ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

DOI: 10.25586/RNU.V9187.19.04.P.082 УДК 004.414.2:161.1

Э.И. Митряев

ФОРМАЛИЗОВАННАЯ МЕТОДИКА ПОСТРОЕНИЯ МОДЕЛИ ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Рассматривается проблема построения защищенной информационной системы при условии воздействия на нее потенциально возможных деструктивных факторов техногенного и антропогенного характера. Для решения практических задач инженерного проектирования предлагается формализованная модель, построенная на основе применения математического аппарата алгебры многомерных матриц. Излагается формализованная методика построения модели защищенной информационной системы и приводится пример ее использования для решения конкретной задачи.

Ключевые слова: информационная система, защита информации, информационная безопасность, уязвимость информационной системы, модели систем защиты информации, критические условия функционирования информационной системы, многомерные матрицы.

E.I. Mitryaev

FORMALIZED METHODOLOGY FOR BUILDING A MODEL OF A SECURE INFORMATION SYSTEM

The article considers the problem of building a secure information system provided that it is affected by potentially possible destructive factors of a man-made and man-made nature. In order to solve practical problems of engineering design, a formalized model is proposed, built on the basis of application of mathematical apparatus of algebra of multidimensional matrices. The article describes the formalized method of building a model of a secure information system and provides an example of its use for solving a specific problem.

Keywords: information system, information protection, information security, information system vulnerability, models of information protection systems, critical conditions of information system operation, multidimensional matrices.

В Большой российской энциклопедии понятие «информационная система» (ИС) определяется как организационно упорядоченная совокупность программно-аппаратных и других вспомогательных средств, обеспечивающая возможность надежного долговременного хранения больших объемов информации, поиска и обработки данных в соответствии с требованиями предметной области (которая моделируется ИС), а также поддерживающая удобный интерфейс [2]. В соответствии с общей теорией системы формально ИС можно представить как совокупность информационных элементов ввода, обработки, переработки, хранения, поиска, вывода и распространения информации, находящихся в отношениях и связях между собой и составляющих определенную целостность, единство.

Цель функционирования ИС состоит в информационном обеспечении эффективной деятельности организационной системы, подсистемой которой она является. Формаль-

ную модель ИС будем строить в виде функционала, построенного на множестве ее функционально-информационных и структурных показателей.

Этот интегральный показатель является функционалом, отображающим структуру ИС и функциональные возможности элементов данной ИС как совокупности информационных элементов ввода, обработки, переработки, хранения, поиска, вывода и распространения информации, находящихся в отношениях и связях между собой и составляющих определенную целостность и единство. Обозначим его через функционально-структурный показатель ИС.

Определим понятие «живучесть» для ИС как сохранение ее работоспособности с определенным качеством функционирования при различных неблагоприятных условиях внешней среды. Качество функционирования ИС в теории принято оценивать интегральным показателем информационной безопасности (ИБ). ИС, отвечающую требованиям по обеспечению критериальных показателей ИБ, принято называть защищаемой информационной системой (ЗИС) [1].

Работоспособность ЗИС определяется как активное функционирование, идущее с изменением обработки, интеграции, передачи и воспроизведения информации адекватно целевой функции – интегральному показателю качества обработки информации по критериям ИБ для поставленной задачи функционирования ЗИС.

Временной показатель активного функционирования ЗИС по критериям ИБ прямо пропорционален знанию о ее состоянии и угрозах. Функционально активная ЗИС отвечает за обработку и передачу информации. Поэтому необходимой составляющей ЗИС является подсистема управления, обеспечивающая ее эффективное функционирование. Обработка и передача информации невозможны без целевых установок на алгоритмы управления функционированием ЗИС. Алгоритмы обработки и передачи информации функционально встроены в структуру ЗИС. При этом представление ЗИС как единой системы обеспечивается структурно-функциональным взаимодействием ее элементов.

В процессе обработки и передачи информации ЗИС ее функциональность постоянно изменяется, а следовательно, меняется и ее структура. Скорость изменения функциональности ЗИС, т.е. скорость перестроения ЗИС под изменяющиеся внешние условия, отражает возможность ее выживания. Для иерархической ЗИС информация, которая на более низком уровне структуры ЗИС противоречит целям ее функционирования (т.е. подсистема ЗИС как автономный модуль эту информацию не способна обработать, так как в ней не встроено соответствующих механизмов), на другом более высоком уровне служит для решения интеграционных задач, обеспечивая функционирование всех иерархически связанных автономных подсистем как единой ЗИС.

