Лекция 2. Постановка задачи определения требований к защите информации.

2.1. Математическое определение требований к защите информации.

В самом общем виде и на чисто практическом уровне **требования к защите могут быть определены как предотвращение угроз информации**, по крайней мере тех из них, проявление которых может привести к существенно значимым последствиям. Но поскольку **защита информации есть случайный процесс** (показатели уязвимости носят вероятностный характер), **то и требования к защите должны выражаться терминами и понятиями теории вероятностей.**

По аналогии с требованиями к надежности технических систем, обоснованным в классической теории систем, требования к защите могут быть сформулированы в виде условия:

$$P_з \geq \overline{P}_з,$$

где $P_з$ **-** вероятность защищенности информации, а $\overline{P}_з$ **-** требуемый уровень защищенности**.** С требованиями, выраженными в таком виде, можно оперировать с использованием методов классической теории систем при решении задач защиты всех классов: анализа, синтеза и управления.

Однако известно, что решение проблем защиты информации сопряжено с исследованиями и разработкой таких систем и процессов, в которых и конкретные методы, и общая идеология классической теории систем могут быть применены лишь с большими оговорками. Для повышения степени адекватности применяемых моделей реальным процессам необходим перевод от концепции создания инструментальных средств получения необходимых решений на инженерной основе к концепции создания методологического базиса и инструментальных средств для динамического оптимального управления соответствующими процессами.

С учетом данного подхода в самом общем виде и на содержательном уровне требования к защите информации необходимо формировать с учетом специфики решаемых задач.

2. Рекомендации по предъявлению требований к защите информации.

Конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов:

- *характером обрабатываемой информации;*
- *объемом обрабатываемой информации;*
- *продолжительностью пребывания информации в АСОД;*
- *структурой АСОД;*
- *видом защищаемой информации;*
- *технологией обработки информации;*
- *организацией информационно-воспитательного процесса в АСОД;*
- *этапом жизненного цикла АСОД.*

По характеру (с точки зрения требуемой защиты) информацию можно разделить на **общедоступную, конфиденциальную, служебную, секретную и совершенно секретную.**

Соответствующие рекомендации по предъявлению требований к защите могут быть следующими.

1.При обработке **общедоступной** информации никаких специальных мер защиты от несанкционированного доступа не требуется.

2.Требования к защите **конфиденциальной** информации определяет пользователь, устанавливающий статус конфиденциальности.

3.При обработке **служебной** информации к ней должен быть обеспечен свободный доступ пользователям учреждения-владельца этой информации (по общему списку); доступ же пользователей, не включенных в общий список, должен осуществляться по разовым санкциям, выдаваемым пользователями, включенными в список.

4.При обработке **секретной** информации в зависимости от ее объема и характера может быть предъявлен один из следующих **вариантов требований**:

а) персональное разграничение - для каждого элемента информации составляется список пользователей, имеющих к нему право доступа;

б) коллективное разграничение - структура баз защищаемых данных организуется в соответствии со структурой подразделений, участвующих в обработке защищаемой информации; пользователи каждого подразделения имеют право доступа только к "своим" данным.

5. При обработке **совершенно секретной** информации список лиц, имеющих право доступа, должен составляться для каждого самостоятельного элемента информации с указанием дней и времени доступа, а также перечня разрешенных процедур.

Требования, обуславливаемые размещением ***объемов защищаемой информации,*** могут заключаться в следующем.

При обработке информации, размещенной **только в ОЗУ**, должны обеспечиваться требуемые уровень защиты и надежность в центральном вычислителе и на коммуникациях ввода-вывода данных. При обработке информации, размещенной **на одном внешнем носителе**, дополнительно к предыдущему должна обеспечиваться защита в соответствующем устройстве ВЗУ и коммуникациях, связывающих это устройство с процессором.

При обработке информации, размещенной **на нескольких внешних носителях,** дополнительно к предыдущему должна обеспечиваться необходимая изоляция друг от друга данных, размещенных на различных носителях при одновременной их обработке.

При обработке информации, размещенной **на очень большом количестве носителей**, дополнительно к предыдущему должна обеспечиваться защита в хранилищах носителей и на коммуникациях, связывающих хранилища, с помещениями, в которых установлены ВЗУ.

С точки зрения ***продолжительности пребывания защищаемой информации в А СОД*** требования к защите формулируются следующим образом.

Информация **разового использования** подлежит защите в процессе подготовки, ввода, решения задач и выдачи результатов решения. После этого защищаемая информация должна быть уничтожена во всех устройствах АСОД.

Информация **временного хранения** дополнительно к предыдущему подлежит защите в течение объявленного времени хранения, после чего должна быть уничтожена во всех устройствах АСОД и на всех носителях, используемых для ее хранения. Продолжительность хранения задается или длиной промежутка времени, или числом сеансов решения соответствующих функциональных задач.

Информация **длительного хранения** подлежит постоянной защите, уничтожение ее должно осуществляться по специальным командам.

Требования, определяемые ***структурой АСОД,*** могут быть сформулированы в следующем виде.

Информация должна защищаться во всех структурных элементах АСОД, причем специфические требования к защите информации в структурных элементах различного тина сводятся к следующему.

1. В терминалах пользователей:

а) защищаемая информация может находиться только во время сеанса решения задач, после чего подлежит уничтожению;

б) **устройства отображения и фиксации информации** должны располагаться так, чтобы исключить возможность просмотра отображаемой (выдаваемой) информации со стороны;

в) информация, имеющая **ограничительный гриф**, должна выдаваться (отображаться) совместно с этим грифом;

г) должны быть предусмотрены **возможности быстрого (аварийного) уничтожения информации,** находящейся в терминале (в том числе и на устройствах отображения).

2. В устройствах группового ввода/вывода (УГВВ);

а) в простых **УГВВ и в сложных с малым объемом ЗУ** защищаемая информация может находиться только во время решения задач, после чего подлежит уничтожению; **в сложных с большим объемом ЗУ** информация может храниться в ВЗУ, однако продолжительность хранения должна быть ограниченной;

б) и *в)* аналогично соответствующим пунктам требований к защите в терминалах пользователей;

г) в УГВВ с возможностями универсального процессора при каждом обращении к защищаемой информации должны осуществляться процедуры:

1) установления подлинности (опознавания) вступающих в работу терминалов и пользователей;

2) проверки законности каждого запроса на соответствие предоставленным пользователю полномочиям;

3) проверки адреса выдачи информации, имеющей ограничительный гриф, и наличия этого грифа;

4) контроля обработки защищаемой информации;

5) регистрации запросов и всех нарушений правил защиты;

д) при выдаче информации в линии связи должны осуществляться:
1)проверка адреса выдачи информации;

2) маскировка (закрытие) содержания защищаемой информации, выдаваемой в линии связи, проходящей по неконтролируемой территории;

е) должны быть предусмотрены возможности аварийного уничтожения информации как в ОЗУ, так и в ВЗУ, а также подачи команды на аварийное уничтожение информации в сопряженных с УГВВ терминалах,

3. В аппаратуре и линиях связи:

а) защищаемая информация должна находиться только в течение сеанса; в ЗУ аппаратуры связи могут храниться только служебные части передаваемых сообщений;

б) линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем во все время передачи информации;

в) перед началом каждого сеанса передачи защищаемой информации должна осуществляться проверка адреса выдачи данных;

г) при передаче большого объема защищаемой информации проверка адреса передачи должна также периодически производиться в процессе передачи (через заданный промежуток времени или после передачи заданного числа знаков сообщения);

д) при наличии в составе аппаратуры связи процессоров и ЗУ должна вестись регистрация данных о всех сеансах передачи защищаемой информации;

е) должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в аппаратуре связи.

