# Оценка уязвимости и рисков


### *В этой главе*

- *Анализрисков*
- *Разработкаметодологииоценкириска*
- *Оценка ущерба, связанная с реализацией угроз*
- *Анализстоимость/эффективность*
- *Группаоценкириска*
- *Элементыуправлениярис ком*

| <<< Этапы | Направления >>> | 010 | | | | 020 | | | | 030 | | | | 040 | | | | 050 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Защита объектов ИС | | | | Защита процессов и программ | | | | Защита каналов связи | | | | ПЭ МИ Н | | | | Управление системой защиты | | | |
| | Основы >>> | База | Структура | Меры | Средства | База | Структура | Меры | Средства | База | Структура | Меры | Средства | База | Структура | Меры | Средства | База | Структура | Меры | Средства |
| | | 011 | 012 | 013 | 014 | 021 | 022 | 023 | 024 | 031 | 032 | 033 | 034 | 041 | 042 | 043 | 044 | 051 | 052 | 053 | 054 |
| 100 | Определение информации, подлежащей защите | 111 | 112 | 113 | 114 | 121 | 122 | 123 | 124 | 131 | 132 | 133 | 134 | 141 | 142 | 143 | 144 | 151 | 152 | 153 | 154 |
| 200 | Выявление угроз и каналов утечки информации | 211 | 212 | 213 | 214 | 221 | 222 | 223 | 224 | 231 | 232 | 233 | 234 | 241 | 242 | 243 | 244 | 251 | 252 | 253 | 254 |
| 300 | Проведение оценки уязвимости и рисков | 311 | 312 | 313 | 314 | 321 | 322 | 323 | 324 | 331 | 332 | 333 | 334 | 341 | 342 | 343 | 344 | 351 | 352 | 353 | 354 |
| 400 | Определение требований к СЗИ | 411 | 412 | 413 | 414 | 421 | 422 | 423 | 424 | 431 | 432 | 433 | 434 | 441 | 442 | 443 | 444 | 451 | 452 | 453 | 454 |
| 500 | Осуществление выбора средств защиты | 511 | 512 | 513 | 514 | 521 | 522 | 523 | 524 | 531 | 532 | 533 | 534 | 541 | 542 | 543 | 544 | 551 | 552 | 553 | 554 |
| 600 | Внедрение и использование выбранных мер и средств | 611 | 612 | 613 | 614 | 621 | 622 | 623 | 624 | 631 | 632 | 633 | 634 | 641 | 642 | 643 | 644 | 651 | 652 | 653 | 654 |
| 700 | Контроль целостности и управление защитой | 711 | 712 | 713 | 714 | 721 | 722 | 723 | 724 | 731 | 732 | 733 | 734 | 741 | 742 | 743 | 744 | 751 | 752 | 753 | 754 |

Для определения соответствующих мер защиты ИС следует использовать системный подход. Решение, как обеспечить защиту, где реализовать защиту в ИС, какими должны быть типы и качество мер и средств защиты, требует проведения соответствующего анализа уязвимости и рисков.

***Процесс анализа рисков включает:***

- оценку возможных потерь из-за использования или зависимости от технологии автоматизированной информационной системы,
- анализ потенциальных угроз и уязвимых мест системы, влияющих на оценки возможных потерь,
- выбор оптимальных по цене мер и средств защиты, которые сокращают риск до приемлемого уровня.

Следует отметить, что с учетом системного подхода, предлагаемого в книге, ***этап проведения оценки уязвимости и рисков (300) проводится по НАПРАВЛЕНИЯМ:***

- для объектов ИС (310),
- для процессов, процедур и программ обработки информации (320),
- для каналов связи (330),
- для побочных электромагнитных излучений (340),
- для механизмов управление системой защиты (350).

Кроме того, ***результаты, полученные от оценки уязвимости и рисков, должны быть отражены в ОСНОВАХ:***

- БАЗА (001),
- СТРУКТУРА (002),
- МЕРЫ (ПОЛИТИКА) (003),
- СРЕДСТВА (004).

Следует учесть, что если методика анализа и не позволяет сделать вывод о величине реального риска при использовании ИС, то она не поможет и в создании эффективной защиты ИС. Необходимо использовать такой подход для оценки риска, который бы обеспечивал достаточную точность и применение в простой и понятной форме.

## Анализ рисков (300)

Анализ рисков предполагает изучение и систематизацию угроз ЗИ, а также определение требований к средствам защиты.