Этим объясняется необходимость проектирования в ЗИС новых иерархических уровней функционирования ЗИС при ее нацеливании на решение новых задач. Эволюция ЗИС показывает, что для каждого уровня ее иерархии существует свой элемент функционально-структурного показателя. Этот элемент должен быть функционально-структурным элементом базовой ЗИС. Данное требование имеет принципиальный характер для сложившейся практики проектирования систем защиты информации как автономно-независимых модулей. При таком подходе за универсальностью и экономичностью модульного проектирования теряется качество обеспечения показателей информационной безопасности для проектируемой ЗИС.

Определим условия, при которых ЗИС становится неработоспособной, т.е. переходит в состояние, когда функциональные или структурные нарушения в организации ЗИС делают ее неуправляемой. Обозначим эти состояния как критические для функционирования ЗИС (КСЗИС). КСЗИС – минимально возможная для конкретной структуры ЗИС совокупность уже утраченных функциональных элементов и связей, отсутствие которых приводит к неработоспособности какой-то подсистемы ЗИС.

Как уже отмечалось, необходимой составляющей ЗИС является система управления (СУ), обеспечивающая ее эффективное функционирование. Система управления ЗИС должна строить иерархию СУ и предоставлять каждому элементу этой СУ и целым иерархическим уровням (подсистемам) необходимые ресурсы, для того чтобы этот элемент СУ или подсистема СУ были способны решать определенную им задачу по управлению функционированием ЗИС.

Структурные (самые опасные) нарушения СУ ЗИС проистекают из того, каким образом ЗИС разделена на управляющий орган и объект управления. От варианта структуры управления ЗИС зависит ее ИБ и, следовательно, ее работоспособность и качество обработки и передачи информации.

Соответствие и адекватность ЗИС поставленным целям функционирования образуется за счет ее слаженно функционирующих функционально-структурных элементов и подсистем. Это достигается за счет многофункциональности каждой подсистемы ИС и ее функционально-структурного элемента. Чем многофункциональнее (автономно-независимее) эти функционально-структурные элементы и подсистемы, тем совершеннее ЗИС.

Придание многофункциональности функционально-структурным элементам и подсистемам ЗИС связано с усилением их «открытости» для внешних воздействий (обеспечение каждой функции определяется каналом связи с внешней средой). Высокий уровень «открытости» функционально-структурных элементов, подсистем и ЗИС в целом опасен, так как расширяются каналы связи с внешней средой и, как следствие, растет количество угроз.

Как может происходить воспроизведение и поддержание адекватности поставленным целям функционирования ЗИС в условиях внешней среды? Чтобы производить обработку и передачу информации, необходимо воспроизводить и поддерживать структуру и функциональные возможности функционально-структурных элементов и подсистем ЗИС (дополнять, перестраивать, уничтожать). Функционально-структурный показатель ЗИС выражается в ее структуре. Важно правильно технически эти функционально-структурные элементы спроектировать и технологически верно их функционально связать.

Качество функционирования ЗИС определяется ее структурой и функциональностью. Функционально ЗИС предназначена для выполнения определенных целевых функций и обеспечивается постоянным обновлением функционально-структурных элементов и программного обеспечения ЗИС. Целевые функции определяют структуру и программно-аппаратное обеспечение ЗИС. Между целевой функцией и структурой ЗИС существует взаимно однозначное соответствие, которое обеспечивается условиями функционирования ЗИС, т.е. ее взаимодействием с внешней средой.

Взаимодействие ЗИС с внешней средой обеспечивается системой защиты информации (СЗИ) для конкретной ЗИС. Именно СЗИ, адекватно моделирующая внешнюю среду, должна обеспечивать качество устойчивого функционирования ЗИС по показателям ИБ.

