Костин Н. А.

Раздел V. Методическое обеспечение инженерно-технической защиты информации

Лекция 5.1

Рекомендации по моделированию системы инженерно-технической защиты информации

Часть1

Москва, 2012

Содержание лекции:

1. **Алгоритм проектирования (совершенствования) системы защиты информации**
2. **Моделирование объектов защиты**
3. **Моделирование угроз информации**
4. **Моделирование каналов несанкционированного доступа к информации**

Литература:

Торокин А. А. Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.

Введение

Методическое обеспечение включает комплекс методик и рекомендаций, обеспечивающих при их выполнении рациональный уровень инженерно-технической защиты информации. По существу эти методики должны для конкретных условий содержать ответы в виде алгоритмов, правил, рекомендаций на следующие вопросы:

--последовательность (алгоритм) работ по обеспечению инженерно-технической защиты на требуемом уровне;

--источники защищаемой информации, их характеристики, факторы, влияющие на безопасность содержащейся в них информации;

--угрозы безопасности информации, вероятность их реализации и причиняемый ими ущерб;

--рациональные меры, обеспечивающие требуемый уровень безопасности при минимальных затратах.

Кроме того, методическое обеспечение должно содержать математический аппарат для проведения необходимых оценок показателей в процессе оптимизации защиты.

1. Алгоритм проектирования (совершенствования) системы защиты информации

Задача проектирования (разработки, совершенствования) системы защиты информации и ее элементов возникает тогда, когда создается новая организация с закрытой (секретной, конфиденциальной) информацией или существующая система не обеспечивает требуемый уровень безопасности информации.

Построение новой системы или ее модернизация предполагает:

--определение источников защищаемой информации и описание факторов, влияющих на ее безопасность;

--выявление и моделирование угроз безопасности информации;

--определение слабых мест существующей системы защиты информации;

--выбор рациональных мер предотвращения угроз;

--сравнение вариантов по частным показателям и глобальному критерию, выбор одного или нескольких рациональных вариантов;

--обоснование выбранных вариантов в докладной записке или в проекте для руководства организации; доработка вариантов.

Последовательность проектирования (модернизации) системы защиты включает три основных этапа:

-моделирование объектов защиты;

-моделирование угроз информации;

-выбор мер защиты.

Рис. 27.1. Алгоритм проектирования системы защиты информации

Основным методом исследования систем защиты является моделирование. **Моделирование предусматривает создание модели и ее исследование (анализ).**

Описание или физический аналог любого объекта, в том числе системы защиты информации и ее элементов, создаваемые для определения и исследования свойств объекта, представляют собой его модель. В модели учитываются существенные для решаемой задачи элементы, связи и свойства изучаемого объекта.

Различают **вербальные, физические и математические модели** и соответствующее моделирование.

Вербальная модель описывает объект на национальном и профессиональном языках. Человек постоянно создает вербальные модели окружающей его среды и руководствуется ими при принятии решений. Чем точнее модель отображает мир, тем эффективнее при прочих равных условиях деятельность человека. На способности разных людей к адекватному моделированию окружающего мира влияют как природные (генетические) данные, так и воспитание, обучение, в том числе на основе собственного опыта, физическое и психическое состояния человека, а также мировоззренческие модели общества, в котором живет конкретный человек.

Физическая модель представляет материальный аналог реального объекта, который можно подвергать в ходе анализа различным воздействиям и получать количественные соотношения между этими воздействиями и результатами. Часто в качестве физических моделей исследуют уменьшенные копии крупных объектов, для изучения которых отсутствует инструментарий.

Модели самолетов и автомобилей продувают в аэродинамических трубах, макеты домов для сейсмических районов испытывают на вибростендах и т. д. Но возможности физического моделирования объектов защиты и угроз ограничены, так как трудно и дорого создать физические аналоги реальных объектов.

Математическое моделирование предусматривает создание и исследование математических моделей реальных объектов и процессов. Математические модели могут разрабатываться в виде *аналитических зависимостей выходов системы от входов*, *уравнений для моделирования динамических процессов в системе*, *статистических характеристик реакций системы на воздействия случайных факторов*.

Математическое моделирование позволяет наиболее экономно и глубоко исследовать сложные объекты, чего, в принципе, нельзя добиться с помощью вербального моделирования или что чрезмерно дорого при физическом моделировании.

