Ретроспективный анализ подходов к формированию множества угроз информации

Вопрос об угрозах информации возник практически одновременно с началом регулярного сбора, обработки и использования информации. Известно, что шифрование информации в целях сохранения ее тайны применял еще древнеримский диктатор Цезарь. За столетия развития традиционных (бумажных) технологий выработана весьма стройная и высокоэффективная система выявления и нейтрализации угроз.

Особую актуальность и новое содержание проблемы формирования множества угроз приобрела в 60-е - 70-е годы нашего столетия в связи с регулярным использованием для обработки и хранения информации средств электронно-вычислительной техники. При этом раньше других интерес был проявлен к угрозам физической целостности информации, поскольку другие виды угроз были менее актуальны. (Например, угроза несанкционированного получения информации в значительной мере нейтрализовывалась ограничениями на автоматизированную обработку секретных данных). Но по мере расширения сфер и масштабов использования вычислительной техники проблемы предупреждения несанкционированного получения закрытой информации приобретали все большую остроту, в связи с чем росла и актуальность задачи выявления соответствующих угроз.

При обработке информации средствами электронно-вычислительной техники (ЭВТ) возникает большое количество угроз как прямого несанкционированного доступа к защищаемой информации, так и косвенного ее получения средствами технической разведки.

Известно пять групп основных угроз: хищение носителей, запоминание или копирование информации, несанкционированное подключение к аппаратуре, несанкционированный доступ к ресурсам ЭВТ, перехват побочных излучений и наводок.

В некоторых источниках предпринята попытка классификации угроз, причем в качестве критерия классификации принят тип средств, с помощью которого может быть осуществлено несанкционированное получение

информации. Выделено три типа средств: человек, аппаратура и программа. В группе угроз, в реализации которых основную роль играет человек, названы: хищение носителей, чтение информации с экрана, чтение информации с распечаток; в группе, где основным средством выступает аппаратура подключение к устройствам и перехват излучений; в группе, где основное средство программа — несанкционированный программный доступ, программное дешифрование зашифрованных данных, программное копирование информации с носителей.

Также, угрозы могут быть классифицированы по возможному их источнику; причем выделено три класса: природные (стихийные бедствия, магнитные бури, радиоактивное излучение и наводки); технические (отключение или колебания электропитания, отказы и сбои аппаратно-программных средств, электромагнитные излучения и наводки, утечки через каналы связи); созданные людьми, причем различаются непреднамеренные и преднамеренные действия различных категорий лиц.

В руководящем документе Гостехкомиссии России (сейчас ФСТЭК) введено понятие модели нарушителя в автоматизированной системе (АС), причем в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами, причем выделяются четыре уровня этих возможностей:

1. *первый* — возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;
2. *второй* — дополнительно к предыдущему предусматривает возможности создания и запуска собственных программ с новыми функциями обработки информации;
3. *третий* — дополнительно к предыдущему предполагает возможности управления функционированием АС, т.е. воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования);

4. *четвертый* — определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав средств системы собственных технических средств с новыми функциями обработки информации.

Предполагается, что нарушитель на своем уровне является специалистом высшей квалификации, знает все об АС, в том числе и о средствах защиты.

Своеобразный вид угроз представляют специальные программы, скрытно и преднамеренно внедряемые в различные функциональные программные системы и которые после одного или нескольких запусков разрушают хранящуюся в них информацию и/или совершают другие недозволенные действия. К настоящему времени известно несколько разновидностей таких программ: *электронные вирусы, компьютерные черви, троянские кони*.

Электронные вирусы — это такие вредоносные программы, которые не только осуществляют несанкционированные действия, но обладают способностью к саморазмножению, в силу чего представляют особую опасность дня электронно-вычислительных сетей. Однако, для размножения им необходим носитель (файл, диск), что, естественно, создает для злоумышленников определенные трудности в осуществлении их несанкционированных действий.

Троянскими конями названы такие вредоносные программы, которые злоумышленно вводятся в состав программного обеспечения и в процессе обработки информации осуществляют несанкционированные процедуры, чаще всего - процедуры незаконного захвата защищаемой информации, например, записывая ее в определенные места ЗУ или выдавая злоумышленникам.

