3 Модель угроз и модель нарушителя физической безопасности

Угроза - потенциальная возможность совершения действий направленных на нарушение безопасности объекта.

Причинами возникновения угроз могут быть (фактор неопределенности):

- действие нарушителей;
- воздействие стихийных сил;
- сбои в работе средств СФЗ;
- воздействие субъективного фактора.

Исходными данными для проведения оценки и анализа угроз безопасности служат результаты анкетирования субъектов отношений, направленные на уяснение направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых на объекте и условий расположения и эксплуатации объекта.

Для составления перечня угроз необходимо:

- определить перечень актуальных источников угроз;
- определить перечень актуальных уязвимостей;
- оценить взаимосвязь угроз, источников угроз и уязвимостей;
- определить перечень возможных атак на объект;
- оценить возможные последствия реализации угроз.

3.1 Анализ возможных источников угроз безопасности

Физическая безопасность работает с набором угроз, уязвимостей и контрмер, отличающимся от компьютерной и информационной безопасности. Угрозы физической безопасности в большей степени направлены на кражу, вандализм, терроризм, а также могут быть связаны с природными катаклизмами и политическими событиями.

Угрозы направлены на защищаемые объекты:

– персонал;

– финансовые средства;

– информация, носители информации;

– средства и системы информатизации (автоматизированные системы и вычислительные сети, линии телеграфной, телефонной, факсимильной, радиосвязи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);

– материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

– объекты, обеспечивающие жизнедеятельность предприятия (энерго, тепло, водоснабжение).

– технические средства и системы охраны и защиты ресурсов.

Важное место среди защищаемых объектов занимает информация и носители информации. Для анализа угроз безопасности информации необходимо рассматривать два вида угроз: угроза воздействия нарушителя на информацию (кража, искажение, разглашение, модификация и т.д.) и угроза утечки по различным каналам: акустическим, визуально-оптическим, электромагнитным, материально-вещественным.

Основные элементы описания угроз утечки информации по техническим каналам представлены на рисунке 3.1.

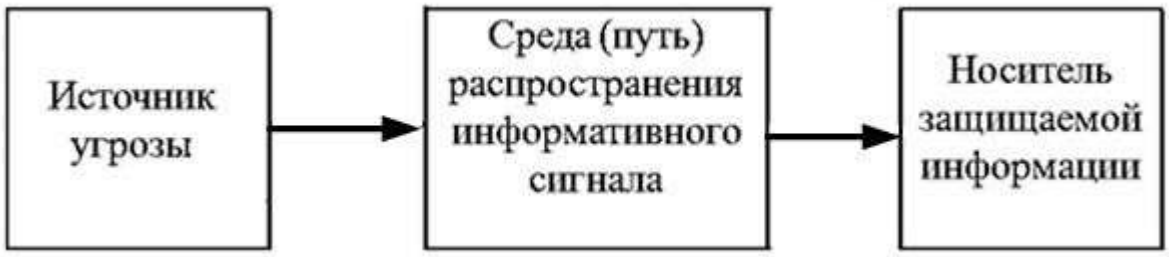

Рисунок 3.1 - Основные элементы угроз утечки информации

Угрозы утечки информации по техническим каналам:

− угрозы утечки речевой (акустической) информации по техническим каналам;

− угрозы утечки видовой (графической) информации ограниченного доступа визуальнооптическими средствами;

− угрозы утечки информации ограниченного доступа по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка информации - неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к ней и ее получения разведками.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Носитель защищаемой информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Все множество источников угроз физической безопасности можно разделить на антропогенные и естественные. Антропогенные источники угроз связаны с деятельностью человека, естественные источники угроз включают техногенные и стихийные источники угроз. Стихийные источники угроз включают обстоятельства, составляющие непреодолимую силу, носящие объективный и абсолютный характер. К стихийным источникам относятся:

– природные катаклизмы;

– события социально-политического характера.

Классификация угроз безопасности представлена на рисунке 3.2.