***Изучение и систематизация угроз ЗИ предусматривает следующие этапы:***

- выбор объектов ИС и информационных ресурсов, для которых будет проведен анализ;
- разработка методологии оценки риска;
- анализ угроз и определение слабых мест в защите;
- идентификация угроз и формирование списка угроз;
- формирование детального списка угроз и матрицы угрозы/элементы ИС или информационные ресурсы.

Для построения надежной защиты необходимо выявить возможные угрозы безопасности информации, оценить их последствия, определить необходимые меры и средства защиты и оценить их эффективность.

Поскольку анализ всей информационной инфраструктуры (особенно для крупных объектов) далеко не всегда оправдан с экономической точки зрения, в ряде случаев целесообразно сосредоточиться на наиболее важных, учитывая приближенность итоговой оценки. С этих же позиций следует оценивать возможные угрозы и их последствия.

Разнообразие потенциальных угроз столь велико, что все равно не позволяет предусмотреть каждую из них, поэтому анализируемые виды уместно выбирать с позиций здравого смысла, одновременно выявляя не только собственно угрозы, вероятность их осуществления, масштаб потенциального ущерба, но и их источники.


*Разнообразие угроз столь велико...*

Оценка рисков производится с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящие потенциальную угрозу в разряд реально опасных и, следовательно, требующие принятия дополнительных защитных мер.

Как правило, существует несколько решений по нейтрализации каждой. При оценке их стоимости и эффективности следует учитывать не только расходы на закупку оборудования и программных средств, но и возможность экранирования одним сервисом безопасности нескольких прикладных, его совместимость

с аппаратно-программной структурой организации, стоимость обучения персонала для работы с ним.

Когда намеченные меры приняты, необходимо проверить их действенность, например произвести автономное и комплексное тестирование программно-технического механизма защиты. Если проверка показывает, что в результате проделанной работы остаточные риски снизились до приемлемого уровня, то можно намечать дату ближайшей переоценки, если нет — следует проанализировать допущенные ошибки и провести повторную оценку рисков.

Защита ИС должна учитывать интересы и потребности организации в целом. Эта цель может быть достигнута только тогда, когда в решении задачи участвуют представители соответствующих отделов организации. Такой список включает участников анализа риска компьютерных систем и приложений.

## Разработка методологии оценки риска (301)

Должны быть получены оценки предельно допустимого и существующего риска осуществления угрозы в течение некоторого времени. В идеале для каждой из угроз должно быть получено значение вероятности ее осуществления в течении некоторого времени. Это поможет соотнести оценку возможного ущерба с затратами на защиту. На практике для большинства угроз невозможно получить достоверные данные о вероятности реализации угрозы и приходится ограничиваться качественными оценками. При разработке методологии оценки риска могут быть использованы методы системного анализа.

## Оценка ущерба, связанная с реализацией угроз (300)

Производится оценка ущерба, который может нанести деятельности организации реализация угроз безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации.

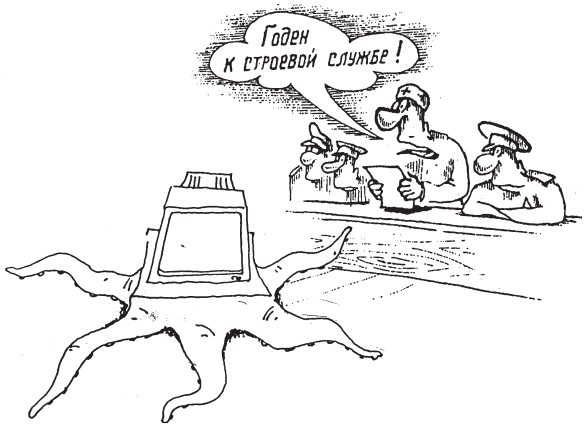
Оценка затрат на мероприятия, связанные с защитой и остаточного риска.

Производится предварительная оценка прямых затрат по каждому мероприятию без учета затрат на мероприятия, носящие комплексный характер.

## Анализ стоимость/эффективность (301)

Расходы на систему защиты информации необходимо соотнести с ценностью защищаемой информации и других информационных ресурсов, подвергающихся риску, а также с ущербом, который может быть нанесен организации в результате реализации угроз. По завершении анализа уточняются допустимые остаточные риски и расходы по мероприятиям, связанным с защитой информации.

## Итоговый документ (301)




*Группа оценки риска...*

***По результатам проведенной работы составляется документ, содержащий:***

- перечни угроз ЗИ, оценки рисков и рекомендации по снижению вероятности их возникновения;
- защитные меры, необходимые для нейтрализации угроз;
- анализ стоимость/эффективность, на основании которого делаются выводы о допустимых уровнях остаточного риска и целесообразности применения конкретных вариантов защиты.