К *компьютерным червям* отнесены вредоносные программы, подобные по своему воздействию электронным вирусам, но не требующие для своего размножения специального носителя. Они обычно используют дополнительный вход в операционную систему, который создается для удобства ее отладки и который нередко забывают убрать по окончанию отладки.

Раньше других появились и использовались в злоумышленных целях троянские кони, сведения о них относятся еще к семидесятым годам, причем наиболее распространенной несанкционированной процедурой было считывание информации с областей ЗУ, выделяемых законным пользователям. Первое сообщение о возможности создания электронных вирусов было сделано в 1984 г. на одной из конференций по безопасности информации, а уже в 1985 г. была осуществлена вирусная атака на компьютерную систему подсчета голосов в конгрессе США, вследствие чего она вышла из строя. В 1987 г. зафиксированы факты появления вирусов в нашей стране.

О возможных последствиях таких угроз мощно судить по следующему примеру. Адъюнкт Корнельского университета США 25-летний Роберт Моррис (кстати, сын сотрудника Агентства национальной безопасности США) 2 ноября 1988 г. произвел вирусную атаку на национальную сеть Milnet/Arpanet и международную компьютерную сеть Internet, в результате чего было выведено из строя около 6000 компьютеров. Вирус был введен в один из узлов сети, затем он разослал свои копии (длина 99 строк на языке Си), в другие узлы. В узле-получателе копия копировалась и выполнялась. В процессе выполнения с узла-источника копировалось остальное тело вируса. Общий размер вируса составил около 60 Кбайт. Хотя вирус не производил действий по разрушению или модификации информации, а способы ликвидации его были найдены уже на второй день, ущерб от его действия оценивался более чем в 150 тысяч долларов. Исследовательскому же центру НАСА в г. Маунтинн Вью (Калифорния) пришлось на два дня закрыть свою сеть для восстановления нормального обслуживания 52000 пользователей.

Уже такого беглого взгляда на вредоносные программы достаточно, чтобы убедиться в большой опасности их как угроз информации в современных средствах ЭВТ.

2.4. Цели и задачи оценки угроз информации в современных системах ее обработки

Оценка угроз заключается в определении значений тех показателей, которые необходимы для решения всех задач, связанных с построением и эксплуатацией механизмов защиты информации. Тогда общую задачу оценки угроз можно представить совокупностью следующих составных частей:

1. обоснование структуры и содержания системы показателей, необходимых для исследований и практического решения всех задач, связанных с защитой информации;

2. обоснование структуры и содержания тех параметров, которые оказывают существенное влияние на значения показателей уязвимости информации;

3. разработка комплексов моделей, отображающих функциональные зависимости показателей от параметров и позволяющих определять значения всех необходимых показателей уязвимости информации во всех представляющих интерес состояниях и условиях жизнедеятельности СОД;

4. разработка методологии использования моделей определения значений показателей уязвимости при исследованиях и практическом решении различных вопросов защиты, или иначе — разработка методологии оценки уязвимости информации.

В следующих параграфах данной главы излагаются методы подхода к решению перечисленных составных задач.

2.5. Система показателей уязвимости информации

Для системной оценки уязвимости информации в системе обработки данных (СОД) необходима система показателей, которая отражала бы все требования к защите информации, а также структуру СОД, технологию и условия автоматизированной обработки информации.

Уязвимость информации необходимо оценивать в процессах: разработки и внедрения СОД, функционирования СОД на технологических участках

автоматизированной обработки информации, функционирования СОД независимо от процессов обработки информации. Уязвимость информации в процессе разработки и внедрения СОД обуславливается уязвимостью создаваемых компонентов системы и создаваемых баз данных.

Особое значение на данной стадии имеет минимизация уязвимости программного обеспечения, поскольку от этого существенно зависит общая уязвимость информации в СОД.