Рисунок 3.1 – Источники угроз физической безопасности

Техногенные источники угроз - это технические средства и технологии, которые могут выйти из-под контроля человека. К техногенным источникам угроз относятся:

- средства связи;
- сети электропитания;
- системы кондиционирования;
- технические средства обработки информации;
- программное обеспечение (ПО).

Техногенные источники угроз могут быть как внешними, так и внутренними. К внешним техногенным источникам угроз относятся:

− сбои в электроснабжении объекта;

− нарушения в работе систем жизнеобеспечения зданий;

− нарушения в работе вычислительных сетей из-за внешних воздействий;

− сбои в работе сетей телефонной связи.

К внутренним техногенным источникам угроз относятся:

− неправильное конфигурирование инженерно-технических средств защиты (систем СКУД, ОПС, видеонаблюдения и связи), приводящие к непроизводительным затратам;

− незапланированная потеря каналов связи, невозможность управления системой охранно-пожарной сигнализации и видеонаблюдения на объектах с пульта централизованного наблюдения;

− нарушение функционирования пульта централизованного наблюдения у оперативного дежурного (некомпетентность оператора, сбой программного обеспечения, выход из строя отдельных комплектующих компьютера, др.);

− нарушение работы системы СКУД, несанкционированный пропуск посторонних лиц на территорию объектов, допуск к материальным ценностям, конфиденциальной информации.

Антропогенные источники - субъекты внутри или вне организации, целенаправленные или ошибочные действия которых являются причиной нарушения безопасности . К ним относятся нарушители внешние и внутренние.

3.2 Модель нарушителя физической безопасности

Нарушитель - лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охранно-пожарной сигнализации без разрешения ответственного лица, пользователя, владельца, а также лицо, оказывающее ему содействие в этом.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов все нарушители могут быть отнесены к следующим двум категориям:

− категория I – лица, не имеющие права доступа в контролируемую зону;

− категория II – лица, имеющие право доступа в контролируемую зону.

Все потенциальные нарушители подразделяются на:

− внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны;

− внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами КЗ. В качестве внешнего нарушителями из числа лиц категории I могут выступать:

− бывшие сотрудники предприятий отрасли;

− представители конкурирующих организаций;

− представители преступных организаций;

− промышленная разведка;

− представители обслуживающих организаций (монтаж оборудования, ремонт элементов системы жизнеобеспечения зданий и т.п.).

Внешний нарушитель может осуществлять:

− несанкционированное проникновение в контролируемые зоны;

− совершение кражи защищаемых ценностей и информации;

− перехват видовой информации из-за пределов КЗ;

− перехват речевой информации из-за пределов КЗ;

− перехват информации, обрабатываемой техническими средствами за счет их утечки по ТКУИ с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;

− деструктивные воздействия через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;

− несанкционированный доступ к защищаемым объектам организации с использованием специальных технических средств;

− перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа (НСД) к информации организационно-техническими мерами;

– вывод из строя элементов системы физической защиты.

Внутренний нарушитель - нарушитель из числа лиц, имеющих право доступа без сопровождения в охраняемые зоны, является сотрудником организации.

Наибольшую опасность для инфромационной безопасности предприятия представляют его сотрудники, так как они имеют доступ в контролируемые зоны и к служебной информации и достаточную осведомленность. Внутренние нарушители могут быть разделены на преднамеренных и непреднамеренных.

Непреднамеренные:

− совершающие нарушения по неосторожности, из-за непрофессионализма,

− манипулируемые (не осознающие совершаемых нарушений).

Преднамеренные:

− выполняющие задания внешних заинтересованных лиц (конкурентов, промышленной разведки и т.п.),

− в целях саботажа.

Модель (образ) нарушителя представляет собой его комплексную характеристику, отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения.

Характеристики нарушителя учитываются при определении требований к комплексу инженерно-технических средств охраны и/или его составным частям.

Составляющие модели нарушителя:

– категории нарушителя и его возможные тактические методы (внешние, внутренние, внешние в сговоре с внутренними);

– возможные действия нарушителя (применение силы, хищение, дезинформация и т.д.);

– причины и мотивы действий нарушителя;

– возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

Для описания моделей нарушителей в качестве критериев классификации рассматриваются следующие критерии.