Возможности математического моделирования ограничиваются уровнем формализации описания объекта и степенью адекватности математических выражений реальным процессам в моделируемом объекте.

Для моделирования сложных систем все шире применяется метод математического моделирования, называемый **имитационным моделированием**. Оно предполагает определение реакций модели системы на внешние воздействия, которые генерирует ЭВМ в виде случайных чисел. Статистические характеристики (математическое ожидание, дисперсия, вид и параметры распределения) этих случайных чисел должны с приемлемой точностью соответствовать характеристикам реальных воздействий. Функционирование системы при случайных внешних воздействиях описывается в виде алгоритма действий элементов системы и их характеристик в ответ на каждое воздействие на входе. Таким образом имитируется работа сложной системы в реальных условиях. Путем статистической обработки выходных результатов при достаточно большой выборке входных воздействий получаются достоверные оценки работы системы. Например, достаточно объективная оценка эффективности системы защиты информации при многообразии действий злоумышленников, которые с точки зрения службы безопасности носят случайный характер, возможна, как правило, на основе имитационного моделирования системы защиты.

Другое перспективное направление математического моделирования, которое представляет интерес для моделирования объектов защиты и угроз информации, — **компьютерные деловые игры.**

Компьютерные деловые игры — аналог деловых игр людей, применяемый для решения проблем в организационных структурах.

Деловая игра имитирует процесс принятия решения в сложных условиях недостаточности достоверной информации людьми, играющими роль определенных должностных лиц. Участниками компьютерной игры являются два человека или компьютер и человек. Причем за сотрудника службы выступает человек, а злоумышленника — компьютер или человек. Например, злоумышленник — компьютер устанавливает в случайном месте закладное устройство, а другой игрок — человек производит поиск закладного устройства с помощью различных выбранных средств по показаниям виртуальных приборов моделей этих средств.

Моделирование объектов защиты предусматривает определение источников с защищаемой информацией и разработку моделей материальных объектов защиты.

К объектам защиты относятся источники защищаемой информации и контролируемые зоны, в которых находятся эти источники.

В результате этого этапа определяются:

--модели объектов защиты с указанием всех источников информации с описанием факторов, влияющих на их безопасность;

--цена С защищаемой информации каждого i-го источника.

На основе полученных результатов на этапе моделирования угроз выявляются угрозы безопасности информации, производится оценка ожидаемого от их реализации потенциального ущерба и ранжирование угроз по потенциальному ущербу.

При моделировании угроз определяются риск (вероятность) угрозы Ру и ущерб Су в случае ее реализации. Знание ущерба позволяет также определить количество угроз, нейтрализация которых обеспечит допустимый уровень безопасности информации Суд. Для этого достаточно произвести последовательно сложение ущерба от угроз, начиная с последней в списке, и сравнить полученную сумму с допустимым ущербом. Черта под угрозами списка при условии приблизительного равенства суммарного ущерба от не предотвращенных угроз допустимому для владельца информации значению разделит список на 2 части. Верхняя, большая часть списка угроз включает угрозы, которые необходимо нейтрализовать для обеспечения допустимого уровня безопасности информации, нижняя — малосущественные угрозы.

Последовательность ранжированных угроз определяет последовательность выбора мер защиты на 3-м этапе. Этот этап начинается с определения мер защиты по нейтрализации первой, наиболее опасной угрозы, далее — второй угрозы и т. д. Если предотвращение угрозы в конце итерации достигается несколькими мерами, то вариант выбирается по критерию «эффективность-стоимость», т. е. из нескольких вариантов, обеспечивающих приблизительно равную безопасность, выбирается вариант с меньшими затратами. В качестве эффективности варианта наиболее часто используется отношение величины уменьшения ущерба при выбранной мере защиты к затратам на реализацию этого варианта. Из вариантов выбирается тот, для которого это отношение больше.