Условия автоматизированной обработки информации характеризуются главным образом совокупностью следующих параметров:

– структурой СОД, чем определяется состав, подлежащих защите объектов и элементов; наличием и количеством угроз, потенциально возможных в структурных компонентах СОД;

– количеством и категориями лиц, которые могут быть потенциальными нарушителями статуса защищаемой информации; режимами автоматизированной обработки информации.

Уязвимость информации в процессе функционирования СОД независимо от процесса обработки информации обуславливается тем, что современные СОД представляют собою организационную структуру с высокой концентрацией информации, которая может быть объектом случайных или злоумышленных воздействий даже в том случае, если автоматизированная обработка ее не осуществляется.

Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры уязвимости информации наиболее целесообразно принять вероятность нарушения защищаемых характеристик ее при тех условиях сбора, обработки и хранения, которые имеют место в СОД, а также потенциально возможные размеры (математическое ожидание) нарушения защищенности информации.

Основными параметрами, определяющими вероятность нарушения защищенности информации, являются:

– количество и типы тех структурных компонентов СОД, в которых оценивается уязвимость информации;

– количество и типы случайных угроз, которые потенциально могут проявиться и оказать негативное воздействие на защищаемую информацию;

– количество и типы злоумышленных угроз, которые могут иметь место и оказать воздействие на информацию;

– число и категории лиц, которые потенциально могут быть нарушителями правил обработки защищаемой информации; виды защищаемой информации.

Множество разновидностей различных показателей уязвимости определяется декартовым произведением чисел, характеризующих количество значений всех значащих параметров. Если не разделять угрозы на случайные и злоумышленные (т.е. рассматривать их единым множеством) и не разделять защищаемую информацию на виды, то структура полного множества разновидностей показателей уязвимости может быть наглядно представлена так, как показано на рис. 2.4, из которого следует, что два показателя занимают особое положение, а именно: первый находится в самом начале выбранной системы координат, второй — в самом конце классификационной структуры, т.е. занимает крайнее положение справа, вверху и спереди.

