
– осуществление контроля целостности и управление системой защиты.

Поскольку ЭТАПОВ семь и по каждому необходимо ответить на 16 известных вопросов, то в общей сложности для формирования представления о СЗИС необходимо ответить на 112 вопросов. Очевидно, что по каждому вопросу – элементу матрицы – может возникнуть ряд уточнений. В общем случае количество элементов матрицы может быть определено из соотношения:

$$K = O_i \times H_j \times Э_k,$$

где

K – количество элементов матрицы;
O_i – количество составляющих блока ОСНОВЫ;
H_j – количество составляющих блока НАПРАВЛЕНИЯ;
$Э_k$ – количество составляющих блока ЭТАПЫ.

В рассматриваемом примере O_i = 4, H_j = 4, $Э_k$ = 7, соответственно, общее количество элементов матрицы равно 112.

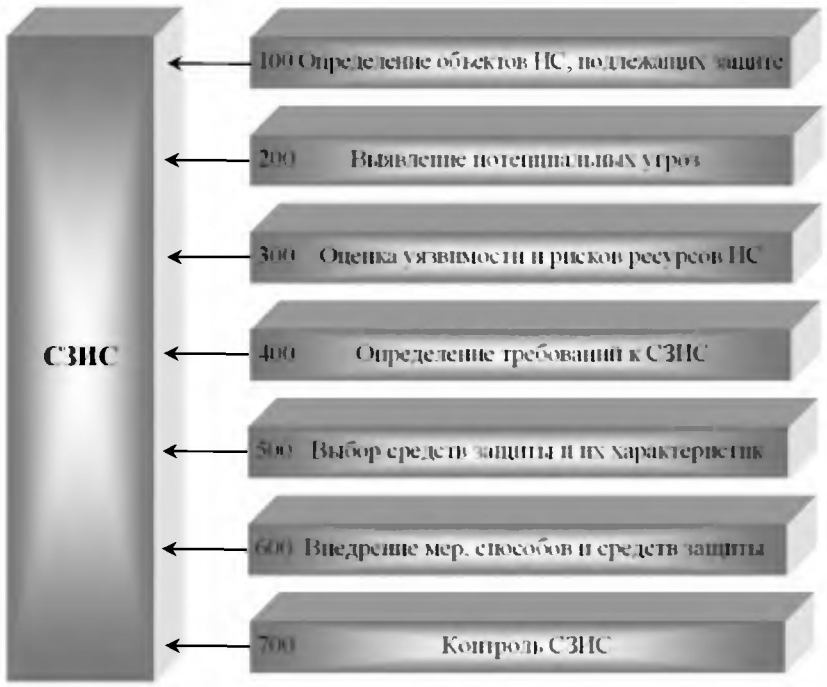

Рис.5. Координата ЭТАПЫ

Пространственный образ предложенной объемной матрицы можно представить в виде прямоугольного параллелепипеда, на гранях которого отложены, соответственно, ОСНОВЫ, НАПРАВЛЕНИЯ И ЭТАПЫ. Для наглядности понимания предложенной модели СЗИС трансформируем трехмерную фигуру в двухмерную, то есть развернем грани в плоскости и получим трехмерную матрицу в виде двухмерной таблицы.

Соответственно, матрица – это специальная таблица, позволяющая логически сопоставить между собой элементные базы блоков ОСНОВЫ, НАПРАВЛЕНИЯ и ЭТАПЫ. При этом матрица является универсальной формой, которая наполняется содержанием в каждом конкретном случае исходя из поставленных перед исследуемой или создаваемой СЗИС задач.

Каждый элемент матрицы имеет соответствующую нумерацию, где:

– первое знакоместо № X00 соответствует номерам компонентов блока ЭТАПЫ;

– второе знакоместо № 0X0 соответствует номерам составляющих блока НАПРАВЛЕНИЯ;

– третье знакоместо № 00X соответствует номерам составляющих блока ОСНОВЫ.