## Группа оценки риска (302)

Группа оценки риска может состоять из такого числа участников, которое позволяло бы учесть все разнообразие требований и указаний, регламентирующее порядок использования ИС. Такую группу целесообразно иметь в следующем составе:

- **Администраторы ИС** несут ответственность за функционирование ИС. Они могут обеспечить группу оценки риска информацией о корректных параметрах конфигурации ИС, включая аппаратные средства ЭВМ, программное обеспечение, данные, и распределение функций ИС по ее компонентам. Администраторы ИС могут также указать непосредственные воздействия, которые могут произойти, если угроза будет реализована.
- **Руководство организацией** ответственно за поддержку политики безопасности ИС, обеспечивая финансирование требуемых служб безопасности и разрабатывая документы, гарантирующие достижение целей политики безопасности. Руководство организацией

ответственно за правильную оценку долгосрочных последствий реализации угрозы.

- **Сотрудники службы безопасности** ответственны за разработку политик безопасности организации и их соблюдение.
- **Владельцы данных и приложений** обязаны гарантировать, что их данные и приложения адекватно защищены и доступны уполномоченным пользователям.
- **Пользователи ИС** обязаны предоставлять точную информацию об используемых ими приложениях, данных и ресурсах ИС.

Конечная цель эффективной защиты ИС не может быть достигнута, если изначально в группе не будет сильного лидера.

## Элементы управления риском (353)

Термин *управление риском* обычно используется для обозначения процесса определения риска, применения средств защиты для сокращения риска и затем определения, приемлем ли остаточный риск.

*Определение*

***Проблемы, которые должны быть решены при оценке защищенности ИС, включают:***

1. ***Ценности*** — Что должно быть защищено?
2. ***Угрозы*** — От чего необходимо защищать ценности и какова вероятность реализации угрозы?
3. ***Воздействия*** — Каковы будут непосредственные разрушения после реализации угрозы (например, раскрытие информации, модификация данных)?
4. ***Последствия*** — Каковы будут долгосрочные результаты реализации угрозы (ущерб репутации организации, потеря бизнеса)?
5. ***Меры защиты*** — Какие эффективные меры защиты (службы безопасности и механизмы) требуются для защиты ценностей?
6. ***Риск*** — После реализации мер защиты приемлем ли остаточный риск?

***Цель оценки риска*** состоит в том, чтобы определить риск для ИС. Процесс оценки риска проводится в два шага. На первом — определяют границы ИС для анализа, требуемую степень детализации описания ИС при оценке и методологию, которая будет использоваться. На втором — проводится анализ риска. Анализ риска может быть разбит на идентификацию ценностей, угроз и уязвимых мест, оценку вероятностей и измерение риска.

***Цель минимизации риска*** состоит в том, чтобы применить эффективные меры защиты таким образом, чтобы остаточный риск в ИС стал приемлем. Минимизация риска состоит из трех частей: определения тех областей, где риск недопустимо велик; выбора наиболее эффективных средств защиты; оценивания мер защиты и определения, приемлем ли остаточный риск в ИС.

***Процесс управления риском включает следующие этапы:***

1. Определение степени детализации, границ анализа и методологии.
2. Идентификация и оценка ценностей.
3. Идентификация угроз и определение вероятности.
4. Измерение риска.
5. Выбор соответствующих средств защиты.
6. Внедрение и испытания средств защиты.
7. Проверка остаточного риска.

### Этап 1 — Определение степени детализации (311)

На этом этапе определяется какие информационные и технические ресурсы из состава ИС и с какой детальностью должно рассматриваться в процессе управления риском. Перечень может включать ИС в целом или ее части, такие, как функции коммуникаций данных, функции сервера, приложения, и т.д.

Степень детализации можно представлять как сложность созданной логической модели всей ИС или ее частей, отражающую глубину процесса управления риском. Степень детализации будет отличаться для разных областей ИС. Например, некоторые области могут рассматриваться поверхностно, в то время как другие — глубоко и детально.

### Этап 2 — Идентификация и оценка ценностей (302)

В ходе оценки ценностей выявляются и назначаются стоимости ресурсов ИС. Этот шаг позволяет выделить ресурсы, приоритетные с точки зрения организации защиты.

Ценности могут быть определены на основании воздействий и последствий для организации. Оценка рисков предполагает не только стоимость ресурсов, но и последствия в результате раскрытия, искажения, разрушения или порчи информационных и технических ресурсов ИС.

Стоимость ресурсов может быть представлена в терминах потенциальных потерь. Эти потери могут быть основаны на стоимости восстановления, потерях при

непосредственном воздействии и последствий. Одна из простейших методик оценки потерь для ценности состоит в использовании качественного ранжирования на высокие, средние и низкие потери.