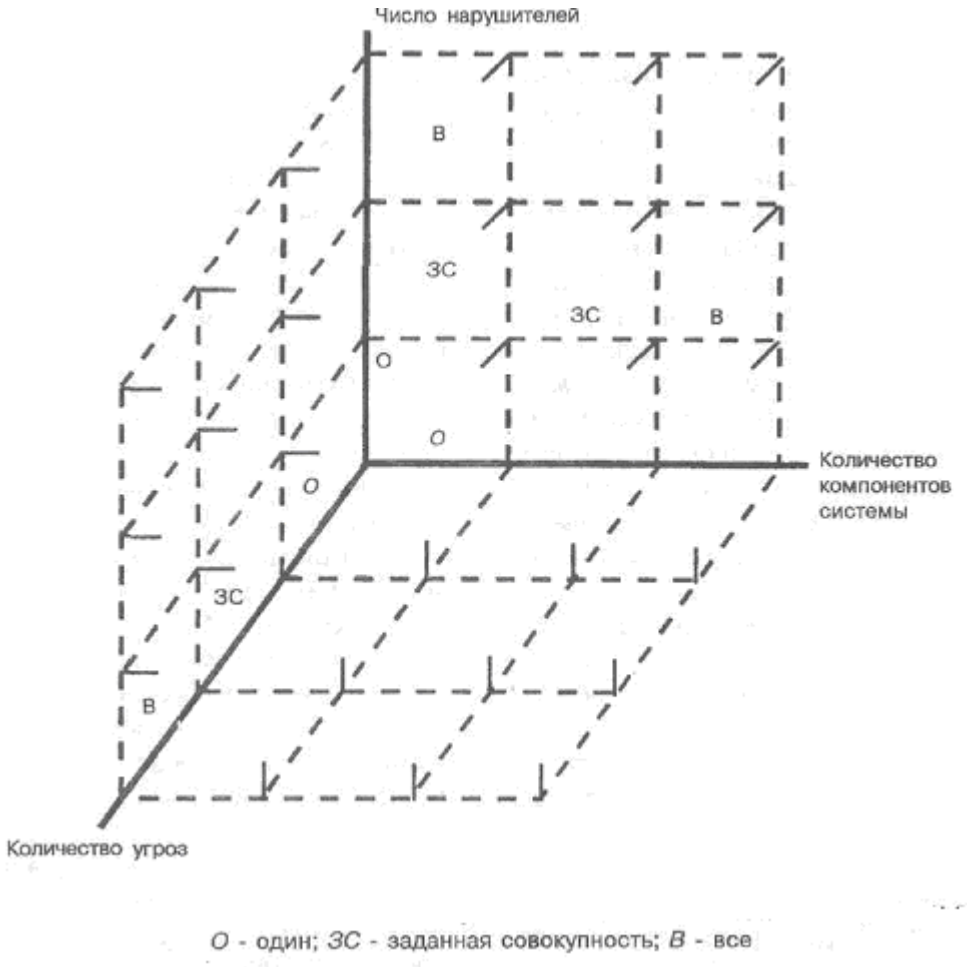

Рис. 2.4. Структура множества показателей уязвимости информации в СОД.

Первый показатель обозначает уязвимость информации в одном структурном компоненте СОД при однократном проявлении одной угрозы и относительно одного потенциального нарушителя. Все другие показатели приведенного на рисунке множества могут быть выражены в виде некоторой функции этого показателя. Второй выделенный выше показатель характеризует общую уязвимость, т.е. уязвимость информации в СОД в целом по всем потенциально возможным угрозам относительно всех потенциально возможных нарушителей. Первый показатель назовем *базовым*, второй — *общим*. Тогда другие показатели приведенного на рис. 2.4. множества можно назвать частично обобщенными.

Однако для исследования и практического решения задач зашиты информации наряду с рассмотренными выше необходимы еще такие показатели, которые характеризуют *наиболее неблагоприятные ситуации* с точки зрения уязвимости информации. Такими являются: самый уязвимый

структурный компонент АСОД, самая опасная угроза, самый опасный нарушитель. Эти показатели могут быть названы *экстремальными*.

2.6. Классификация и содержание угроз информации

Одной из наиболее принципиальных особенностей проблемы защиты информации является абсолютный характер для обеспечения возможностей реализации упреждающей стратегии зашить требования полноты всех угроз информации, потенциально возможных в современных СОД. Даже одна неучтенная (невыявленная или непринятая все внимание) угроза может в значительной мере снизить эффективность защиты. В то же время проблема формирования полного множеств угроз относится к числу ярко выраженных неформализованных проблем. Обусловлено это тем, что архитектура современны средств автоматизированной обработки информации, организационное структурное функциональное построение информационно-вычислительных систем и сетей, технология и условия автоматизированной обработки информации такие, что накапливаемая, хранимая и обрабатываемая информация подвержена случайным влияниям чрезвычайно большого числа факторов многие из которых должны быть квалифицированы как дестабилизирующие. Убедительным доказательством справедливости утверждения о неформализуемости задачи формирования полного множества угроз может служить тот факт, что в имеющихся достаточно многочисленных публикациях по проблемам защиты информации обсуждаемая задача практически даже не поставлена.

Таким образом, возникает ситуация, когда, с одной стороны, требование необходимости решения задачи является абсолютным, а с другой, регулярные методы решения этой задачи отсутствуют. Рассмотрим возможные подходы разрешения данного противоречия.

Одним из наиболее адекватных и эффективных методов формирования и особенно проверки множества потенциально возможных угроз является *метод натурных экспериментов*. Суть его заключается в том, что на существующих

СОД проводятся специальные эксперименты, в процессе которых выявляются и фиксируются проявления различных дестабилизирующих факторов. При надлежащей организации экспериментов и достаточной их продолжительности можно набрать статистические данные, достаточные для обоснованного решения рассматриваемой задачи. Однако постановка таких экспериментов будет чрезвычайно дорогостоящей и сопряжена с большими затратами сил и времени. Поэтому данный метод целесообразен не для первоначального формирования множества угроз, а для его уточнения и дополнения, осуществляемого попутно с целевым функционированием СОД.