Таким образом, функционально ЗИС можно представить в виде двух связанных структурно и функционально подсистем, одна из которых служит для выполнения целевых задач функционирования ЗИС, а другая – для взаимодействия ЗИС с внешней средой. При этом СЗИ можно рассматривать как самостоятельную ЗИС, моделирующую функции внешней среды (модель функционирования внешней среды, в которой функционально и структурно определена ЗИС).

Для функционирования СЗИ как самостоятельной ЗИС необходимы:

1) согласованность технологии и технического обеспечения вход-выходных параметров устройств и каналов связи СЗИ и ЗИС;

2) семантическая согласованность языков программного обеспечения алгоритмов управления функционированием СЗИ и ЗИС.

ЗИС – это инструмент для управления бизнес-процессом, поэтому пользователь подходит к разработке ЗИС с позиций частных задач своего бизнес-процесса. При этом ЗИС строится как инструмент, ограниченный по функциональным возможностям и по времени устойчивого функционирования. Такой подход значительно снижает возможности активного функционирования ЗИС при изменяющихся условиях внешней среды.

Чтобы исключить ограничения по функциональным возможностям и по времени устойчивого функционирования проектируемой ЗИС, необходимо проектировать ЗИС с учетом возможности их активной работы в различных условиях внешней среды, возможно, и неблагоприятных. Для этого нужен подход к проектированию ЗИС с позиций фундаментальной науки и экспериментальной практики.

На сегодняшний день в разработке теории защиты информации, объединяющей широкий спектр проблем, связанных с обеспечением ИБ в процессе генерирования, обработки, хранения и передачи информации в автоматизированной системе, используется концептуально-эмпирический подход. Сущность и содержание данного подхода к защите информации заключается в том, что на основе опыта защиты информации, полученного на этапе эмпирического подхода, удалось некоторым образом подойти к унификации используемого для решения задач защиты методико-инструментального базиса.

В качестве основы формирования соответствующей этому этапу концепции была принята следующая схема организации защиты информации на основе эмпирического подхода:

1. Изучение среды защиты.
2. Анализ уязвимости информации.
3. Определение требований к защите.
4. Построение механизмов защиты.

В рамках данной методологии следует разделить проектирование ЗИС и СЗИ. При этом проектирование СЗИ следует вести как проектирование самостоятельного универсального модуля, работающего автономно с учетом всех возможных условий функционирования конкретных ЗИС без нарушения качества их работы.

Так как интегральным показателем качества работы ЗИС является ИБ, то все методы и модели проектирования СЗИ должны представляться интегральной системой, практически реализующей нормальные алгоритмы обеспечения показателей ИБ в форме модели СЗИ, обеспечивающей качество функционирования различных конкретных ЗИС.

Условия для создания отдельных элементов структуры СЗИ (модели):

1. Каждая структурная модель СЗИ функционально нацелена на решение определенных задач взаимодействия с внешней средой.

2. Структурные элементы СЗИ самонастраиваемы и адаптированы к процессам внешней среды, на которые они нацелены.

3. Взаимное влияние структурных элементов СЗИ в процессе ее функционирования должно быть исключено.

В структуре СЗИ должен быть интеграционный блок, обеспечивающий взаимность структурных элементов СЗИ между собой и с ЗИС. Взаимосвязь СЗИ с ЗИС обеспечивает коррекцию алгоритмов функционирования ЗИС при угрожающих воздействиях внешней среды. Взаимодействие структурных элементов СЗИ между собой определяется настройкой интеграционного блока, задаваемой внутренней программой, описывающей различные типовые репрезентативные реакции структурных элементов на внешние угрозы.

Задача проектирования – создать такую СЗИ, чтобы она могла обеспечивать защиту информации, обрабатываемой в ЗИС, используемой для решения определенного класса функциональных задач в конкретных сферах практической деятельности. Многие решения в области защиты информации часто принимаются на интуитивно-понятийном уровне без каких-либо теоретических и экономических расчетов и обоснований.

Для противостояния процессу нарушения качества функционирования ИС необходимо произвести системную классификацию процессов обеспечения защищенности ЗИС, т.е. выделить в модели внешней среды процессы, влияющие на качество функционирования ЗИС. Эти процессы следует алгоритмически описать в виде формальных моделей, из которых уже можно построить формальную модель СЗИ, адекватно отражающую процессы внешней среды, отрицательно влияющие на ЗИС.

