УДК 004.414.2=161.1

Э.И. Митряев[1]

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассматривается проблема разработки модели представления системы (процессов) информационной безопасности, которая на основе научно-методического аппарата позволяла бы решать задачи создания, использования и оценки эффективности системы защиты информации для проектируемых и существующих уникальных информационных систем.

Для решения практических задач инженерного проектирования предлагается аналитическая модель, построенная на основе применения математического аппарата многомерных матриц. В статье излагается алгоритм построения модели информационной безопасности и дается методология проведения исследований при построении данной модели для конкретных проектируемых информационных систем.

Ключевые слова: *информационная система, защита информации, информационная безопасность, система информационной безопасности, проектирование систем и средств защиты информации, многомерные матрицы.*

E.I. Mitryaev

DEVELOPMENT OF INFORMATION SAFETY MATHEMATICAL MODEL

In this article is examined a problem of development of the presentation of system (processes) model for informative safety that on the basis of scientifically-methodical vehicle would allow to solve the tasks of creation, use and estimation of efficiency of the safety system of priv for the designed and existent unique informative systems.

For the decision of practical tasks of engineering design the analytical model built on the basis of application of mathematic multidimensional matrices vehicle is offered. In the article the algorithm of construction of model of information safety is expounded and methodology of realization of researches is given at the construction of this model for the concrete designed information systems.

Keywords: *information system, priv, information safety, system of information safety, planning of systems and facilities of priv, multidimensional matrices.*

Практическая задача обеспечения информационной безопасности (ИБ) состоит в разработке модели представления системы (процессов) ИБ, которая на основе научно-методического аппарата позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих уникальных ИС. Что понимается под моделью СЗИ? Насколько реально создать такую модель?

В 1996 г. в работе Грушо А.А. и Тимониной Е.Е. «Теоретические основы защиты информации» был высказан и обоснован тезис о том, что гарантированную защищенность в информационной системе следует понимать как гарантированное выполнение априорно заданной политики безопасности. Конструктивность такого подхода к формулированию гарантий политики безопасности закладывается и определяется проверкой наличия заданного набора свойств при проектировании ИС. Однако эти требования рассматриваются без учета связи между собой, т.е. они формальны и не структурированы. Качественное описание свойств системы (например, «идентификация и аутентификация» или «контроль целостности») не касается взаимосвязи данных механизмов и их количественных характеристик. Существующие методики оценки защищенности ИС представляют собой в первом приближении необходимые условия. Выполнение

[1] Доктор технических наук, профессор, профессор кафедры телекоммуникационных систем и информационной безопасности АНО ВО «Российский новый университет».

заданного набора качественных показателей, с одной стороны, не позволяет оценить количественно каждый показатель информационной безопасности.

Такой подход значительно осложняет разработку проектов информационных систем, отвечающих всё возрастающим требованиям к качеству их функционирования. Признанным наиболее эффективным путем решения сложных задач, не позволяющих проводить адекватное натурное моделирование, является использование математических моделей.

При проектировании систем и средств защиты информации руководствуются следующими основными принципами:

– система информационной безопасности является интегральной частью информационной системы компании и должна функционировать, не нарушая эксплуатационных параметров информационной системы;

– система информационной безопасности основывается на политике безопасности компании, в соответствии с которой четко определяются физические и логические границы системы;

– анализ рисков является основой проектирования и дальнейшего использования СЗИ.

Оценка рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации с точки зрения ИБ.

Информационная безопасность рассматривается как комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей;

Информационная безопасность выражается через показатель, отражающий статус защищенности информационной системы. Отдельные сферы деятельности (системы государственного управления, банки, информационные сети и т.п.) требуют специальных мер обеспечения информационной безопасности и предъявляют особые требования к надежности функционирования в соответствии с характером и важностью решаемых задач. Достигается это за счет реализации комплекса мероприятий и средств защиты, основанных на внутрифирменной политике безопасности в анализе рисков.