На рисунке 6 представлен элемент матрицы № 123, сформированный с учетом следующих составляющих:

НАПРАВЛЕНИЯ		010				020				030				040			
ОСНОВЫ		001	002	003	004	001	002	003	004	001	002	003	004	001	002	003	004
ЭТАПЫ	100																
	200																
	300																
	400																
	500																
	600																
	700																

Рис.6. Пример нумерации элемента матрицы № 123

– 100 – определение объектов ИС, подлежащих защите – составляющая № 1 блока ЭТАПЫ;

– 020 – защита процессов и программ – составляющая № 2 блока НАПРАВЛЕНИЯ;

– 003 – меры – составляющая № 3 блока ОСНОВЫ.

Приведем пример содержания данных для элементов матриц №№ 121, 122, 123, 124, которые объединяют следующие составляющие:

– № 1 (100 – определение объектов ИС, подлежащих защите) блока ЭТАПЫ;

– № 2 (020 – защита процессов и программ) блока НАПРАВЛЕНИЯ;

– № 1, 2, 3, 4, (001 – нормативная база, 002 – структура органов, 003 – мероприятия, 004 – используемые средства) блока ОСНОВЫ.

Соответственно, указанные элементы содержат данные:

– элемент № 121 – насколько полно отражены в законодательных, нормативных и методических документах вопросы, определяющие перечень сведений, использующихся в процессах и программах ИС, которые подлежат защите, и порядок определения таких сведений;

– элемент № 122 – выписаны ли функций органов, ответственных за определение сведений, подлежащих защите при использовании их в процессах и программах ИС.

– элемент № 123 – определены ли мероприятия политики безопасности, обеспечивающие своевременное и качественное определение перечня данных, подлежащих защите при использовании их в процессах и программах ИС.

– элемент № 124 – набор каких средств применяется для обеспечения оперативности и качества определения данных, подлежащей защите при использовании их в процессах и программах ИС.

Это содержание только четырех вопросов из ста двенадцати, но ответы на них позволяют сформировать определенное представление об уровне защищенности конкретной ИС.

В общем случае рассматриваются все вопросы – по числу элементов матрицы. Описание этих вопросов позволяет составить практически полное представление о СЗИС и оценить уровень защищенности существующей или моделируемой информационной системы. Именно *системы*, так как динамически-континуально учитываются взаимные логические связи между всеми элементами СЗИС. Повторимся, матрица не существует сама по себе, но формируется исходя из описания конкретной ИС и конкретных задач по защите данных в этой системе (рис. 7).

Предложенная модель представления СЗИС в виде трехмерной матрицы позволяет не только контролировать уровень защищенности информационной системы, но и определять формат и инструментарий при *моделировании* – разработке концепции и/или доктрины создания и функционирования произвольной информационной системы в части ее информационной уязвимости:

– индивида – через контроль трансформации его индивидуальной системы знаков;

– социума (середового информационного пространства) – через управление его минисемиосферой;

– цивилизации (межередового информационного пространства) – через управление семиосферой [10].

