Глава III. Методы и средства обеспечения безопасности информации

3.1 Общая классификация методов и средств обеспечения информационной безопасности АИС

Развитие компьютерных угроз привело к появлению и развитию отрасли знаний, объектом исследований которой является информационная безопасность во всех ее аспектах - организационных, технических, правовых, экономических, философских, социальных и т.д.

Модель системы информационной безопасности в общем виде может быть представлена следующим образом. С объектом, являющимся составной частью АИС, связано множество действий, в том числе и несанкционированных. Между объектом (***O***) и угрозой (***T***) существует множество отношений, которые образуют граф, в котором дуга $<t_n,o_n>$ существует тогда и только тогда, когда t_n является средством доступа к объекту o_n (*рис. 14.а*).

Следует отметить, что связь между t_n и o_n характеризуется типом “один ко многим”, т.е. одна угроза покрывает множество объектов, в свою очередь, один объект уязвим от более чем одной угрозы. Наличие дуги типа $<t_n,o_n>$ характеризует незащищенный объект АИС.

Целью СИБ является создание барьера, который предохраняет объекты от возможных угроз. Для этого вводится множество M, включающее средства обеспечения безопасности АИС. Любое $m_m \in M$ должно устранить дугу $<t_n,o_n>$ в общем графе и обеспечить противостояние попыткам несанкционированного доступа. Возможность противостояния (сопротивления) СИБ является основной характеристикой элементов $m_m \in M$. Данное множество преобразует первоначальную дугу $<t_n,o_n>$ в форму:

$<t_n, m_m>$ и $<m_m, o_n>$ (3.1)

Модификацией данной модели является:

$S=<O,T,M,V,B>$, (3.2)

где O - множество защищенных объектов ($o_n \in O$);

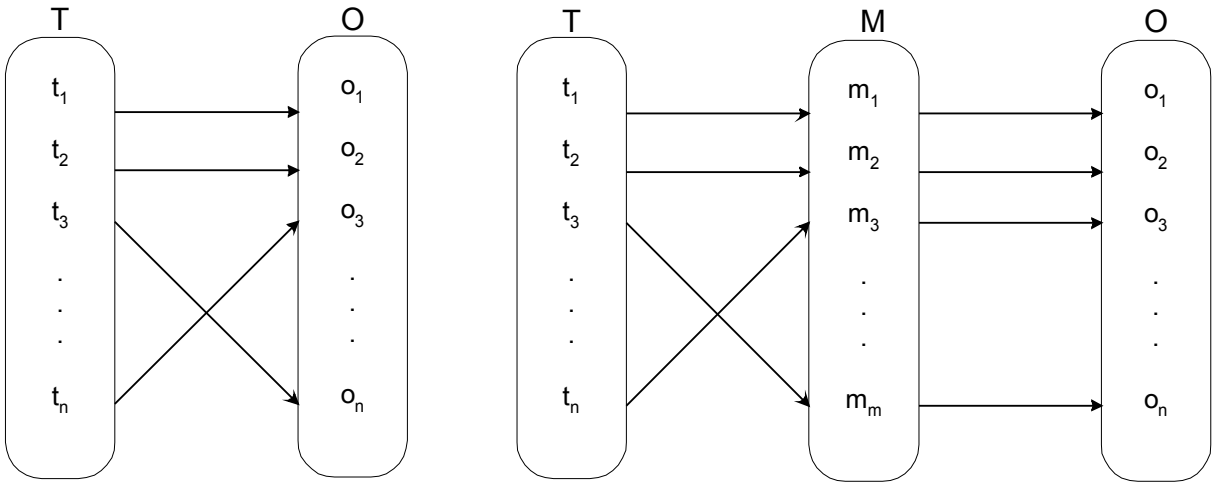
T- множество угроз ($t_n \in T$);

M- множество средств защиты ($m_m \in M$);

V - множество уязвимых мест (отображение $\mathbf{T}x\mathbf{O}$ на множестве $V_n=<t_n,o_n>$ - пути проникновения);

B - множество барьеров (отображение $\boldsymbol{VxM}$ или $\boldsymbol{TxMxO}$ на множестве $B_n=<t_n,m_m,o_n>$).

В свою очередь элемент множества барьеров B описывается тремя



$t_n \in T$ $o_n \in T$ $t_n \in T$ $m_m = M$ $o_n \in O$

а) б)

Рис.14. Модель взаимодействия угроз и объектов АИС: *а* - без системы информационной безопасности, *б* - при наличии системы информационной безопасности.