В основе методологии оценки риска лежит понятие ущерба, который получает собственник ИС при реализации конкретной угрозы. Такой же подход можно применить и при анализе информационной безопасности ИС по результатам оценки ее показателей.

Разработка формализованной модели ИБ

Предварительные замечания

Основной задачей модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Специфическими особенностями решения задачи создания систем защиты информации (СЗИ) являются:

• неполнота и неопределенность исходной информации о составе ИС и характерных угрозах;

• многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) СЗИ;

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

• невозможность применения классических методов оптимизации.

При моделировании реальный объект (или процесс) обычно представляется в идеализированной форме, упрощающей исследование.

Выбор модели – сложная задача. Ее решение осуществляется с учетом множества факторов.

Во-первых, следует четко выделить цель моделирования.

Во-вторых, должны быть установлены основные причинно-следственные связи, важные для решаемой задачи.

В-третьих, следует оценить желаемую точность результатов моделирования.

Часто приходится создавать систему защиты информации в условиях большой неопределенности.

В процессе проектирования и испытаний СЗИ рекомендуется по возможности использовать исходные данные, отличающиеся от действительных, но позволяющие при последующей загрузке системы действительными данными не проводить доработки. Загрузка действительных данных должна производиться только после проверки функционирования системы защиты информации в данной ИС.

Это замечание позволяет формировать множество параметров безопасности предварительно.

Формализация представления ИБ

Для наиболее полного представления об информационной безопасности, чтобы охватить все аспекты проблемы, формально представим процесс ИБ в трехмерном измерении.

Рассмотрим три «координаты измерений процесса ИБ» – три группы составляющих модели ИБ.

Согласно нормативным документам, информационная безопасность имеет три основные составляющие:

1) конфиденциальность – защита чувствительной информации от несанкционированного доступа;

2) целостность – защита точности и полноты информации и программного обеспечения;

3) доступность – обеспечение доступности информации и основных услуг для пользователя в нужное для него время.

При нарушении работоспособности ИС в результате реализации каких-то преднамеренных или непреднамеренных деструктивных факторов ухудшаются значения критериальных показателей ИБ для данной ИС.

Критериальные показатели ИБ технически определяются качеством работы структурно-функциональных элементов ИС. Отсюда можно предложить следующий формальный алгоритм построения области устойчивого функционирования ИС.

ИБ рассматриваем как некоторый функционал, который переводит элементы множества структурно-функциональных характеристик ИС в множество показателей оценки качества ее функционирования (критериальные показатели ИБ).

Формально определим пространство показателей качества функционирования ИС. В этом пространстве сформируются два множества элементов:

1) множество характеристик структурно-функциональных элементов ИС (ЭИС), наиболее сильно влияющих на качество функционирования ИС;

2) множество критериальных показателей интегрального функционала ИБ (ЭИБ).

Определим в этом пространстве ИБ как функциональный оператор, который переводит элементы множества ЭИС в элементы множества ЭИБ.

В дальнейшем необходимо определить формальные операторы такого отображения. Для этого надо исследовать формальную и логическую связь структурно-функциональных элементов ИС с критериальными показателями ИБ.

В пространстве, определенном на множестве элементов ИБ (ЭИБ), построим систему координат (на начальном этапе – трехмерную). По осям данной системы координат будем откладывать критериальные показатели ИБ (рис. 1).

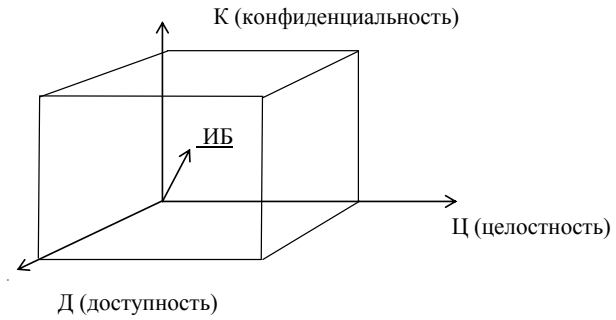

Рис. 1. Представление интегрального показателя ИБ в трехмерном координатном пространстве критериальных показателей

Каждое значение интегрального показателя ИБ в этом координатном пространстве будем представлять вектором с координатами, соответствующими значениям критериальных показателей ИБ.