С учетом одного из основных принципов ИБ для ЗИС стойкость защиты во всех звеньях ИС должна быть примерно одинакова. Для этого необходимо выполнение следующего требования: адекватность модели СЗИ и модели внешней среды должна быть также примерно одинакова для всех процессов, влияющих на качество функционирования ЗИС. Для построения модели СЗИ, адекватной модели внешней среды, в которой функционирует ЗИС, необходимо провести анализ:

1) процессов, обеспечивающих качество функционирования ЗИС, определяемых политикой информационной безопасности;

2) процессов, порождаемых внешней средой, которые описываются известной моделью угроз.

На основе данного анализа выбирается модель СЗИ, сравнимая со средними и оптимальными значениями показателей ИБ для репрезентативной группы моделей ЗИС, имеющих схожие функциональные цели и задачи. Построенная таким образом модель СЗИ будет эффективно встраиваться в ЗИС репрезентативной группы, обеспечивая заданные показатели качества функционирования этих ЗИС.

Функциональность ИС определяется ее структурой и архитектурой, и, следовательно, архитектура СЗИ должна быть инвариантна архитектуре ЗИС конкретной репрезентативной группы. Этого можно достичь, если для связи СЗИ с конкретной ЗИС иметь промежуточный программно-аппаратный модуль, обеспечивающий взаимосвязь СЗИ

и ЗИС. В результате создается автономная СЗИ и ряд программно-аппаратных модулей, выполняющих функции адаптеров связи этой СЗИ с конкретной ЗИС. Технологически и экономически это проще, чем для каждой ЗИС проектировать свою СЗИ.

Основная задача построения автономной СЗИ – создание ее архитектуры, специфичной для существующей технологии обработки информации, т.е. учитывающей концептуальные положения теории защиты информации и стратегии развития информационного общества, которая принята в форме государственной программы информатизации экономики.

Основной целевой задачей СЗИ является обеспечение качества решения функциональных задач ИС по показателям ИБ. Целевой функционал ЗИС выражается в структуре СЗИ и функциональных возможностях элементов этой структуры. В то же время функциональные возможности СЗИ в общем случае не сводимы к функциональным возможностям ее элементов, т.е. не являются их простой суммой.

Качество функционального представления СЗИ множеством ее структурных элементов определяется качеством обработки информации в соответствии с интегральной совокупностью критериальных показателей ИБ. Скорость процесса интеграции функциональных значений обрабатываемых структурными элементами СЗИ данных, поступающих из внешней среды, и их передачи в ЗИС является важнейшей характеристикой СЗИ, отражающей возможности устойчивого функционирования ЗИС. Свойства самой СЗИ, ее изначальная функциональность и реакция на влияние внешней среды определяют ее способность быть дополнением к ЗИС.

Для формального представления связей между структурно-функциональными элементами СЗИ хорошо подходит аппарат многомерных матриц. Использование аппарата многомерных матриц для моделирования процессов ИБ рассматривалось автором в работе [3]. Аппарат многомерных матриц позволяет формально представить все многообразие отношений между элементами структуры СЗИ. При этом каждый элемент в этой матрице активен и может быть также представлен в виде матрицы.

Литература

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // Кодекс. URL: http://docs.cntd.ru/document/gost-r-50922-2006 (дата обращения: 16.09.2019).
2. Информационная система // Большая российская энциклопедия. URL: https://bigenc.ru/technology_and_technique/text/3444940 (дата обращения: 16.09.2019).
3. *Митряев Э.И.* Разработка математической модели информационной безопасности // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ, управление». 2017. Вып. 3. С. 24–27.

Literatura

1. GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniya // Kodeks. URL: http://docs.cntd.ru/document/gost-r-50922-2006 (data obrashcheniya: 16.09.2019).
2. Informatsionnaya sistema // Bol'shaya rossijskaya entsiklopediya. URL: https://bigenc.ru/technology_and_technique/text/3444940 (data obrashcheniya: 16.09.2019).
3. *Mitryaev E.I.* Razrabotka matematicheskoj modeli informatsionnoj bezopasnosti // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz, upravlenie". 2017. Vyp. 3. S. 24–27.