компонентами. Например, дуга $b_5<t_5,m_5,o_5>$ обеспечивает противостояние угрозе t_5 возможности доступа к объекту o_5 с помощью средства защиты m_5 (*рис. 14.б.*) и характеризует вероятность появления угрозы - p, размер угрозы при проникновении к объекту - l, степень сопротивления угрозе - r.

Во многих работах предпринимались попытки классификации средств обеспечения информационной безопасности [30,152,35,153,119, 173 и др.], но отдельные подходы неполностью характеризуют природу угроз и возможности защиты из-за узости используемых признаков классификации. Например, с точки зрения используемых методов, в [35,38, 30,137,135,170 и др.] средства обеспечения безопасности классифицируются на правовые, организационно - административные, программно - технические и криптографические.

На основе проведенного анализа работ [149,38,30,137,135,102,101 и др.], нами предлагается общая классификация методов и средств обеспечения информационной безопасности, представленная на рис 15.

При реализации механизмов безопасности в коммерческих компьютерных системах используются в основном локальный и комплексный подходы [149]. Локальные методы применяются если угроза реально оценена и хорошо разработаны механизмы защиты на отдельных участках компьютерной системы (в определенных узлах сети, на отдельных компьютерах). Поэтому они используются в тех случаях, когда угрозы носят узконаправленный характер (например, компьютерные вирусы). Комплексный подход приемлем при необходимости обеспечения информационной безопасности всей системы в целом, или если спектр реальных угроз превышает допустимый уровень.

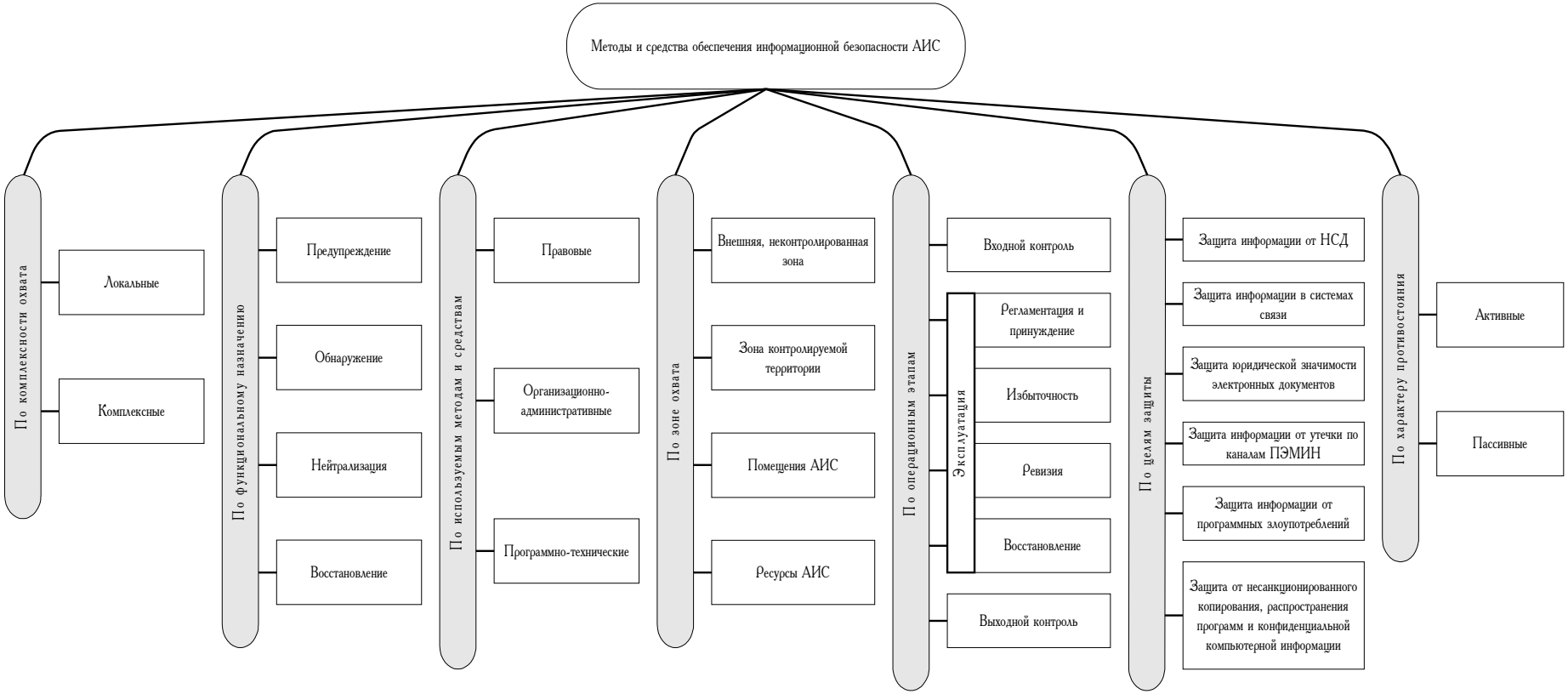


Рис. 15. Общая классификация методов и средств обеспечения информационной безопасности АИС.