Интегральный показатель ИБ формально представляется в виде трехмерной матрицы значений критериальных показателей ИБ.

В общем случае количество элементов данной матрицы может быть определено из соотношения:

$$М_{иб} = К_i \times Ц_j \times Д_k,$$

где $М_{иб}$ – количество элементов матрицы ИБ;

$К_i$ – количество составляющих блока «Конфиденциальность»;

$Ц_j$ – количество составляющих блока «Целостность»;

$Д_k$ – количество составляющих блока «Доступность».

Элементы матрицы имеют соответствующую нумерацию. Каждый из элементов матрицы обозначается следующим образом:

– первое знакоместо (Х00) соответствует номерам составляющих блока «Целостность»;

– второе знакоместо (0Х0) соответствует номерам составляющих блока «Конфиденциальность»;

– третье знакоместо (00Х) соответствует номерам составляющих блока «Доступность».

Целостность	Конфиденциальность	010		020	
	Доступность	.011	.012	021	.022
100.....	.....	...111...	...112...	...121...	...122
200.....	.....	...211...	...212...	...221...	...222
300.....	.....	...311...	...312...	...321...	...322

Рис. 2. Примерный вид матрицы интегрального показателя ИБ

Для построения данного координатного пространства необходимо исследовать взаимосвязь и корреляцию между критериальными показателями ИБ.

Цель такого исследования – показать, как по значениям двух показателей ИБ можно получить оценку третьего показателя и в целом – оценку интегрального показателя ИБ.

За основу такого исследования можно принять величину времени, которое необходимо для восстановления качества функционирования данной ИС, оцениваемое по тому или иному критериальному показателю ИБ. Тогда в клетках матрицы рис. 2 будут стоять соответствующие значения времени.

Используя математический аппарат многомерных матриц, можно интегральный показатель ИБ формально представлять в виде трехмерной матрицы значений критериальных показателей ИБ. В итоге, в координатном пространстве, построенном на критериальных показателях ИБ, можно построить область устойчивого функционирования ИС, где значение интегрального показателя ИБ отвечает требуемым значениям. Границу этой области формируют параметры, при значении которых ИС работает на грани устойчивости. За пределами этой границы ИС неработоспособна.

Предложенная модель представления интегрального показателя ИБ в виде трехмерной матрицы позволяет не только жестко отслеживать взаимные связи между элементами средств защиты информации, но может также выступать в роли руководства по созданию системы информационной безопасности.

При проектировании системы информационной безопасности для конкретной проектируемой ИС можно рассматривать различные возможные варианты реализации ИС, обеспечивая требуемые технико-экономические показатели. В этом случае проектируемую информационную систему описываем техническими параметрами, характеризующими ее работу. На множестве этих параметров строим область устойчивого функционирования ИС. На рис. 1 эта область представлена в виде пространственного куба, построенного на координатах критериальных показателей ИБ.

Формируя различные воздействия, выводящие ИС за пределы области устойчивого функционирования, можно уже на предпроектной стадии получить количественную оценку требуемых показателей качества функционирования проектируемой ИС.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

2. ГОСТ Р50922-2006 Защита информации. Основные термины и определения.

3. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости проекта.

4. Соколов Н.П. Введение в теорию многомерных матриц. – Киев : Наукова думка, 1972. – 176 с.

5. Хоффман Л. Современные методы защиты информации / пер. с англ.; под ред. В.А. Герасименко. – М. : Сов. радио, 1980. – 264 с.

6. Шелухин О.И., Тенякшев А.М., Осин А.В. Модели информационных систем. – М. : Радиотехника, 2005.