4.В центральном вычислителе:

а) защищаемая информация в ОЗУ может находиться только во время сеансов решения соответствующих задач, в ВЗУ - минимальное время, определяемое технологией решения соответствующей прикладной задачи в АСОД;

б) и в) - аналогично соответствующим пунктам требований к защите в УГВВ;

г) при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей и ведение протоколов их работы;

д) всякое обращение к защищаемой информации должно проверяться на санкционированность;

е) при обмене защищаемой информации, осуществляемом с использованием линий связи, должна осуществляться проверка адреса корреспондента;

ж) должны быть предусмотрены возможности аварийного уничтожения всей информации, находящейся в центральном вычислителе, и подачи команды на аварийное уничтожение информации в сопряженных устройствах.

5. В ВЗУ:

а) сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;

б) устройства управления ВЗУ, на которых установлены носители с защищаемой информацией, должны иметь замки, предупреждающие несанкционированное изъятие или замену носителя;

в) должны быть предусмотрены возможности автономного аварийного уничтожения информации на носителях, находящихся на устройствах ВЗУ.

6. В хранилище носителей:

а) все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;

б) носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

в) при выдаче и приемке носителей должна осуществляться проверка личности получающего (сдающего) и его санкции на получение (сдачу) этих носителей;

г) должны быть предусмотрены возможности аварийного уничтожения информации на носителях, находящихся в хранилищах.

7. В устройствах подготовки данных:

а) защищаемая информация должна находиться только в течение времени ее подготовки;

б) устройства подготовки должны быть размещены так, чтобы исключались возможности просмотра обрабатываемой информации со стороны;

в) в специальных регистрационных журналах должны фиксироваться время обработки информации, исполнителе идентификаторы использованных носителей и возможно другие необходимые данные;

г) распределение работ между операторами должно бить таким, чтобы минимизировать осведомленность их о содержании обрабатываемой информации;

д) должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в подразделениях подготовки данных,

8. Требования к защите информации, обуславливаемые территориальной распределенностью АСОД, заключаются в следующем:

а) в компактных АСОД (размещенных в одном помещении) достаточно организовать и обеспечить требуемый уровень защиты в пределах того помещения, в котором размещены элементы АСОД;

б) в слабораспределенных АСОД (размещенных в нескольких помещениях, но на одной и той же территории) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи, с помощью которых сопрягаются элементы АСОД, расположенные в различных помещениях, для чего должны быть или постоянный контроль за этими линиями связи, или исключена передача по ним защищаемой информации в явном виде;

в) в сильно распределенных АСОД (размещенных на нескольких территориях) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи большой протяженности, что может быть достигнуто предупреждением передачи по ним защищаемой информации в открытом виде.

3. Методики определения требований к защите информации.

Требования, обуславливаемые ***видом защищаемой информации,*** могут быть сформулированы в таком виде.

1. К защите документальной информации предъявляются следующие требования:

а) должна обеспечиваться защита, как оригиналов документов, так и сведений о них, накапливаемых и обрабатываемых в АСОД;

б) применяемые средства и методы защиты должны выбираться с учетом необходимости обеспечения доступа пользователям различных категорий:

1) персонала делопроизводства и библиотеки оригиналов;

2) специалистов подразделения первичной обработки документов;

3) специалистов функциональных подразделений автоматизируемых органов.

2. При обработке фактографической быстроменяющейся информации должны учитываться требования:

а) применяемые средства и методы защиты не должны существенно влиять на оперативность обработки информации;

б) применяемые средства и методы защиты должны выбираться с учетом обеспечения доступа к защищаемой информации строго ограниченного круга лиц.

3. К защите фактографической исходной информации предъявляются требования:

а) каждому пользователю должны быть обеспечены возможности формирования требований к защите создаваемых им массивов данных, в пределах предусмотренных в АСОД возможностей зашиты;

б) в системе защиты должны быть предусмотрены средства, выбираемые и используемые пользователями для защиты своих массивов по своему усмотрению.

4. К защите фактографической регламентной информации предъявляются требования;

а) применяемые средства и методы зашиты должны быть рассчитаны на длительную и надежную защиту информации;

б) должен обеспечиваться доступ (в пределах полномочий) широкого круга пользователе;

в) повышенное значение приобретают процедуры идентификации, опознавания, проверки полномочий, регистрации обращений и контроля выдачи.

Требования, обуславливаемые *технологическими схемами автоматизированной обработки информации,* сводятся к тому, что в активном состоянии АСОД должна обеспечиваться защита на всех технологических участках автоматизированной обработки информации и во всех режимах.

С точки зрения *организации вычислительного процесса в АСОД* требуемая защита должна обеспечиваться при любом уровне автоматизации обработки информации, при всех способах взаимодействия пользователей со средствами автоматизации и при всех режимах работы комплексов средств автоматизации.

Специфические требования к защите для различных уровней автоматизации обработки информации состоят в следующем:

а) при автономном решении отдельных задач или их комплексов основными макропроцессами автоматизированной обработки, в ходе которых должен обеспечиваться необходимый уровень защиты, являются:

1) сбор, подготовка и ввод исходных данных, необходимых для решения задач;

2) машинное решение задач в автономном режиме;

3) выдача результатов решения;

б) в случае полусистемной обработки дополнительно к предыдущему на участках комплексной автоматизации должна быть обеспечена защита в ходе осуществления следующих макропроцессов:

1) автоматизированного сбора информации от датчиков и источников информации;

2) диалогового режима работы пользователей ЭВМ;

в) в случае системной обработки дополнительно к предыдущему должна быть обеспечена защита в ходе таких макропроцессов:

1) прием потока запросов и входной информации;

2) формирование пакетов и очередей запросов;

3) диспетчирование в ходе выполнения запросов;

4) регулирование входного потока информации.