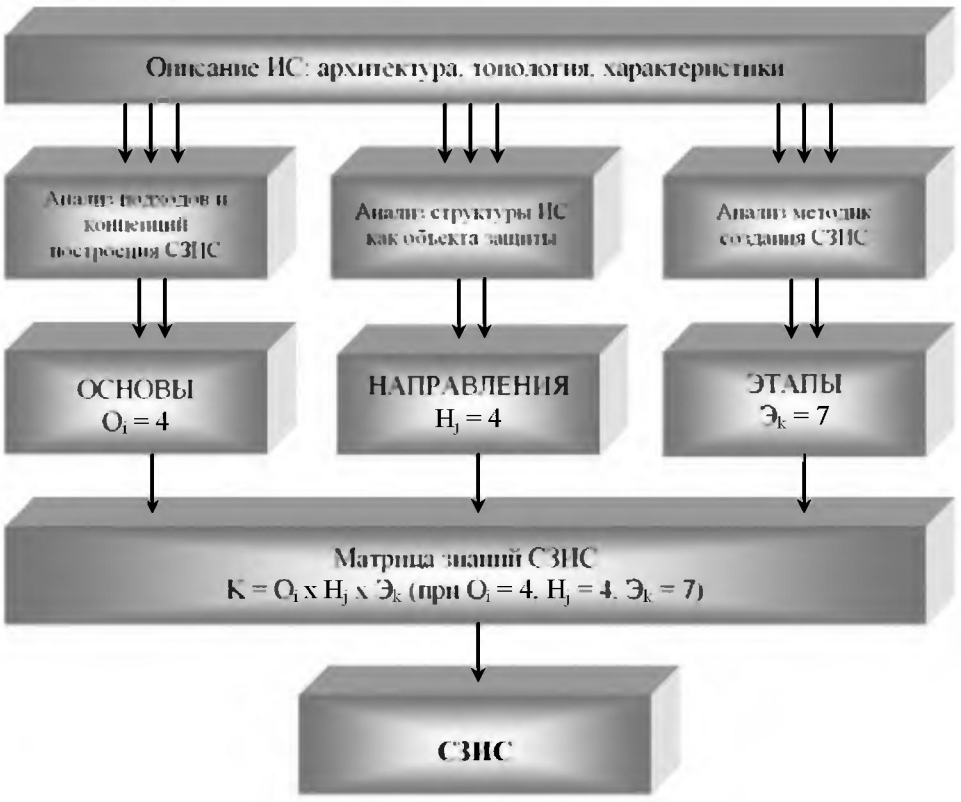

Рис.7. Формирование матрицы знаний СЗИС на основе описания ИС

Очевидно, что, заполнив все элементы матрицы соответствующими требованиями, можно сформулировать достаточно полное техническое задание на создание произвольной СЗИС, при этом сформулировать эти требования можно на основе произвольных стандартов: глобальных – международных, региональных – европейских, азиатских и т. д., национальных – американских, украинских и т.д. Таким образом, матрица знаний системы защиты информационной системы имеет следующий вид – рисунок 8.

Собственно, модель СЗИС в виде матрицы знаний создана, а описание элементов матрицы знаний СЗИС представлено в авторской монографии «Информационное измерение национальной безопасности в контексте процессов глобального развития».

Соответственно, встает вопрос об оценке эффективности СЗИС. Универсальность матричного подхода в том и состоит, что и ответ на этот вопрос можно получить на основе трехмерной матрицы, когда по всем элементам матрицы необходимо выставить соответствующие оценки (рис. 9).

НАПРАВЛЕНИЯ		Защита объектов 010				Защита процессов 020				Защита коммуникаций 030				Управление защитой 040			
ОСНОВЫ		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
ЭТАПЫ	Объект защиты 100	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144
	Источник угроз 200	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244
	Оценка рисков 300	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344
	Цели защиты 400	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444
	Средства защиты 500	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544
	Внедрение защиты 600	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644
	Контроль защиты 700	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744

Рис.8. Матрица знаний системы защиты информационной системы

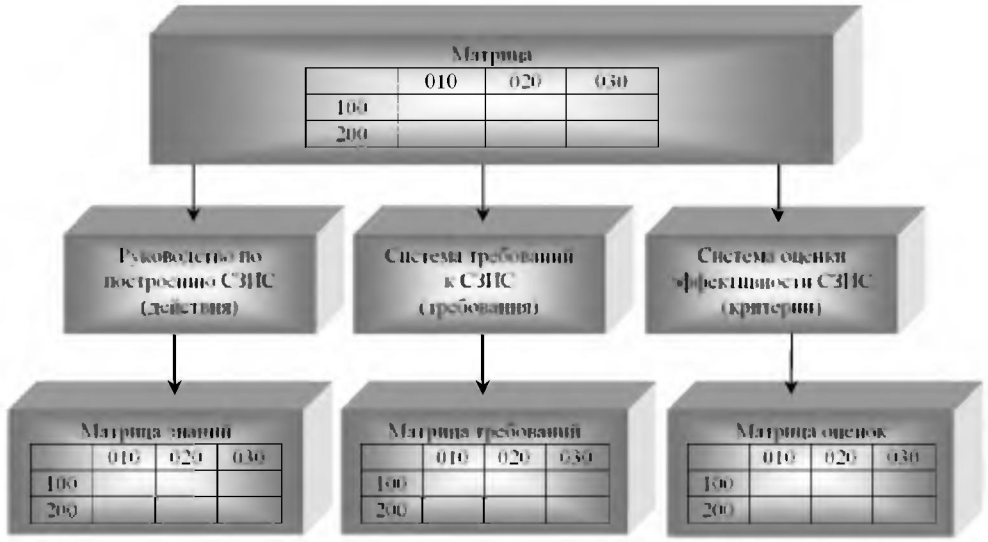

Рис.9. Свойства матрицы СЗИС

Реализация изложенного подхода на основе трехмерной матрицы в виде программ оценки эффективности СЗИС для технических систем реализована В. Домаревым [5] на основе таблиц Excel. Очевидно, с высокой степенью сохранения качества оценки эти методы можно применять и для социальных элементов и групп, рассматривая их сквозь призму ноосферной парадигмы информации как информационные системы [11].