Для каждой выбранной меры защиты рассчитываются необходимые затраты на всем ее жизненном цикле (от ее реализации до прекращения). Если обозначить затраты на нейтрализацию к-й угрозы информации i-го источника через $C_{укi}$, то процедура выбора мер защиты условно завершается при выполнении условия $\sum_{k=1}\sum_{i=1} C_{укi} \geq C_{рз}$, где $C_{рз}$ — ресурс, выделяемый на защиту информации. Условность означает, что после выполнения этого условия целесообразно продолжить выбор с целью определения и оценки затрат для мер, использование которых превышает выделенный ресурс. Эти результаты позволят определить оставшиеся угрозы и необходимые для их нейтрализации дополнительные затраты.

Выбором меры защиты, предотвращающей одну угрозу, завершается одна итерация проектирования системы защиты. После ее завершения в соответствии с указанной на рис. 1 обратной связью корректируются модели объектов защиты и угроз информации. Корректировка моделей объектов защиты заключается во внесении в них выбранных мер. Эти меры виртуально меняют защищенность информации и, соответственно, характеристики угроз ей. Кроме того, при корректировке список угроз сокращается сверху на единицу.

Итерации продолжаются до достижения допустимого уровня безопасности или при превышении выделенного на защиту информации ресурса. При выполнении указанных условий процесс построения (совершенствования) требуемой системы завершается или продолжается с целью определения дополнительного ресурса.

После рассмотрения руководством предлагаемых вариантов (лучше двух для предоставления выбора), учета предложений и замечаний, наилучший, с точки зрения лица, принимающего решения, вариант (проект, предложения) финансируется и реализуется путем проведения необходимых закупок материалов и оборудования, проведения строительно-монтажных работ, наладки средств защиты и сдачи в эксплуатацию системы защиты или ее дополнительных элементов.

2. Моделирование объектов защиты

Исходные данные для моделирования объектов защиты содержатся в перечнях сведений, содержащих семантическую и признаковую информацию и составляющих государственную или коммерческую тайну.

Для организаций, независимо от формы собственности, конкретный перечень сведений, составляющих **государственную тайну**, основывается на перечне сведений, отнесенных к государственной тайне в приложении Закона Российской Федерации «О государственной тайне» и на перечнях сведений заказывающего или выполняющего заказ ведомства.

В коммерческих структурах перечень сведений, составляющих **коммерческую тайну,** определяется руководством организации. Перечни защищаемых демаскирующих признаков продукции разрабатываются при ее создании.

Структурирование информации представляет собой многоуровневый процесс детализации и конкретизации тематических вопросов перечней сведений. Например, тематический вопрос перечня сведений «перспективные разработки» на более нижнем уровне иерархии разделяется на «направления разработок», ниже — тематика, далее разработчики, документы и т. д. Процесс структурирования продолжается до уровня иерархии, информация на котором содержится в одном конкретном источнике (должностном лице, документе, продукции т. д.). Одни и те же источники могут содержать информацию разных тематических вопросов, а информация разных источников по некоторым тематическим вопросам может пересекаться. •

№ источника информации	*Наименование источника информации*	*Вид информации источника*	*Гриф секретности (конфиденциальности) информации*	*Цена информации*	*Контролируемая зона, в которой находится источник информации*
1	2	3	4	5	6
.....					

В помещениях размещается большинство источников информации: люди, документы, разрабатываемая малогабаритная продукция и ее элементы, средства обработки и хранения информации и др., а также источники функциональных и опасных сигналов.

Крупногабаритная продукция размещается в складских помещениях или на открытых пространствах.

Источники информации в помещениях размещаются или отображаются:

-на столах помещения;

-в ящиках письменных столов помещения;

-в книжных шкафах помещения;

-в металлических шкафах помещений;

-в компьютерах;

-на экранах монитора и телевизора;

-на плакатах или экранах видеопроекторов, укрепляемых на стенах во время конференций, совещаний и других мероприятий по обсуждению вопросов с закрытой

Описание источников информации включает описание пространственного расположения источников информации и условий (факторов), влияющих на защищенность содержащейся в источниках информации (характеристик инженерных конструкций вокруг мест нахождения источников информации, радио- и электрооборудования, средств коммутации и др.).

Моделирование проводится на основе моделей контролируемых зон с указанием мест расположения источников защищаемой информации — планов помещений, этажей зданий, территории в целом.

На планах помещений указываются в масштабе места размещения ограждений, экранов, воздухопроводов, батарей и труб отопления, элементов интерьера и других конструктивных элементов, способствующих или затрудняющих распространение сигналов с защищаемой информацией, а также места размещения и зоны действия технических средств охраны и телевизионного наблюдения.