В зависимости от способа взаимодействия пользователей с комплектом средств автоматизация предъявляются следующие специфические требования:

а) при автоматизированном вводе информации должны быть обеспечены условия, исключающие несанкционированное попадание информации одного пользователя (абонента) в массив другого, причем должны быть обеспечены возможности фиксирования и документального закрепления момента передачи информации пользователя банку данных АСОД и содержания этой информации;

б) при неавтоматизированном вводе должна быть обеспечена защита на неавтоматизированных коммуникациях "Пользователь - АСОД", на участках подготовки данных и ври вводе с местных УГВВ;

в) при пакетном выполнении запросов пользователей должно исключаться размещение в одном и том же пакете запросов на обработку информации различных ограничительных грифов;

г) при обработке запросов пользователей в реальном масштабе времени данные, поступившие от пользователей, и данные, подготовленные для выдачи пользователям, в ЗУ АСОД должны группироваться с ограничительным грифом, при этом в каждой группе должен быть обеспечен уровень защиты, соответствующий ограничительному грифу данных группы,

В зависимости от режимов функционирования комплексов средств автоматизации предъявляют следующие специфические требования:

а) в однопрограммном режиме работы в процессе выполнения программы должны предупреждаться:

1) несанкционированное обращение к программе;

2) несанкционированный ввод данных для решаемой задачи;

3) несанкционированное прерывание выполняемой программы;

4) несанкционированная выдача результатов решения;

б) в мультипрограммном режиме сформулированные выше требования относится к каждой из выполняемых программ и дополнительно должно быть исключено несанкционированное использование данных одной программы другой;

в) в мультипроцессорном режиме сформулированные выше требования должны обеспечиваться одновременно во всех участвующих в решении задачи процессорах, кроме того, должно быть исключено несанкционированное вклинивание в вычислительный процесс при распараллеливании и при диспетчеризации мультипроцессорного выполнения программ.

Требования, обуславливаемые *этапом жизненного цикла АСОД,* формулируются так:

а) на этапе создания АСОД должно быть обеспечено соответствие возможностей системы защиты требованиям к защите информации, сформулированным в задании на проектирование, кроме того, должно быть исключено несанкционированное включение элементов (блоков) в компоненты АСОД (особенно системы зашиты);

а) на этапе функционирования АСОД в пассивном ее состоянии должна быть обеспечена надежная защита хранящейся информации и исключены возможности несанкционированных изменений компонентов системы;

в) на этапе функционирования АСОД в активном ее состоянии дополнительно к сформулированным выше требованиям должна быть обеспечена надежная защита информации во всех режимах автоматизированной ее обработки.

Так могут быть представлены общие рекомендации по формированию требований к защите информации.

Нетрудно однако, видеть, что приведенные выше требования хотя и содержат полезную информацию, но недостаточны для выбора методов и средств защиты информации в конкретной АСОД. Решение каждой конкретной задачи может быть найдено на пути структурно-логического анализа систем и ситуаций защиты и структурированного их описания с широким

применением методологии и методов рассмотренной в гл. 2 неформальной теории систем.

Последовательность решения задачи в указанной постановке, очевидно, должна быть следующей:

1) разработка методов оценки параметров защищаемой информации;

2) формирование перечня и классификация факторов, влияющих на требуемый уровень защиты информации;

3) структуризация возможных значений факторов;

4) структуризация поля потенциально возможных вариантов сочетаний значений факторов (вариантов условий защиты);

5) оптимальное деление поля возможных вариантов на типовые классы;

6) структурированное описание требований к защите в пределах выделенных классов.

Подходы к решению перечисленных составляющих задач рассматриваются в следующих параграфах.

Лекция 2.2. Методы оценки параметров защищаемой информации.

План лекции.

1. Показатели для оценки параметров защищаемой информации.
2. Оценка важности информации.
3. Оценка полноты и релевантности информации.

1. Показатели для оценки параметров защищаемой информации.

Информация становится для современного общества все более и более значимым ресурсом, опережая в этом традиционно считавшиеся важнейшими сырьевые и энергетические ресурсы. Информационное обеспечение становится важнейшим видом обеспечения практически всех без исключения сфер деятельности общества и быта людей. Но для того, чтобы в процессе деятельности информация эффективно выполняла свою роль, необходимо уметь оценивать значимость ее для эффективности соответствующей деятельности, имея в виду при этом, что в условиях информационного общества она является объектом и продуктом труда. Таким образом, для оценки информации необходимы показатели двух видов:

1) характеризующие информацию как обеспечивающий ресурс в процессе деятельности общества, или привычнее - в процессе решения различных задач;

2) характеризующие информацию как объект труда в процессе информационного обеспечения решаемых задач.

Показатели первого вида носят прагматический характер, их содержание определяется ролью, значимостью, важностью информации в процессе решения задач, а также количеством и содержанием информации, имеющейся в момент решения соответствующей задачи**.** Причем здесь **важно** не просто количество сведений в абсолютном выражении, а **достаточность** (полнота) их **для информационного обеспечения решаемых задач и адекватность**, т.е. соответствие текущему состоянию тех объектов или процессов, к которым относится оцениваемая информация. Кроме того, важное значение имеет **чистота информации**, т.е. отсутствие среди необходимых данных ненужных данных или, как принято говорить, шумов. В наукометрии такая характеристика названа **релевантностью информации.** Наконец для эффективности решения задач немаловажное значение имеет **форма представления информации с точки зрения удобства восприятия и использования ее в процессе решения задач.** Такую характеристику принято называть **толерантностью.**

Таким образом, показатели первого вида: ***важность,*** значимость с точки зрения тех задач, для решения которых используется оцениваемая информация; ***полнота информации*** для информационного обеспечения

решаемых задач; ***адекватность,*** т.е. соответствие текущему состоянию соответствующих объектов или процессов; ***релевантность информации,*** поступающей для информационного обеспечения решаемых задач; ***толерантность*** поступающей информации.

Показатели второго вида должны характеризовать информацию как **объект труда**, над которым осуществляются некоторые процедуры в процессе переработки ее с целью информационного обеспечения решаемых задач. В этом качестве информация **выступает**, во-первых, **как сырье**, добываемое и поступающее на обработку, во-вторых, **как полуфабрикат**, образуемый в процессе обработки, и, в-третьих, **как продукт обработки**, выдаваемый для использования. Причем процесс обработки информации может быть представлен в **естественной последовательности**: добыча сырья - переработка сырья и получение на этой основе необходимых полуфабрикатов - переработка полуфабрикатов с целью получения конечного продукта. Естественно, что при этом **информация непременно должна оцениваться по совокупности рассмотренных выше показателей первого вида.** Вернее даже будет сказать, что ***технологические процессы обработки информации должны организовываться таким образом, чтобы конечный продукт обработки, т.е. информация, выдаваемая для использования, наилучшим образом удовлетворяла всей совокупности показателей первого вида.***

Для обработки информации используются различные **средства**, основными из которых являются средства **фиксации**, средства **передачи** и средства **переработки**. С точки зрения использования этих средств **основными характеристиками выступают** форма, способ представления и объемы информации безотносительно к ее смысловому содержанию**.** Поскольку, как известно, информация представляется в виде некоторой последовательности символов, т.е. кодируется, то в качестве основных характеристик второго вида могут выступать две: 1) способ, система кодирования информации; 2) объем информации или вернее объем последовательности кодов, отражающих обрабатываемую информацию**.**

Однако этого недостаточно. В общем случае на всех участках технологических маршрутов обработки имеются потенциальные возможности проявления большого количества дестабилизирующих факторов, которые могут оказать негативное воздействие на информацию. В силу этого в процессе обработки информации неизбежно приходится принимать меры противодействия дестабилизирующим факторам, причем, чем важнее информация, тем большие усилия должны предприниматься в указанных целях. Причем здесь **важность информации должна рассматриваться как в смысле значимости ее для решаемых задач, так и в смысле организации обработки.** Таким образом, и здесь также необходим показатель важности информации.