Система управления, в формате государства – политическая система, наполнив соответствующим контентом каждую из ячеек матрицы СЗИС, по технологии обратной связи может континуально-непрерывно сканировать общественно-политическое состояние социума и по результатам сканирования вносить соответствующие коррективы в нормативно-правовую базу – правила поведения населения государства.

Соответственно, универсальность предложенного метода состоит еще и в том, что его можно применять для анализа информационной безопасности произвольных видов – как технико-технологических, так и гуманитарных систем.

При этом постоянно необходимо помнить, что инерционность системы управления влечет за собой протяженность во времени, необходимую на разработку, внедрение и реализацию новых (скорректированных) правил поведения. Соответственно, повторимся, всегда присутствует элемент запаздывания в реакции, если, конечно, их сумеет оценить система управления, на внутренние и внешние информационные воздействия.

При этом стоит отметить, что Вероятность объективной оценки общественно-политической ситуации в государстве зависит от IQ системы управления. Однако, если система управления подвержена информационному влиянию другой системы с отличающимся IQ, такая вероятность стремится к нулю. Например, эту ситуацию можно было наблюдать во время информационных войн в национальном информационном пространстве Украины во время президентских выборов 2004 и парламентских 2006 годов. Очевидно, что даже радикальная корректировка

законодательной базы, что по некоторым вопросам и происходило – в пакетных голосованиях изменяли даже Конституцию, не в состоянии стабилизировать социальную систему государства – привести в состояние устойчивого равновесия общественное сознание. То есть при применении информационных матриц для исследования состояния информационной системы необходимо постоянно учитывать фактор инерционности системы.

Выводы. Собственно, применение технологий моделирования и программирования в политологии и социологии позволяет говорить о начале в истории цивилизации нового исторического периода – периода формирования *классического* информационного оружия. Информационного оружия, теория которого едва приоткрывается за информационной вуалью нейролингвистического программирования [12]. И независимо от уровня социально-экономического развития политическая система государства, как система управления, обязана создавать и реализовывать собственные комплексные программы развития национального информационного пространства в соответствующем законодательном оформлении [13].

Список литературы

1. Домарєв В.В. Інформаційна безпека як складова частина національної безпеки України. – http://www.domarev.kiev.ua
2. Хассен С. Освобождение от психологического насилия. – М., 2001.
3. Стариш А.Г. Философия информации. – Симферополь: Таврия, 2004.
4. Расторгуев С.П. Философия информационной войны. – М., 2000.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ДиаСофт, 2004.
6. Стариш А.Г. Информационные матрицы как элементная база ноосферы // Регіональні проекції державної політики: В 2-х т., Т. 2.– Сімферополь: Таврія, 2003.
7. Горбулін В.П., Качинський А.Б. Методологічні засади розробки стратегії національної безпеки України. – http://www.niisp.gov.ua/vydanna/panorama/issue.php?s=prnb0&issue=2004_3
8. Лачинов В.М., Поляков А.О. Информодинамика или Путь к Миру открытых систем. – 2-е изд. – СПб., 1999.
9. Варивода Я. Массовое сознание как объект национальной безопасности. – http://www.geocities.com/nspilka/library/warywoda.html
10. Лотман Ю.М. Семиосфера. – СПб., 2001.
11. Стариш А.Г. Информационное измерение национальной безопасности в контексте процессов глобального развития. – Симферополь: Таврия, 2005.
12. Алдер Г. НЛП. – СПб.: Питер, 1999.
13. Горбенко І., Потей О., Прокоф'єв М. Системний аналіз переходу від концепції національної інформаційної політики до доктрини інформаційної безпеки України. – К., 2002.

Поступила в редакцию 09.08.2006 г.