1 Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;
- причинение ущерба объекту;
- преднамеренное проникновение при отсутствии враждебных намерений;
- случайное проникновение.

2 Степень принадлежности вероятного нарушителя к объекту:

- вероятный нарушитель - сотрудник охраны;
- вероятный нарушитель - сотрудник учреждения;
- вероятный нарушитель - посетитель;
- вероятный нарушитель - постороннее лицо.

3 Степень осведомленности вероятного нарушителя об объекте:

- детальное знание объекта;
- осведомленность о назначении объекта, его внешних признаках;
- неосведомленный вероятный нарушитель.

4 Степень осведомленности нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;

− информация о системе охраны вообще, но не о системе охраны конкретного объекта;

− неосведомленный вероятный нарушитель.

5 Степень профессиональной подготовленности вероятного нарушителя:

− специальная подготовка по преодолению систем охраны;

− вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6 Степень физической подготовленности вероятного нарушителя:

− специальная физическая подготовка;

− низкая физическая подготовка.

7 Владение вероятным нарушителем различными способами маскировки.

8 Степень технической оснащенности вероятного нарушителя.

9 Способ проникновения вероятного нарушителя на объект.

На основе изложенных критериев выделяют четыре категории нарушителя:

− нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;

− нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;

− нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;

− нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

Модели нарушителя по типу бывают: неформализованные, формализованные.

Неформализованная модель нарушителя представляет собой словесное описание его, отражает причины и мотивы действий, его возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей, способы реализации исходящих от него угроз, место и характер действия, возможная тактика.

Типовая модель нарушителя представлена в таблице 3.1.

Таблица 3.1 - Типовая модель нарушителя

Тип нарушителя	Категория	Подготовленность нарушителя								
		Психофизическая			Техническая			Осведомленность		
		В	С	Н	В	С	Н	В	С	Н
Внутренние	Сотрудники, имеющие санкционированный доступ к материальным ценностям		+			+		+		
	Сотрудники, имеющие доступ к финансовым ценностям		+			+		+		
	Сотрудники, имеющие доступ к служебной информации	+			+			+		
	Сотрудники, имеющие доступ к элементам системы защиты		+			+			+	
	Обслуживающий персонал (охрана, инженерно-технические службы)			+		+			+	
Внешние	Уполномоченный персонал разработчиков, который имеет право на техническое обслуживание	+			+			+		
	Уволенный сотрудник		+			+			+	
	Недобросовестные партнеры		+			+			+	
	Конкуренты		+				+		+	
	Посетители			+			+			+

Формализованная модель нарушителя представляет собой математическое описание его, которое обычно строится на основе теории графов и методов нечеткой логики, позволяющих делать выводы на основе неполных сведений об анализируемом объекте. Формализованная модель нарушителя может быть основана на многокритериальном ранжировании с применением рейтингового метода. Формализация нечеткой информации проводится на основе лингвистического подхода с переходом к единой количественной шкале, при этом строятся базы знаний для модели определения уровня опасности потенциального нарушителя. Уровень нарушителя может быть в диапазоне от 0 – абсолютно неопасный нарушитель, до 1 – очень опасный нарушитель. Который способен проникнуть на объект и при этом достигнуть поставленной цели почти со стопроцентной вероятностью [3,19].

3.3 Характеристика каналов утечки защищаемой информации

Понятие «утечка» относится к защищаемой информации. Утечка информации – это несанкционированный перенос информации от ее источника к нарушителю. Утечка информации осуществляется за счет ее разглашения, утери или кражи носителей информации, переноса ее с помощью полей. При утечке информации, из-за увеличения круга ее потребителей, цена информации уменьшается [33, 34].

Физическая среда несанкционированного распространения носителя защищаемой информации от ее источника к нарушителю образует канал утечки информации. Вид канала утечки зависит от вида носителя информации. Основными классификационными признаками технических каналов утечки информации является физическая природа носителя, по этому признаку все каналы утечки бывают:

- оптические;
- радиоэлектронные;
- акустические;

– вещественные.