Рассмотрим подходы к определению значений перечисленных показателей.

2. Оценка важности информации.

1) Важность информации. В соответствии с изложенным выше, важность информации есть обобщенный показатель, характеризующий, с одной стороны, значимость информации с точки зрения тех задач, для решения которых она используется, а с другой - с точки зрения организации ее обработки. Иными словами, **важность информации должна оцениваться, по крайней мере, по двум группам критериев: по назначению информации и по условиям ее обработки.**

В первой группе, очевидно, следует выделить такие два составляющих критерия, как важность самих задач дня обеспечиваемой деятельности и степень важности информации для эффективного решения соответствующей задачи**.**

Во второй группе также выделяются два составляющих критерия: уровень потерь в случае нежелательных изменений информации в процессе обработки под воздействием дестабилизирующих факторов и уровень затрат на восстановление нарушенной информации**.**

Обозначим:

$K_{ви}$ - коэффициент важности информации;

$K_{вз}$ - коэффициент важности задач, для обеспечения решения которых используется информация;

$K_{из}$ - коэффициент важности информации для эффективного решения задач;

$K_{пи}$ - коэффициент важности информации с точки зрения потерь при нарушении ее качества;

$K_{св}$ - коэффициент важности информации с точки зрения стоимости восстановления ее качества.

Тогда, очевидно:

$$K_{ви} = f(K_{вз}, K_{из}, K_{пи}, K_{св}) \qquad (7.1)$$

Иными словами, для оценки важности информации необходимо уметь определять значения перечисленных выше коэффициентов и знать вид функциональной зависимости (7.1). Однако на сегодняшний день неизвестно ни то, ни другое, и есть веские основания утверждать, что и в ближайшем будущем эта проблема не будет решена.

В качестве выхода из положения используем следующий подход, основанный на неформально-эвристических методах. Значения входящих в формулу (7.1) критериев будем выражать лингвистическими переменными. Возможные значения этих переменных на рис 7.1. Затем сформируем возможные комбинации критериев в пределах каждой группы. Результаты этой работы приведены в табл. 7.1а и 7.1б. Сведем теперь воедино полученные результаты, что и даст итоговую классификацию информации по важности. Эта классификация приведена, а табл. 7.2. При этом сделано предположение, что диагональные (слева вверх направо) элементы классификационной структуры являются одинаково важными.

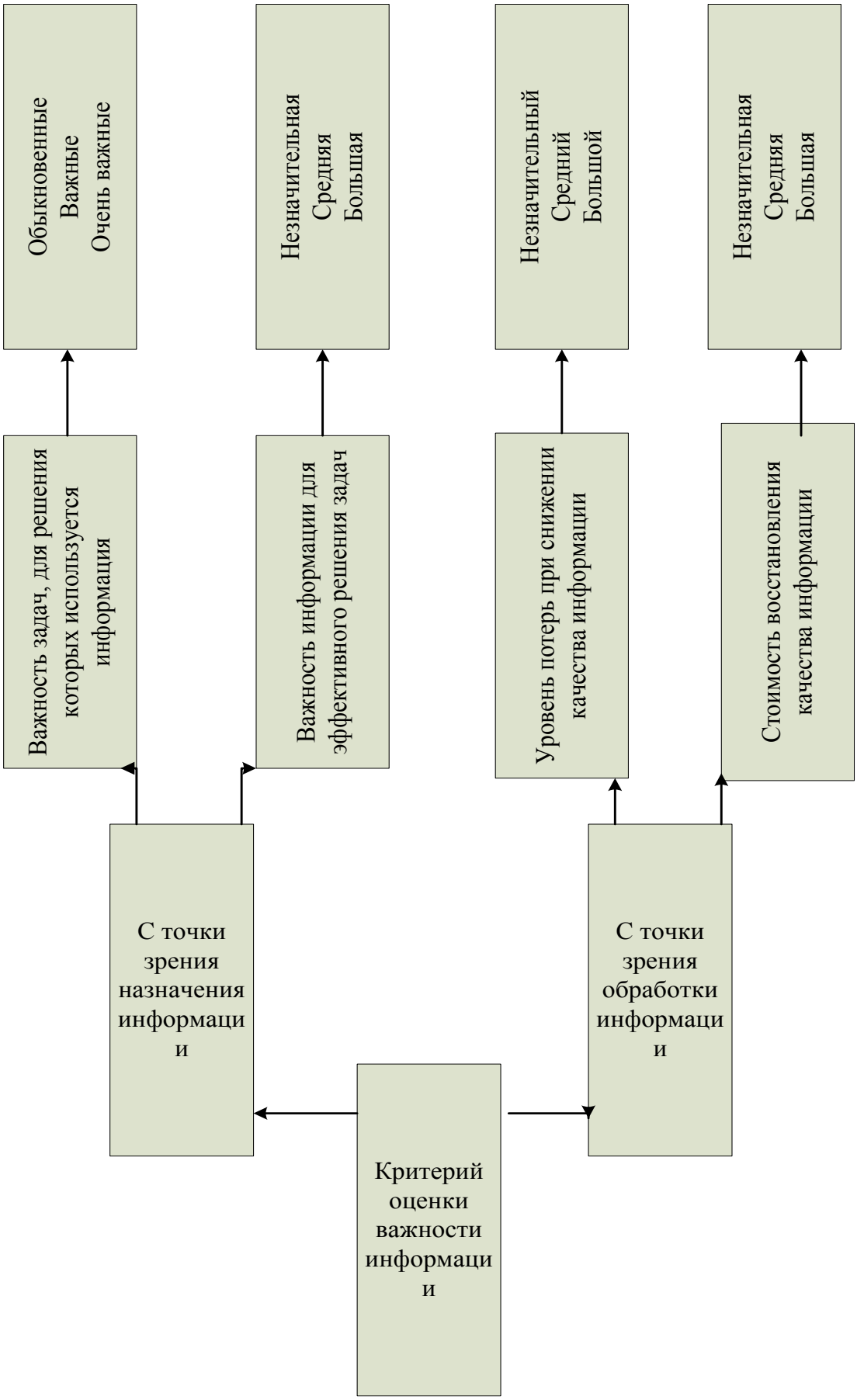

Рисунок 7.1- Структура и значения критериев оценки важности информации

Таблица 7.1 - Первичная классификация информации по важности

а) Относительно назначения

Значения критерия "Важность задачи"	Важность информации для задачи		
	Незначительная	Средняя	Большая
Обыкновенная	1н	2н	Зн
Важная	4н	5н	бн
Очень важная	7н	8н	9н