Для первоначального формирования возможно более полного множества угроз наиболее целесообразно использовать экспертные оценки в различных их модификациях. Однако при этом не может быть гарантировано формирование строго полного их множества. Поэтому будем называть формируемое таким образом множество относительно полным, подчеркивая этим самым его полноту относительно возможностей экспертных методов.

В соответствии с рассмотренной там методикой проводились работы по формированию относительно полных множеств угроз различного вида.

Для примера рассмотрим далее структуру и содержание относительно полного множества *каналов несанкционированного получения информации КНПИ)*. Под *КНПИ* понимаются такие угрозы, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами или процессами, не имеющими на это законных полномочий.

Прежде всего было установлено, что с целью формирования возможно более полного множества КНПИ необходимо построить строго полную классификационную их структуру. Такая структура может быть построена, если в качестве критериев классификации выбрать следующие два показателя:

1. отношение к состоянию защищаемой информации в СОД;
2. степень взаимодействия злоумышленника с элементами СОД.

По первому критерию будем различать два состояния: безотносительно к обработке (несанкционированное получение информации может иметь место

даже в том случае, если она не обрабатывается, а просто хранится в СОД) и в процессе непосредственной обработки средствами СОД.

Полная структуризация второго критерия может быть осуществлена выделением следующих его значений:

1. без доступа к элементам СОД (т.е. косвенное получение информации);

2. с доступом к элементам СОД, но без изменения их состояния или содержания;

3. с доступом к элементам СОД и с изменением их содержания или состояния. Классификационная структура КНПИ представлена на рис.2.5.

Полнота представленной классификационной структуры гарантируется тем, что выбранные критерии классификации охватывают все потенциально возможные варианты взаимодействия злоумышленника с АСОД, а структуризация значений критериев осуществлялась по методу деления целого на части.

Таким образом, все множество потенциально возможных КНПИ может быть строго разделено на шесть классов; содержание и обозначение выделенных классов приведены на рис. 2.5.

Следующим шагом на пути решения рассматриваемой задачи является обоснование возможно более полного перечня КНПИ в пределах каждого из шести классов. Эта работа выполнялась преимущественно эвристическими методами, в силу чего полнота полученных перечней не может быть гарантирована. Поэтому сформированное множество КНПИ является полным лишь относительно, т.е. лишь относительно имеющей степени познания природы появления каналов.

Рис. 2.5. Классификационная структура каналов несанкционированного получения информации

2.7. Методы и модели оценки уязвимости информации

Уязвимость информации, т.е. нарушение установленного статуса и требуемого уровня ее защищенности есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в СОД средства защиты не в состоянии оказать достаточного противодействия проявлению угроз нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в СОД в самом общем виде представлена на рис. 2.6.