Так как подавляющее большинство источников информации размещаются в служебных помещениях, целесообразно результаты их обследования объединить в таблице, вариант которой приведен в табл. 27.2.

1	2	3		
1	Название помещения			
2	Этаж		Площадь, м^2	
3	Количество окон, наличие		Куда выходят	

1	2	3		
4	Двери, кол-во, одинарные, двойные		Куда выходят двери	
5	Соседние помещения, название, толщина стен			
6	Помещение над потолком, название, толщина перекрытий			
7	Помещение под полом, название, толщина перекрытий			
8	Вентиляционные отверстия, места размещения, размеры отверстий			
9	Батареи отопления, типы, куда выходят трубы			
10	Цепи электропитания	Напряжение, количество розеток электропитания, входящих и выходящих кабелей		
11	Телефон	Типы, места установки телефонных аппаратов, тип кабеля		
12	Радиотрансляция	Типы громкоговорителей места установки		
13	Электрические часы	Тип, куда выходит кабель электрических часов		
14	Бытовые радиосредства	Радиоприемники, телевизоры, аудио- и видеомагнитофоны, их количество и типы		
15	Бытовые электроприборы	Вентиляторы и др., места их размещения		
16	ПЭВМ	Количество, типы, состав, места размещения		

На планах этажей здания указываются выделенные (с защищаемой информацией) и соседние помещения, схемы трубопроводов водяного отопления, воздухопроводов вентиляции, кабелей электропроводки, телефонной и вычислительной сетей, радиотрансляции, заземления, зоны освещенности дежурного освещения, места размещения технических средств охраны, зоны наблюдения установленных телевизионных камер и т. д.

На плане территории организации отмечаются места нахождения здания (зданий), забора, КПП, граничащие с территорией улицы и здания, места размещения и зоны действия технических средств охраны, телевизионной системы наблюдения и наружного освещения, места вывода из организации кабелей, по которым могут передаваться сигналы с информацией.

Модель объектов защиты представляет собой набор чертежей, таблиц и комментарий к ним, содержащих следующие данные:

--полный перечень источников защищаемой информации с оценкой ее цены;

--описание характеристик, влияющих на защищенность содержащейся в них информации, мест размещения и нахождения ее источников;

--описание потенциальных источников опасных сигналов в местах нахождения источников информации.

Данные моделирования объектов защиты представляют собой лишь исходные данные для следующего этапа — моделирования угроз.

3. Моделирование угроз информации

Моделирование угроз безопасности информации предусматривает **выявление угроз и их анализ** с целью оценки возможного ущерба в случае их реализации.

Определение значений показателей угроз информации представляет достаточно сложную задачу в силу следующих обстоятельств: добывание информации нелегальными путями не афишируется и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные по видам угроз безопасности информации.

Кроме того, следует иметь в виду, что **характер и частота реализации угроз** зависят от криминогенной обстановки в районе нахождения организации и данные об угрозах, например, в странах с развитой рыночной экономикой не могут быть однозначно использованы для российских условий;

оценка угроз информации основывается на прогнозе действий органов разведки. Учитывая скрытность подготовки и проведения разведывательной операции, их прогноз приходится проводить в условиях острой информационной недостаточности;

многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняет возможность выявления и оценки угроз безопасности информации. Каналы утечки информации могут распространяться на достаточно большие расстояния и включать в качестве элементов среды распространения труднодоступные места;

априори не известен состав, места размещения и характеристики технических средств добывания информации злоумышленника.

Учитывая **существенные различия** процессов реализации угроз воздействия и утечки информации, моделирование угроз целесообразно разделить на:

-моделирование каналов несанкционированного доступа к защищаемой информации источников преднамеренных и случайных воздействий;

-моделирование технических каналов утечки информации.

4. Моделирование каналов несанкционированного доступа к информации

Из сил воздействия на носитель информации наибольшие угрозы могут создать *злоумышленники и пожар.* Они образуют каналы несанкционированного доступа к информации. Поэтому моделирование этих каналов предусматривает:

-моделирование каналов несанкционированного доступа злоумышленника к защищаемой информации;

-моделирование каналов несанкционированного доступа стихийных сил.