б) Относительно обработки

Значение критерия "Уровень потерь"	Стоимость восстановления		
	Незначительная	Средняя	Большая
Незначительный	1о	2о	Зо
Средний	4о	5о	6о
Большой	7о	8о	9о

Таким образом, оказалось, что при выбранных значениях составляющих критериев вся информация делится на семнадцать классов важности. Однако номер класса сам по себе не характеризует важность информации на содержательном уровне, да и оперировать семнадцатью

различными классами затруднительно. С целью преодоления указанных трудностей, разделим все элементы классификационной структуры так, как показано в табл. 7.2 пунктирными линиями. В итоге семнадцать классов разделились на семь категорий важности, которым присвоим следующие содержательные наименования:

МлВ - маловажная (категория А);

Об В - обыкновенной важности (категория Б);

Пс В - полусредней важности (категория В);

Ср В- средней важности {категория Г);

Пв В - повышенной важности (категория Д);

Бл В - большой важности (категория Е);

ЧрВ- чрезвычайной важности (категория Ж).

Таблица 7.2- Итоговая классификация информации по важности

Важность информации		Относительно обработки								
		1о	2о	3о	4о	5о	6о	7о	8о	9о
Относительно назначения	1н	1	2	3	4	5	6	7	8	9
	2н	2	3	4	5	6	7	8	9	10
	3н	3	4	5	6	7	8	9	10	11
	4н	4	5	6	7	8	9	10	11	12
	5н	5	6	7	8	9	10	11	12	13
	6н	6	7	8	9	10	11	12	13	14
	7н	7	8	9	10	11	12	13	14	15
	8н	8	9	10	11	12	13	14	15	16
	9н	9	10	11	12	13	14	15	16	17

С такими житейски понятными категориями оперировать гораздо проще, однако для проведения аналитических расчетов необходимо иметь количественное выражение показателей важности. Для обеспечения этих возможностей поступим следующим образом. Естественно предположить,

что важность информации категории А убывает от класса 3 к классу 1, приближаясь к 0, а категории Ж возрастает от класса 15 к классу 17, приближаясь к 1. Естественно также предположить, что возрастание важности информации от класса 1 к классу 17 происходит неравномерно; наиболее адекватной, видимо, будет зависимость в виде логистической кривой. Графически это можно представить так, как показано на рис. 7.2.

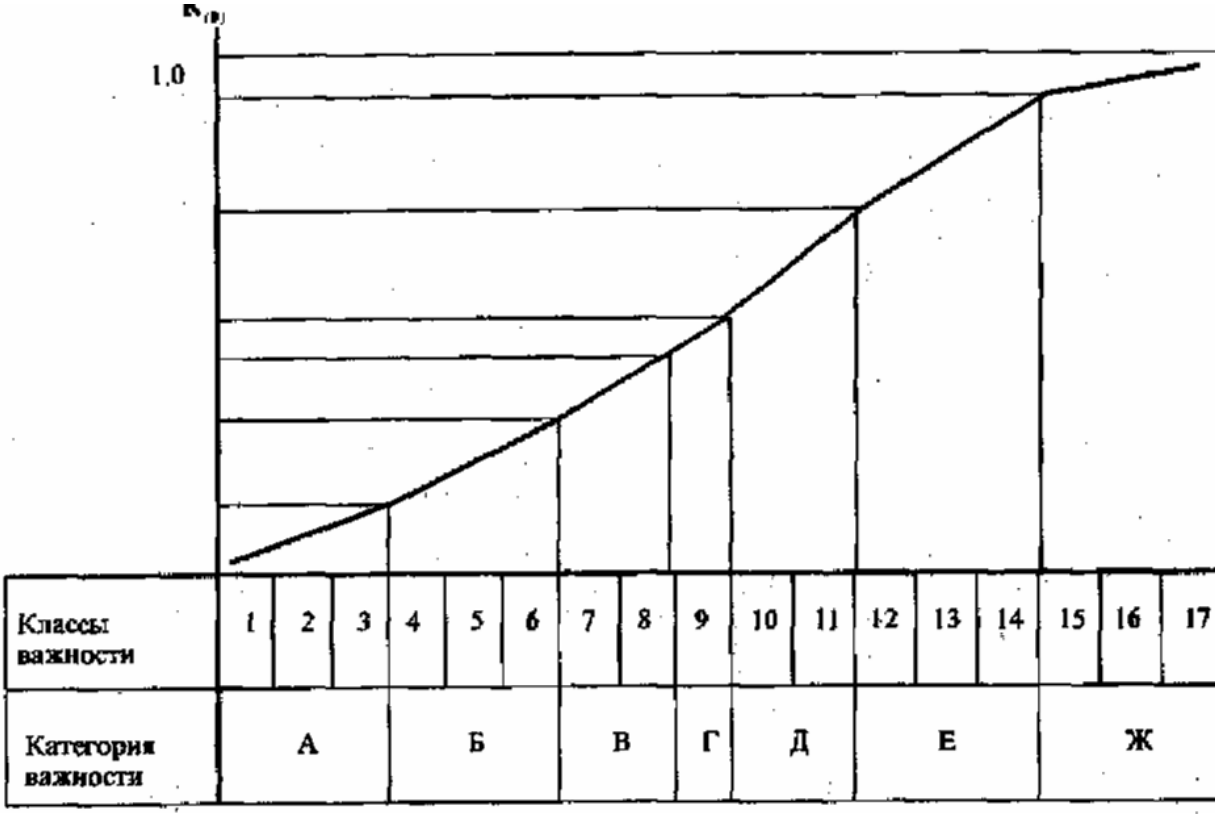

Рисунок 7.2- График коэффициента важности информации

Нетрудно видеть, что теперь мы имеем все необходимое для строго алгоритмического определения показателя важности информации, причем как в качественном, так и в количественном выражениях. Последовательность и содержание такой оценки приведены на рис. 7.3.

Рисунок 7.3. Последовательность и содержание оценки важности информации.

3. Оценка полноты и релевантности информации.