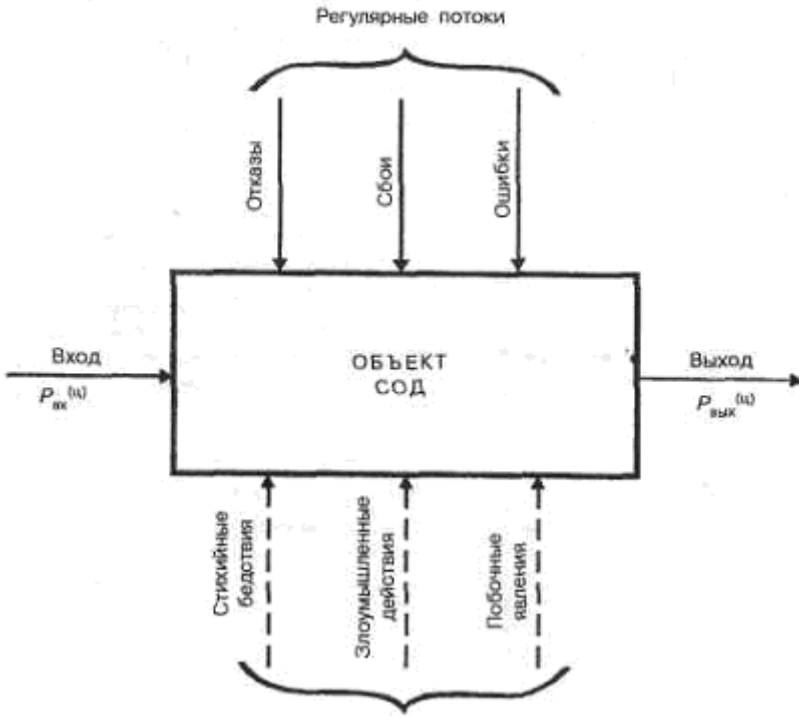

Рис. 2.6. Общая модель процесса уязвимости информации

Приведенная модель детализируется при изучении конкретных видов уязвимости информации: нарушения целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на то обстоятельство, что *подавляющее большинство нарушений целостности информации осуществляется в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации в каждом объекте СОД существенно зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход*.

Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов СОД), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений СОД и их оборудования. Что касается злоумышленных действий, то они

связаны главным образом с несанкционированным доступом к ресурсам СОД. При этом наибольшую опасность представляет занесение вирусов.

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных СОД несанкционированное получение информации возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов само по себе не ведет к несанкционированному получение информации, оно лишь способствует появлению; КНПИ, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в современных СОД для самого общего случая представлена на рис. 2.7.

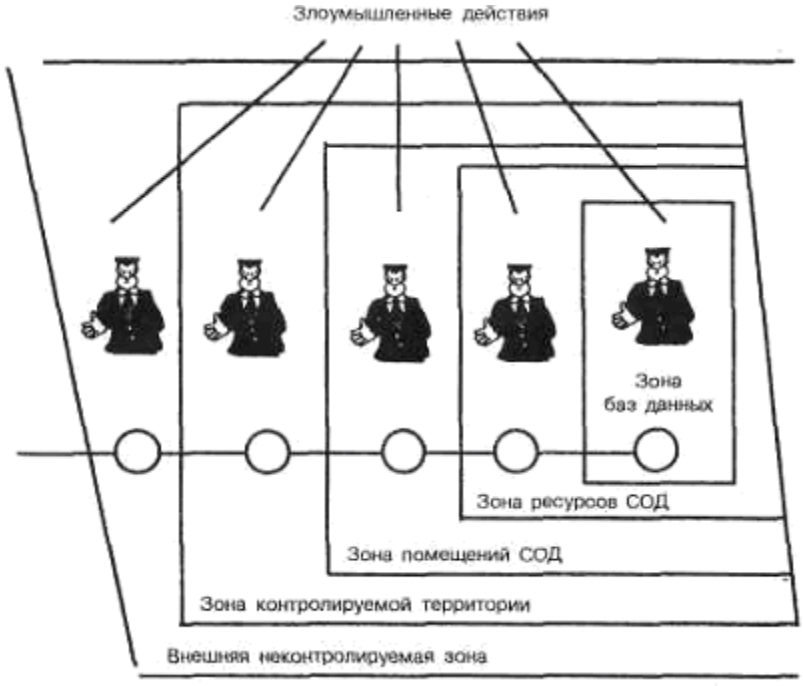

Рис. 2.7. Структурная схема потенциально возможных злоумышленных действий в СОД

Выделенные на рисунке зоны характеризуются следующим образом:

– *внешняя неконтролируемая зона* — территория вокруг СОД, на которой персоналом и средствами СОД не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;

– *зона контролируемой территории* — территория вокруг помещений СОД, которая .непрерывно контролируется персоналом или средствами СОД;

– *зона помещений СОД* — внутреннее пространство тех помещений, в которых расположены средства системы:

– *зона ресурсов СОД* — та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;

– *зона баз данных* — та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий:

– нарушитель должен получить доступ в соответствующую зону;

– во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий КНПИ;

– соответствующий КНПИ должен быть доступен нарушителю соответствующей категории;

– в КНПИ в момент доступа к нему нарушителя должна находиться защищаемая информация.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного копирования информации. Принципиальными особенностями этого процесса являются следующие:

1. любое несанкционированное копирование есть злоумышленное действие;

2. несанкционированное копирование может осуществляться в организациях-разработчиках компонентов СОД, непосредственно в СОД и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного копирования информации у разработчика и в СОД есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной выше (см. рис. 2.7.) моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок. Тогда модель процесса размножения в самом общем виде может быть представлена так, как показано на рис. 2.8.