Классификация каналов утечки информации представлена в таблице 3.2.

Таблица 3.2 - Классификация каналов утечки информации

Признак классификации	Наименование канала	Пример, краткое описание
По виду носителя	оптические	окна, двери, прозрачные межкомнатные перегородки
	радиоэлектронные	Телефоны, розетки, линия электропередач. ПЭВМ, система оповещения, ОПС
	акустические	окна, двери, батареи, водопровод, стены
	вещественные	документы на бумажных носителях, черновики, отходы производства
По структуре	простые	состоят из одного канала утечки
	составные	состоят из нескольких каналов одновременно
По способу организации	случайные	одноразовое добывание информации
	организованные	создаются злоумышленником для регулярного добывания информации
По времени функционирования	постоянные	утечка носит регулярный характер
	эпизодические	утечка носит кратковременный характер
По степени скрытия информации	открытые	передача информации в открытом виде
	технически закрытые	с использованием технических средств сокрытия канала утечки
	зашифрованные	с использованием шифрования информации

Технический канал утечки информации характеризуется показателями, которые позволяют оценить риск утечки:

- пропускная способность канала утечки;
- длина технического канала утечки;
- относительная информативность канала.

Все эти показатели зависят от параметров источника сигнала, среды распространения и приемника сигнала.

Источник сигнала характеризуется следующими показателями:

- мощность сигнала;
- диаграмма направленности излучения сигнала;
- параметрами спектра сигнала;
- динамическим диапазоном сигнала.

Среда распространения характеризуется:

- скоростью распространения носителя в среде;
- коэффициентом передачи или ослабления энергии сигнала;
- видом и мощностью помех.

Основными параметрами приемника являются:

- диапазон принимаемых частот;
- чувствительность;
- селективность;
- вид и уровень искажений.

Наибольшими потенциальными возможностями по добыванию семантической информации о видовых демаскирующих признаках обладает оптический канал, в котором информация добывается путем фото и видеосъемки.

Основным каналом получения сигнальных демаскирующих признаков является радиоэлектронный канал. В значительном меньшем объеме утечка информации возможна в акустическом и вещественном каналах. Комплексное добывание информации осуществляется злоумышленником по нескольким параллельным или последовательным каналам утечки.

3.4 Модель угроз физической безопасности защищаемого объекта

Угрозы физической безопасности объектов определяются типом источников угроз и направлением действия угроз. Соответственно угрозы могут быть антропогенного, техногенного или стихийного характера, направлены они могут быть как на материальные, финансовые ценности, так и на защищаемую информацию. Типы угроз: диверсия, терроризм, нарушение технологических процессов, хищение материальных ресурсов, информации. Основные угрозы физической безопасности приведены в таблице 3.3

Таблица 3.3 - Основные угрозы физической безопасности

Угроза	Тип источника угроз
1	2
Несанкционированное проникновение в КЗ	Антропогенный
Совершение диверсии в КЗ	Антропогенный
Совершение террористических актов	Антропогенный
Несанкционированные действия, приводящие к нарушению производственных технологических процессов	Антропогенный
Несанкционированный доступ к компьютерам	Антропогенный
Кража технических средств с хранящейся в них информацией	Антропогенный
Кража носителей информации	Антропогенный
Кража материальных и финансовых ценностей	Антропогенный
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств	Антропогенный
Прослушивание телефонных и радиопереговоров	Антропогенный
Внедрение «закладок»	Антропогенный
Воздействие на технические средства в целях нарушения их работоспособности	Техногенный
Воздействие на программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации	Техногенный
Воздействие на средства защиты информации	Техногенный