Полнота есть показатель, характеризующий меру достаточности информации для решения соответствующих задач. Отсюда следует, что данный показатель, так же как и предыдущий является относительным: полнота информации оценивается относительно вполне определенной задачи или группы задач. Поэтому, чтобы иметь возможность определять показатель полноты информации, необходимо для каждой задачи или группы задач заблаговременно составить перечень сведении, которые необходимы для их решения. Для представления таких сведений удобно воспользоваться так называемыми объектно-характеристическими таблицами (ОХТ), каждая из которых есть двухмерная матрица, по строкам которой приведен перечень наименовании объектов, процессов или явлений, которые входят в круг интересов соответствующей задачи, а по столбцам - наименования их характеристик (параметров), значения которых необходимы для решения задачи. Сами значения характеристик будут располагаться на пересечении соответствующих строк и столбцов. Совокупность всех ОХТ, необходимых для обеспечения решения всех задач предприятия (учреждения, другой организации), может быть названа информационным кадастром объекта. Таким образом, непременным условием оценки полноты информации является наличие информационного кадастра.

Методика оценки полноты может быть следующей.

Обозначим через $d_{\mu\nu}$ элемент, находящийся в μ-и строке и ν-м столбце рассматриваемого компонента соответствующей ОХТ, причем:

$$d_{\mu\nu} = \begin{cases} 1, \text{если по данному элементу информация имеется;} \\ 0, \text{в противном случае.} \end{cases}$$

Тогда в качестве меры коэффициента полноты информации в данной ОХТ можно принять величину:

$$K_{\Pi} = \frac{\sum_{\forall\mu}\sum_{\forall\nu} d_{\mu\nu}}{mn}, \qquad (7.4)$$

где m - число строк,

n - число столбцов в рассматриваемой ОХТ.

Однако при этом не учитывается важность, значимость различных элементов, причем важность в том смысле, как это рассматривалось выше. Пусть

$K^{(в)}_{\mu\nu}$ есть коэффициент важности элемента μ-й строки и ν-го столбца.

Тогда, очевидно, в качестве меры взвешенной полноты информации в рассматриваемой ОХТ можно принять величину:

$$K_{\Pi}^{(в)} = \frac{\sum_{\forall \mu} \sum_{\forall v} d_{\mu v} K_{\mu v}^{(в)}}{mn \sum_{\forall \mu} \sum_{\forall v} K_{\mu v}^{(в)}} \qquad (7.5)$$

Релевантность есть такой показатель информации, который характеризует соответствие ее потребностям решаемой задачи. Для количественного выражения данного показателя обычно используют так называемый коэффициент релевантности $K^{(p)}$ определяющий отношение объема релевантной информации N_p к общему объему анализируемой информации N_0:

$$K^{(p)} = \frac{N_p}{N_0} \qquad (7.6)$$

Сущность коэффициента релевантности очевидна, но трудности практическое его использования сопряжены количественным выражением объема информации. В сфере научно-технической информации под N_0, например, понимается общее количество документов, выданных на запрос, а под N_p - количество релевантных среди общего объема.

К оценке релевантности фактографической информации можно подойти следующим образом. Пусть имеется информационный кадастр, состоящий из некоторого количества ОХТ. Тогда релевантность η-й ОХТ можно выразить формулой:

$$K_{\eta}^{(p)} = \frac{\sum_{\forall \mu} \sum_{\forall v} d_{\mu v \eta}^{(p)}}{m_{\eta} n_{\eta}}, \qquad (7.7)$$

где

$$d_{\mu v \eta}^{(p)} = \begin{cases} 1, \text{если } d_{\mu v} \ \eta\text{-й ОХТ соответствует решаемой задаче;} \\ 0, \text{в противном случае.} \end{cases}$$

или с учетом коэффициентов важности элементов ОХТ:

$$K_{\eta}^{(p)} = \frac{\sum\limits_{\forall\mu}\sum\limits_{\forall\nu} d_{\mu\nu\eta}^{(p)} K_{\mu\nu\eta}^{(в)}}{m_{\eta} n_{\eta} \sum\limits_{\forall\mu}\sum\limits_{\forall\nu} K_{\mu\nu\eta}^{(в)}} \tag{7.8}$$

Коэффициент релевантности всего информационного кадастра, очевидно, может быть выражен формулой:

$$K_{\eta}^{(p)} = \frac{\sum\limits_{\forall\eta}\sum\limits_{\forall\mu}\sum\limits_{\forall\nu} d_{\mu\nu\eta}^{(p)} K_{\mu\nu\eta}^{(в)}}{\sum\limits_{\forall\mu} m_{\eta} n_{\eta}} \tag{7.9}$$

или с учетом коэффициентов важности элементов ОХТ:

$$K^{(p)} = \frac{\sum\limits_{\forall\eta}\sum\limits_{\forall\mu}\sum\limits_{\forall\nu} d_{\mu\nu\eta}^{(p)} K_{\mu\nu\eta}^{(в)}}{\sum\limits_{\forall\eta} m_{\eta} n_{\eta} \sum\limits_{\forall\mu}\sum\limits_{\forall\nu} K_{\mu\nu\eta}^{(в)}} \tag{7.10}$$

2.3 Методы оценки параметров защищаемой информации.

План лекции.

1. Оценка адекватности информации.
2. Оценка толерантности, эффективности кодирования и объема информации.

1. Оценка адекватности информации.

Под адекватностью информации понимается степень ее соответствия действительному состоянию тех реалий, которые отображает оцениваемая информация. В общем случае адекватность определяется двумя параметрами: объективностью генерирования информации о предмете, процессе или явлении и продолжительностью интервала времени между моментом генерирования информации и текущим моментом, т.е. до момента оценивания ее адекватности.

Объективность генерирования информации, очевидно, зависит от способа получения значений характеристик предмета, процесса или явления и качества реализации способа в процессе получения этих значений.

Классификация характеристик по возможным способам получения их значений приведена на рис. 8.1 Тогда все возможные значения адекватности информации по объективности ее генерирования можно структурировать так, как приведено в табл. 8.1.