В таблице 2 приведены основные характеристики приведенных подходов.

Таблица 2

Основные характеристики подходы к обеспеЧению безопасности информационной системы

№	Требования, параметры, характеристики	Подход	
		Локальный	Комплексный
1.	Существование единой защищенной среды обработки информации	Нет	Да
2.	Применение	Локальное	В крупных и средних КС
3.	Чувствительность к ошибкам установки и настройке средств защиты	Низкая	Высокая
4.	Сложность управления	Нет	Да
5.	Ограничения на свободу действий пользователей	Нет	Да
6.	Гибкость	Нет	Ограниченная
7.	Охват угроз (количество обрабатываемых нарушений)	Низкий	Высокий
8.	Взаимосвязь с системой	Низкая	Высокая

По нашему мнению, при классификации средств и методов защиты необходимо исходить из функционального покрытия угроз безопасности АИС. По своему функциональному назначению методы и средства информационной безопасности можно разделить на следующие разновидности:

- методы и средства *предупреждения* - предназначены для создания таких условий, при которых возможность появления и реализации дестабилизирующих факторов (угроз) исключается или сводится к минимуму;

- методы и средства *обнаружения* - предназначены для обнаружения появившихся угроз или возможности их появления и сбора дополнительной информации;

- методы и средства *нейтрализации* - предназначены для устранения появившихся угроз;

- методы и средства *восстановления* - предназначены для восстановления нормальной работы;

В [149] информационная безопасность разделяется на внешнюю и внутреннюю.

Интересным по содержанию является предложенный в [38, 52 и др.] метод классификации методов и средств защиты, авторы которого предлагают использовать шестирубежную модель защиты, которая состоит из следующих компонентов: территории; здания (помещения); средств (ресурсов) АИС; линий связи, проходящих в пределах помещения; линий связи, проходящих в пределах охраняемой территории; линий связи, проходящие по неконтролируемой территории.

По нашему мнению, для комемерческих АИС методы и средства обеспечения информационной безопасности по зонам охвата следует объединить в четыре зоны: неконтролируемая территория; контролируемая территория; помещения АИС и ресурсы АИС. Таким образом предлагается многоуровневая структура зон защиты АИС (рис. 16), объединяющая использование для каждого уровня соответствующих методов и средств обеспечения безопасности информации.

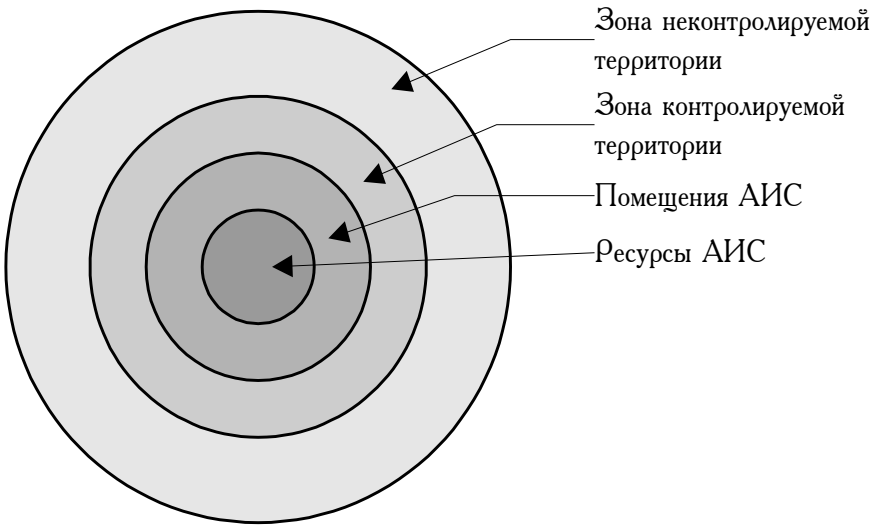


Рис. 16. Структура зон обеспечения информационной безопасности АИС

По операционным этапам можно выделить следующие этапы: при входе в систему: входной контроль; при экслплуатации АИС: регламентация и принуждение, избыточность, ревизия, восстановление; при выходе из системы: выходной контроль.