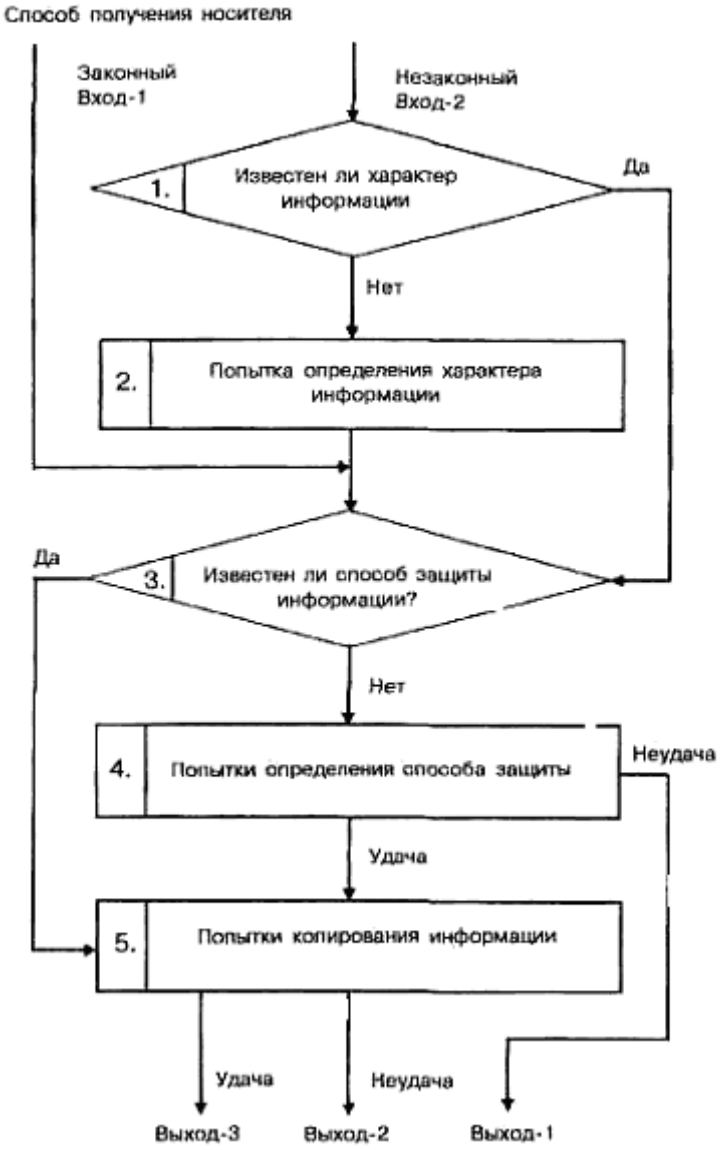

Рис. 2.8. Общая модель процесса несанкционированного копирования информации

Для определения значений показателей уязвимости информации должны быть разработаны методы, соответствующие природе этих показателей и учитывающие все факторы, влияющие на их значение. На основе этих методов должны быть разработаны модели, позволяющие рассчитывать значения любой совокупности необходимых показателей и при любых вариантах архитектурного построения СОД, технологии и условий ее функционирования.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: *эмпирический, теоретический* и *теоретико-эмпирический.*

Сущность *эмпирического подхода* заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба. Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы IBM.

Теоретический подход основывается на знании законов распределения всех случайных величин, характеризующих процессы защиты, и построении на этой основе строгих зависимостей.

Теоретико-эмпирический подход основывается на житейски-естественном представлении процессов негативного воздействия на информацию и выражении этих процессов с использованием основных положений теории вероятностей.