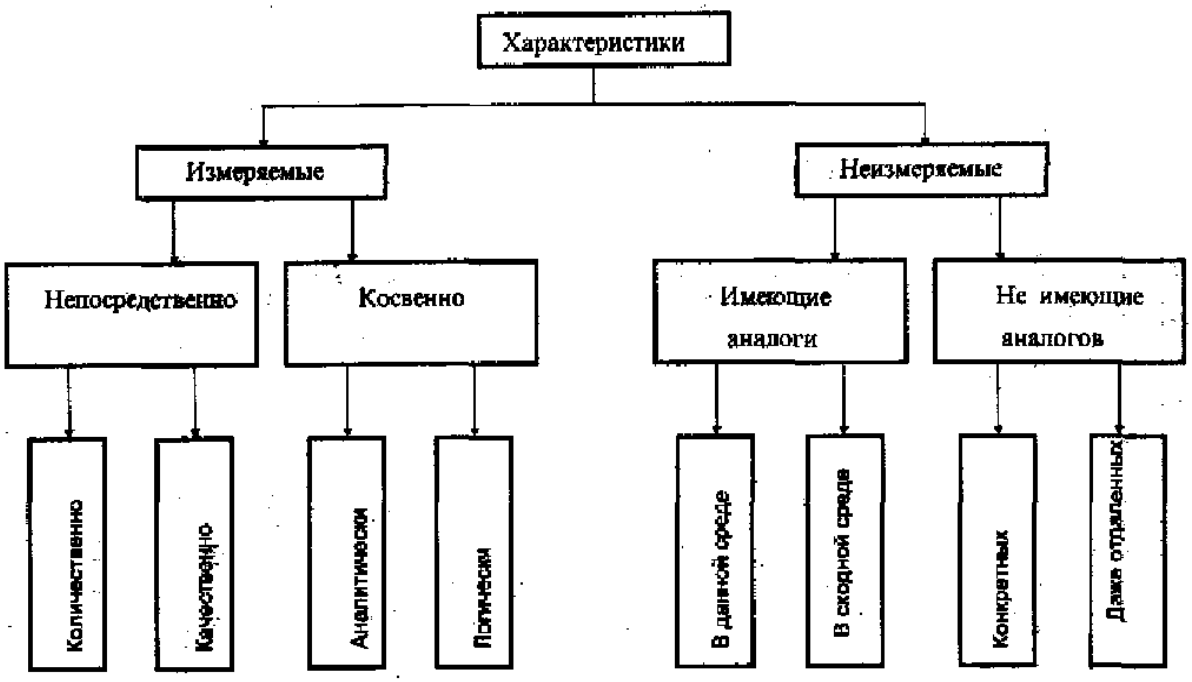

Рисунок. 8.1 - Классификация характеристик по способам получения их значений

Таблица 8.1 - Структуризация значений адекватности информации по объективности генерирования

Тип характеристики			Качество определения значения характеристики		
			Хорошее	Среднее	Плохое
Измеримая	Непосредственно	Количественно	1	2	3
		Качественно	2	3	4
	Косвенно	Аналитически	3	4	5
		Логически	4	5	6
Неизмеримая	Имеющая аналоги	В данной среде	5	6	7
		В исходной среде	6	7	8
	Не имеющая аналогов	Конкретного	7	8	9
		Даже отдаленного	8	9	10

Как и при разработке методики оценки важности информации сделаем естественное предположение, что при хорошем качестве определения значения непосредственно и притом количественно измеряемой характеристики адекватность соответствующей информации будет близка к 1, а при плохом определении значения неизмеряемой характеристики, не имеющей даже отдаленного аналога, адекватность информации близка к нулю. Естественно также предположить, что внутри данного интервала изменение адекватности происходит по логистической кривой, как это показано на рис. 8.2.

Рассмотрим теперь адекватность информации по второму названном выше параметру - продолжительности интервала времени между моментом генерирования информации и текущим моментом. Для оценки адекватности по данному параметру вполне подходящим является известный в теории информации так называемый **закон старения информации.** Его вид показан на рис. 8.3. При этом под $\mathbf{t_0}$ понимается момент времени генерирования оцениваемой информации. Как следует из рисунка, закон старения информации характеризуется четырьмя характерными интервалами:

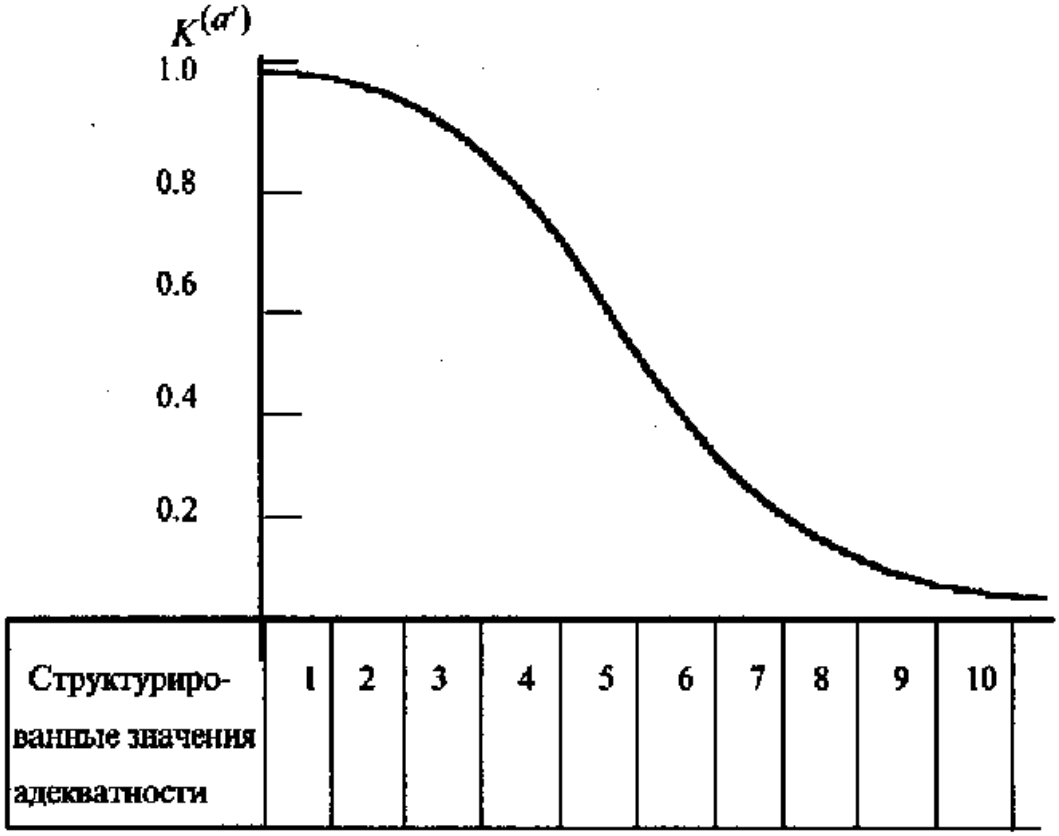

Рисунок 8.2 - График зависимости показателя адекватности информации по способу генерирования

Δt_1 -продолжительность интервала времени, в течение которого оцениваемая информация полностью сохраняет свою адекватность;

Δt_2 -продолжительность интервала времени, в течение которого адекватность информации падает, но не более, чем на одну четверть;

Δt_3 - продолжительность интервала времени, в течение которого адекватность информации падает наполовину;

Δt_4 - продолжительность интервала времени, в течение которого адекватность информации падает на три четверти;