Источники угрозы информации можно условно разделить на 4 группы:

-сотрудники (агенты) зарубежных спецслужб;

-конкуренты на рынке и в борьбе за власть;

-криминальные элементы;

-сотрудники организации, пытающиеся добыть и продать информацию по собственной инициативе или завербованные зарубежной разведкой, конкурентом или криминалом.

В зависимости от квалификации, способов подготовки и проникновения в организацию злоумышленников разделяют на следующие типы:

-***неквалифицированный,*** который ограничивается внешним осмотром объекта, проникает в организацию через двери и окна;

-***малоквалифицированный***, изучающий систему охраны объекта и готовящий несколько вариантов проникновения, в том числе путем взлома инженерных конструкций;

-***высококвалифицированный***, который тщательно готовится к проникновению, выводит из строя технические средства охраны, применяет наиболее эффективные способы и маршруты проникновения и отхода.

Моделирование угроз информации *с учетом квалификации злоумышленника* обеспечивает экономию ресурса на защиту информации в том случае, если удается с достаточно большой достоверностью определить источник угрозы.

В противном случае во избежание грубых ошибок в условиях отсутствия информации о злоумышленнике, его квалификации и технической оснащенности *лучше переоценить угрозу, чем ее недооценить,* хотя такой подход и может привести к увеличению затрат на защиту.

Целесообразен при моделировании угроз информации следующий подход к формированию модели злоумышленника:

-злоумышленник представляет серьезного противника, тщательно готовящего операцию по добыванию информации;

-он изучает обстановку вокруг территории организации, наблю даемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;

-намечает варианты и проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи;

-имеет в распоряжении современные технические средства проникновения и преодоления механических преград.

Для создания модели угрозы физического проникновения, достаточно близкой к реальной, необходимо «перевоплотиться» в злоумышленника и смоделировать операцию проникновения за него.

Для моделирования угроз целесообразно привлекать в качестве «злоумышленников» опытных сотрудников службы безопасности, не участвующих в моделировании объектов охраны и допущенных к обобщенной информации о способах и средствах охраны организации.

Использование в качестве экспертов сотрудников других структурных подразделений недопустимо, так как это может привести к утечке ценной информации. «Злоумышленник» должен выявить на основе данных 1-го этапа организации защиты «слабые места» в существующей системе охраны и определить возможные маршруты его движения к месту нахождения источника.

Маршруты движения обозначаются на соответствующих планах модели объектов охраны. Так как моделирование основывается на случайных событиях, то целесообразно наметить несколько вариантов проникновения.

Основными элементами путей проникновения могут быть:

-естественные (ворота, двери КПП);

-вспомогательные (окна, люки, коммуникационные каналы, туннели, пожарные лестницы);

-специально создаваемые (проломы, подкопы, лазы).

Варианты проникновения могут также существенно отличаться и проводиться:

-скрытно или открыто;

-без использования или с использованием специальных приспособлений;

-без использования или с использованием силовых методов нейтрализации охраны.

Возможность реализации угрозы проникновения злоумышленника к источнику информации оценивается *произведением вероятностей двух зависимых событий*: безусловной вероятностью попытки к проникновению и условной вероятностью преодоления им всех рубежей на пути движения его от точки проникновения до места непосредственного контакта с источником информации — вероятностью проникновения.

Вероятность попытки добыть информацию, в том числе путем проникновения к источнику, зависит от соотношения цены добытой информации и затрат злоумышленника на ее добывание. Вероятность принятия злоумышленником решения на проникновение близка к нулю, если цена информации меньше или соизмерима с затратами на ее приобретение. При превышении цены над затратами эта вероятность возрастает. Так как вероятность не может превысить 1, то зависимость вероятности попытки несанкционированного доступа злоумышленника от соотношения цены информации $C_{ци}$ над затратами $C_{зз}$ можно аппроксимировать выражениями: $P_{ву} = 0$ при условии $C_{ци} / C_{зз} < 1$ и $P_{ву} = 1 - \exp(1 - \alpha_{ву} C_{ци} / C_{зз})$, если $C_{ци} / C_{зз} > 1$, где $\alpha_{ву}$ — коэффициент, учитывающий степень роста зависимости вероятности $P_{ву}$ от соотношения $C_{ци} / C_{зз}$.