Продолжение таблицы 3.3

1	2
Побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации	Техногенный
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ	Техногенный
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств	Техногенный
Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом	Техногенный
Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	Техногенный
Угроза пожара	Стихийный
Угроза наводнения	Стихийный
Отказы и сбои в работе инженерно-технических средств охраны	Техногенный
Отказы и сбои в работе системы электроснабжения	Техногенный
Незапланированная потеря каналов связи, невозможность управления системой ОПС и видеонаблюдения на объектах с пульта централизованного наблюдения	Техногенный
выход из строя системы видеонаблюдения	Техногенный
выход из строя СКУД	Техногенный
Непреднамеренные (ошибочные, случайные, без корыстных целей) нарушения установленных требований при работе с материальными ценностями, финансовыми ресурсами, информацией, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный
Преднамеренные (в корыстных целях, по принуждению, со злым умыслом, т.п.) действия сотрудников, допущенных к материальным, финансовым и информационным ресурсам, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный

Оценка угроз безопасности в результате несанкционированного проникновения злоумышленника на объект или в результате утечки информации по техническим каналам проводится с учётом вероятности реализуемости рассматриваемого пути или канала, а также с учётом цены соответствующего элемента информации.

Обеспечение эффективной безопасности предполагает решение проблем моделирования угроз, их количественной и качественной оценки с учетом сложности структурно-функционального построения системы безопасности, ее элементов, и данных о внешних воздействиях естественного и искусственного происхождения [30].

Модель угроз безопасности - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Для построения модели угроз безопасности можно применить руководящие документы ФСТЭК, разработанные для защиты персональных данных. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Частота реализации угроз безопасности определяется экспертным методом в соответствии с и на основании результатов обследования объекта.

Оценка вероятности реализации угрозы (Y2) определяется по четырем вербальным градациям:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);

– низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);

– средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны (5);

– высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты (10).

С учетом изложенного коэффициент реализуемости угрозы **Y** будет определяться соотношением

$$Y = (Y_1 + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

– если $0 \le Y \le 0{,}3$, то возможность реализации угрозы признается низкой;

– если $0{,}3 < Y \le 0{,}6$, то возможность реализации угрозы средняя;

– если $0{,}6 < Y \le 0{,}8$, то возможность реализации угрозы высокая;

– если $Y > 0{,}8$, то возможность реализации угрозы очень высокая.

Определение опасности угроз проводится экспертным методом с учетом результатов обследования объекта. Y1=5 для среднего уровня исходной защищенности.

Показателем опасности, имеет три значения:

– низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям;

– средняя опасность - если реализация угрозы может привести к негативным последствиям;

– высокая опасность - если реализация угрозы может привести к значительным негативным последствиям.

Определение актуальных угроз безопасности.

Актуальная угроза - угроза, которая может быть реализована и представляет опасность. Правила определения актуальности УБСКХ приведены в таблице 3.4.

Таблица 3.4 - Правила определения актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Пример модели угроз безопасности защищаемого объекта приведен в таблице 3.5

Таблица 3.5 - Модель угроз безопасности защищаемого объекта

Угроза	Вероятность реализации угрозы	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Несанкционированный доступ к компьютерам	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража технических средств с хранящейся в них информацией	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража носителей информации	Маловероятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража материальных и финансовых ценностей	Средняя вероятность (5)	0,5 (средняя)	Высокая	Актуальная
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероятность (5)	0, 6 (средняя)	Высокая	Актуальная

Особое внимание исследований [10, 11] уделено выбору математических методов исследования моделей угроз. При построении модели подчеркивается необходимость учитывать, что угрозы безопасности носят вероятностный характер и имеют высокую степень априорной неопределенности. При оценке угроз безопасности предлагаются:

− теория надежности для описания угроз, создаваемых техническими средствами (сбои, отказы, ошибки и т.д.);

− математическая статистика для описания естественных угроз (природные явления, стихийные бедствия и т.д.);

− теория вероятности для описания угроз, создаваемых людьми по небрежности, халатности и т.д.);

− экспертные методы для описания умышленных угроз.

Рассматривая основное назначение интегрированной системы безопасности как борьбу с угрозами различного характера, авторы считают возможным в качестве одного из комплексных критериев оценки эффективности системы безопасности использовать количественный показатель, связанный с числом угроз, защиту от которых она может обеспечить.

Появление угроз нового характера (экономических, информационных, юридических и других) требует включения в систему безопасности дополнительных средств и подсистем для защиты от данного вида угроз.