Учитывая то обстоятельство, что обе составляющие адекватности информации $K^{(a')}$ и $K^{(a'')}$ зависят от большого числа факторов, многие из которых носят случайный характер, есть основания утверждать, что они в основе своей также имеют случайный характер и поэтому могут интерпретироваться как вероятности того, что информация по соответствующему параметру является адекватной. Поскольку для подавляющего большинства теоретических интересов и практических приложений важно, чтобы информация была адекватна по обоим параметрам, то в соответствии с теоремой умножения вероятностей общий показатель адекватности информации $K^{(a)}$ может быть определен как:

$$K^{(a)} = K^{(a')} K^{(a'')} \qquad (8.1)$$

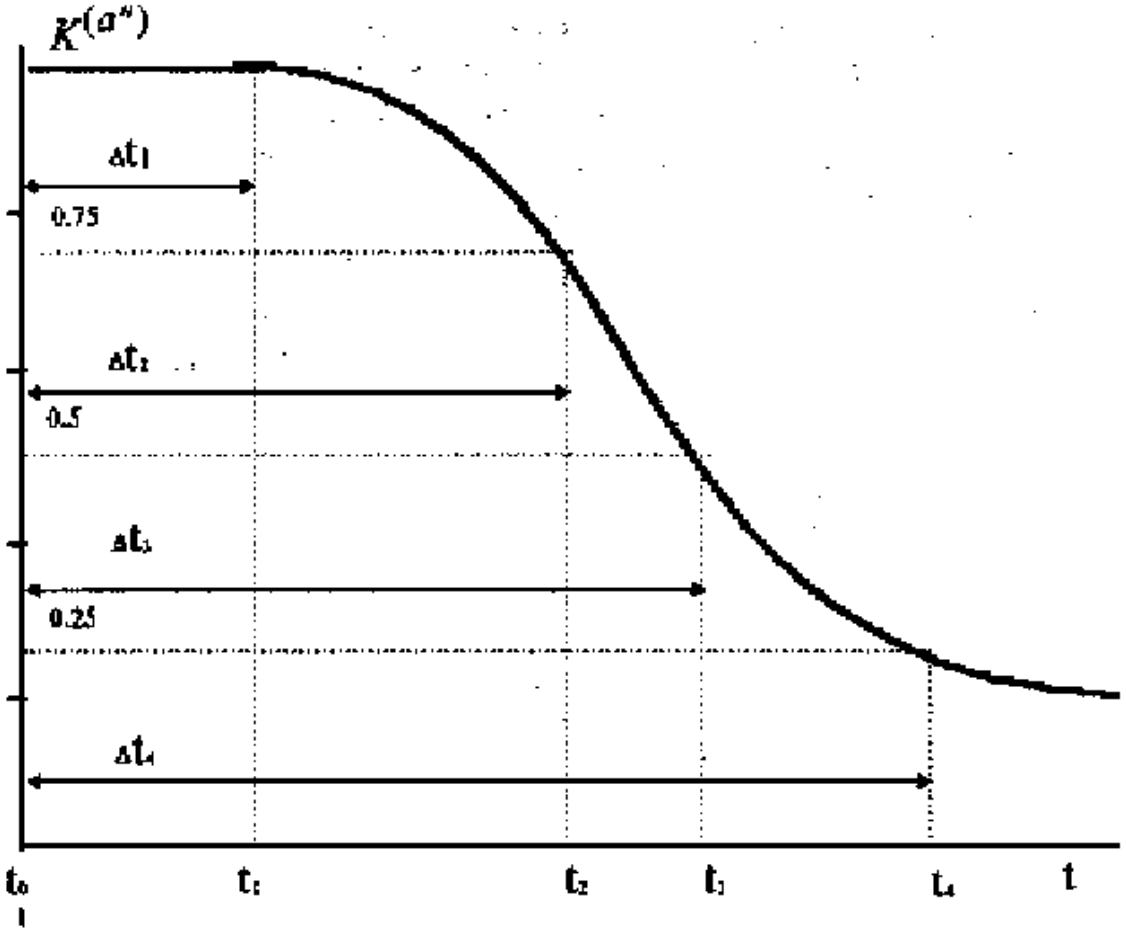

Рисунок 8.3 - Общий вид закона старения информации

Независимость величин $K^{(a')}$ и $K^{(a'')}$ представляется вполне естественной.

2. Оценка толерантности, эффективности кодирования и объема информации.

Толерантность, как отмечалось выше, есть показатель, характеризующий удобство восприятия и использования информации в процессе решения задачи. Уже из самого определения видно, что понятие толерантности является очень широким, в значительной мере неопределенным и субъективный. Даже для цифровой информации значение толерантности может быть самым различным. Поэтому вряд ли можно надеяться на разработку строго формальной методики определения толерантности. Из эвристических методов наиболее подходящими здесь

представляются неформально-эвристические и особенно - методы экпертно-лингвистических оценок. При этом в качестве значений лингвистической переменной могут быть такие:

1) **весьма удобно, комфортно** - когда информация представлена в таком виде, что ее использование в процессе решения задачи происходит естественным образом, не требуя дополнительных усилий;

2) **удобно** - когда использование информации если и требует дополнительных усилий, то лишь незначительных;

3) **средне** - когда использование информации требует дополнительных усилий, вообще говоря, допустимых;

4) **плохо** - когда использование информации сопряжено с большими трудностями;

5) **очень плохо** - когда использование информации или вообще невозможно, или требует неоправданно больших усилий.

Показатели второго вида. Как определено выше, основными показателями второго вида являются эффективность кодирования и объем информации. Поскольку методы определения названных показателей достаточно полно разработаны в теории информации, то специально на них останавливаться нет необходимости.

Требуемый уровень защиты информации должен определяться с учетом значений всех рассмотренных выше показателей. Методика такого определения может базироваться на следующей полуэвристической процедуре:

1) все показатели информации делятся на три категории: определяющие, существенные и второстепенные, причем основным критерием для такого деления должна служить та цель, для достижения которой осуществляется защита информации в соответствующей АСОД;

2) требуемый уровень защиты определяется по значениям определяющих показателей информации;

3) выбранный уровень при необходимости может быть скорректирован с учетом значения существенных показателей. Значения второстепенных показателей при этом могут игнорироваться.

Возможный вариант классификации показателей информации в зависимости от целей защиты приведен в табл. 8.2.

Таблица 8.2 - Классификация значений показателей информации в зависимости от целей защиты.

Показатель информации	Вид сохраняемой тайн			Защита информации как товар
	Военной, государственной, научной	Промышленной, коммерческой	Конфиденциальной	
Важность	Определяющее	Определяющее	Определяющее	Определяющ
Полнота	Существенное	Существенное	Определяющее	Определяющ
Адекватность	Существенное	Существенное	Существенное	Определяющ
Релевантность	Второстепенное	Существенное	Существенное	Существенно
Толерантность	Второстепенное	Второстепенное	Второстепенное	Существенно
Способ кодирования	Второстепенное	Второстепенное	Второстепенное	Существенно
Объем	Второстепенное	Существенное	Существенное	Определяющ