Такая математическая модель достаточно хорошо согласуется с логикой принятия решения злоумышленником на осуществление операции по добывании информации. Действительно, когда $C_{ци} \leq C_{зз}$, то $P_{ву} \approx 0$, затем при увеличении этого соотношения более 1 вероятность попытки проникновения сначала медленно, а затем более существенно возрастает, а при существенном росте соотношение цены и затрат монотонно приближается к 1.

Вероятность проникновения к источнику информации при условии принятия решения злоумышленником на проведение операции (возникновения угрозы) зависит от уровня защищенности источника информации, времени реакции сил нейтрализации, квалификации злоумышленника и его технической оснащенности. В интегральном виде эта вероятность определяется вероятностями обнаружения $P_{оз}$ и необнаружения $P_{нз}$ вторжения злоумышленника системой защиты информации и соотношением времени задержки злоумышленника $\tau_{зз}$ и времени реакции системы защиты $\tau_{рс}$. Так как при $\tau_{зз} << \tau_{рс}$ вероятность проникновения близка к 1, а при противоположном соотношении времен близка к 0, то вероятность проникновения злоумышленника $P_{пз}$ в первом приближении удобно аппроксимировать экспоненциальной функцией $P_{пз} = P_{нз} + P_{оз}\exp(-\beta_{пз}\tau_{зз} / \tau_{рс})$, где $\beta_{пз}$ — коэффициент, учитывающий уровень защищенности организации.

С учетом этих моделей вероятность угрозы воздействия можно оценить по формуле:

$$P_{ув} = P_{ву} \cdot P_{пз} = [1 - \exp(-\alpha_{ву} C_{ци} / C_{зз})][P_{пз} + P_{оз} \exp(-\beta_{пз} \tau_{зз} / \tau_{рс})]$$

при $C_{ци} / C_{рр} > 1$.

Более точные результаты могут быть получены в результате **моделирования проникновения**. Для моделирования проникновения целесообразно использовать аппарат видоизмененных семантических сетей. Семантическая сеть представляет собой граф, узел которого соответствует одному из рубежей и одной из контролируемых зон организации, а ребро — вероятности и времени перехода источника угрозы из одного рубежа (зоны) в другой (другую). Для наглядности целесообразно узел — рубеж представить в виде кружка, а узел — зону — в виде прямоугольника. В свою очередь рубеж и зона могут находиться в разных состояниях.