По целям защиты можно выделить защиту: от НСД; информации в системах связи; юридической значимости электронных документов; от утечки информации по каналам ПЭМИН; информации от программных злоупотреблений; от несанкционированного копирования, распространения программ и конфиденциальной компьютерной информации.

По характеру противодействия выделяются активные и пассивные методы и средства защиты.

На основе анализа объектов информационной безопасности и методов и средств защиты представляется необходимым исследовать их взаимосвязь (рис. 17).

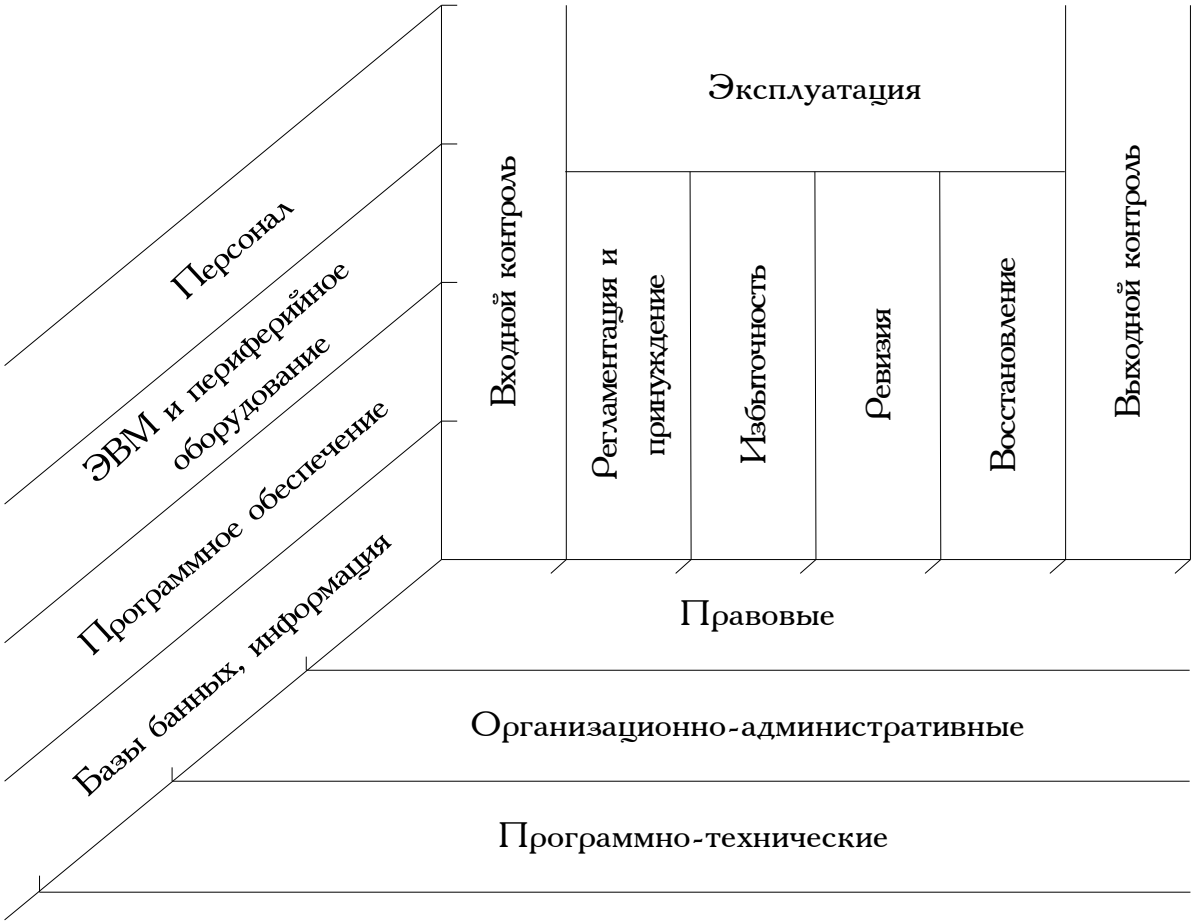


Рис. 17. Взаимосвязь методов и средств и объектов информационной безопасности АИС.

Условно объединив ресурсы АИС в такие группы как персонал, ЭВМ и периферийное оборудование, программное обеспечение и информация, можно отметить, что информационная безопасность каждой компоненты должно быть проверена и обеспечена перед началом использования в АИС (при входе в систему), обеспечена на протяжении жизненного цикла в рамках АИС и проверена и обеспечена при выходе из АИС.

Обеспечение информационной безопасности каждой компоненты должно осуществляться с использованием всего спектра: правовых, организационно-административных и программно-технических методов и средств.