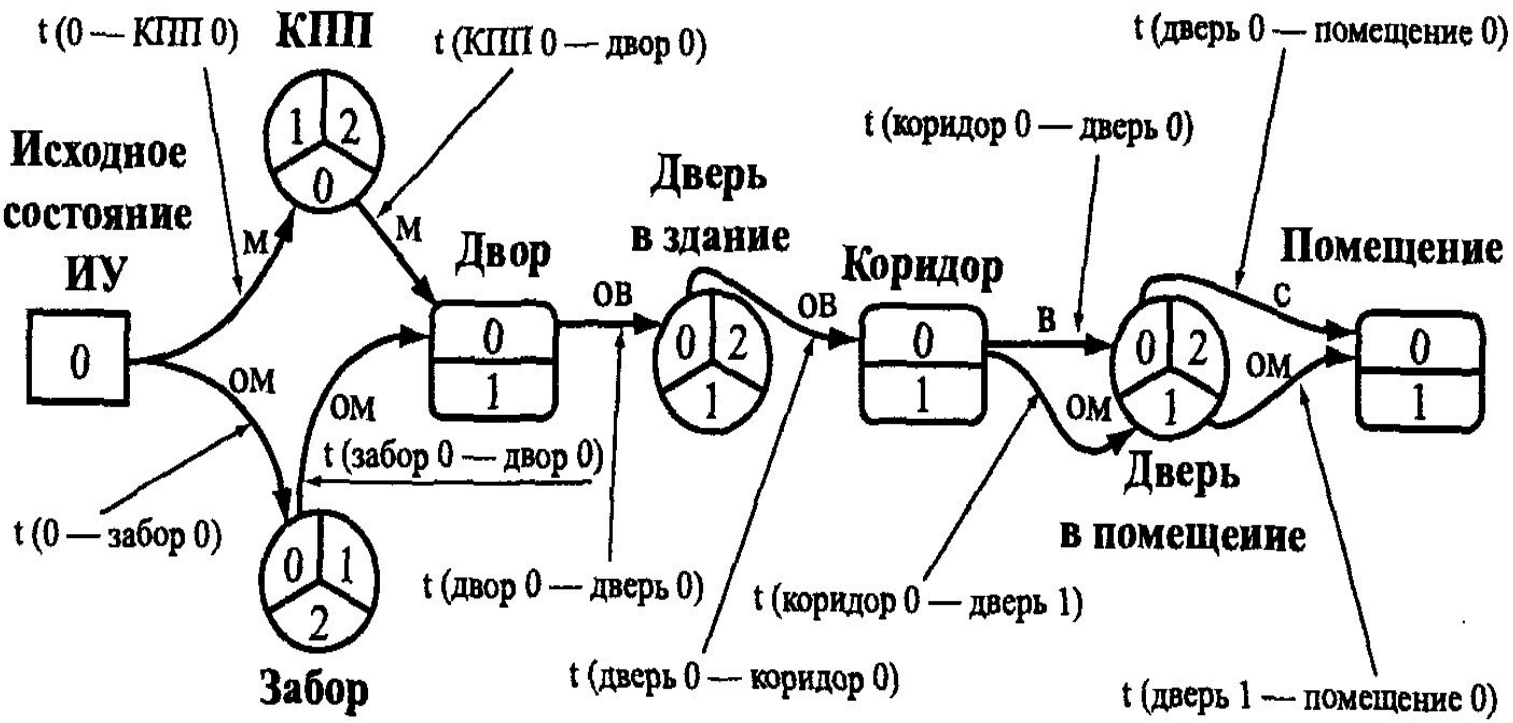

Рис. 27.2. Математическая модель проникновения злоумышленника к источнику информации

Обозначения: ИУ — источник угроз;

м — малая;

ом — очень малая;

в — высокая;

с — средняя;

ов — очень высокая вероятность;

t (КПП0 — двор 0) — время задержки при движении из КПП с 0 состоянием до двора с нулевым состоянием и т. д.

Рубеж может быть **открытым** (состояние 0), **закрытым** без включения технических сигнализации (состояние 1) и закрытым с включенными средствами сигнализации (состояние 2). Например, дверь в рабочее время может быть открытой или закрытой, во внерабочее время — закрытой с подключением охранной сигнализации.

Зона как часть пространства с контролируемым уровнем безопасности может быть **свободной** для прохода и проезда (состояние 0) и **закрытой** (с включенными средствами охраны)— состояние 1. Пример моделей каналов несанкционированного доступа источника угрозы в выделенное помещение показан на рис. 2.

Как следует из рисунка, существует множество путей перехода из нулевого состояния в конечное с разными вероятностями и временами задержками. Каждый путь характеризуется значениями вероятности и времени проникновения. Вероятность проникновения по **i**-му пути равна произведению вероятностей всех **n** промежуточных переходов по этому пути. Время задержки равно сумме задержек на каждом переходе.

Чем выше вероятность и меньше время, тем выше величина угрозы.

Учитывая, что злоумышленник будет выбирать путь с лучшими для решения своей задачи параметрами — с большей вероятностью и меньшим временем проникновения, то угрозы ранжируются по этим параметрам. Если один из путей имеет большую вероятность, но меньшее время проникновения, то при ранжировании возникнет проблема выбора. Для ее решения необходимо два показателя свести к одному. В качестве такого глобального показателя можно использовать не имеющее физического смысла отношение времени задержки и вероятности проникновения по рассматриваемому участку пути. Для такого критерия наибольшую угрозу представляет путь проникновения с меньшими значениями интегрального показателя.

Возможные пути проникновения злоумышленников отмечаются линиями на планах (схемах) территории, этажей и помещений зданий, а результаты анализа пути заносятся в таблицу, вариант которой указан в табл. 27.3.

№ источника информации	Цена информации источника	Путь источника угрозы	Характеристика угрозы		Величина ущерба	Ранг угрозы
			риск проникновения	время проникновения		
1	2	3	4	5	6	7
.....						

Примечание. Под источником угрозы понимается злоумышленник и пожар.