Одним из косвенных результатов этого процесса является создание детальной конфигурации ИС и функциональной схемы ее использования. Эта конфигурация должна описывать подключенные аппаратные средства ИС, главные используемые приложения, важную информацию, обрабатываемую в ИС, а также способ передачи этой информации через ИС. Степень знания конфигурации ИС будет зависеть от степени детализации.

***Конфигурация аппаратных средств содержит*:**

серверы,

автоматизированные рабочие места,

ПК,

периферийные устройства,

соединения с глобальными сетями,

схему кабельной системы,

соединения с мостами или шлюзами и т.д..

***Конфигурация программного обеспечения включает в себя*:**

операционные системы серверов,

операционные системы автоматизированных рабочих мест

операционные системы ПК,

операционную систему ИС,

главное прикладное программное обеспечение,

инструментальное программное обеспечение,

средства управления ИС,

разрабатываемое программное обеспечение,

местоположение программного обеспечения в ИС.

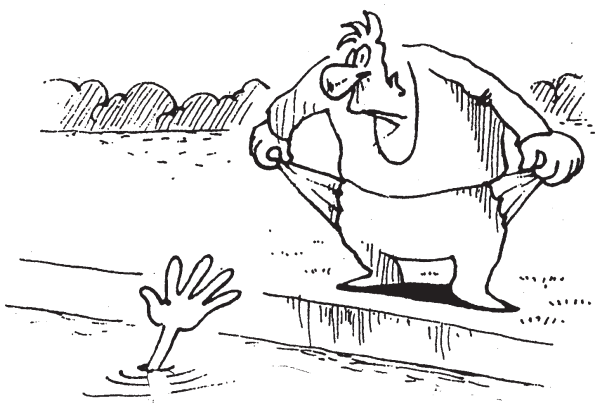
После того, как описание конфигурации ИС закончено и ценности определены, появится представление о том, из чего состоит ИС и какие ресурсы необходимо защищать в первую очередь.

## Этап 3 – Идентификация угроз и определение их вероятности (204)

На этом этапе должны быть выявлены угрозы и уязвимые места, определены вероятности реализации угроз.

Список угроз следует рассматривать в зависимости от степени детализации описания ИС. Концептуальный анализ может указать на абстрактные угрозы и уязвимые места. Более детальный анализ может связать угрозу с конкретной компонентой ИС.

Следует учитывать, что абстрактность угроз, выявленных в результате концептуального анализа, в конечном счете приведет к тому, что и рекомендации относительно средств защиты также будут абстрактными. Это приемлемо при проведении общей оценки риска. Более детальная оценка риска даст рекомендации относительно средства защиты, которое должно уменьшить конкретный риск.



*Идентификакия и оценка ценностей...*

***Угрозы и уязвимые места подробно описаны в главе 8.*** Они могут использоваться как отправная точка при анализе угроз и каналов утечки информации. Любая ценность в ИС, которая была определена как достаточно важная, должна быть исследована, чтобы можно было выявить потенциальные угрозы. Особое внимание должно быть уделено детализации путей, с помощью которых эти угрозы могут быть реализованы.

Существующие средства и меры защиты в ИС должны быть проанализированы, чтобы можно было определить, обеспечивают ли они адекватную защиту, в противном случае это может рассматриваться как уязвимое место. После того, как определенные угрозы и связанные с ними уязвимые места с каждой парой угроза/уязвимое место должна быть связана вероятность того, что эта угроза будет реализована.

## Этап 4 – Измерение риска (301)

В широком смысле мера риска может рассматриваться как описание видов неблагоприятных действий, влиянию которых может подвергнуться система и вероятностей того, что эти действия могут произойти. Результат этого процесса должен определить степень риска для определенных ценностей. Этот результат важен, поскольку является основой для выбора средств защиты и решений по минимизации риска.

Мера риска может быть представлена в качественных, количественных, одномерных или многомерных терминах.

***Количественные*** подходы связаны с измерением риска в терминах денежных потерь.

***Качественные*** — с измерением риска в качественных терминах, заданных с помощью шкалы или ранжирования.

***Одномерные*** — рассматривают только ограниченные компоненты (риск = величина потери * частота потери).

***Многомерные*** подходы рассматривают дополнительные компоненты в измерении риска, такие, как надежность, безопасность или производительность.

Одним из наиболее важных аспектов меры риска является то, что ее представление должно быть понятным и логичным для тех, кто выбирает средства защиты и решает вопросы минимизации риска.

## Этап 5 – Выбор мер и средств защиты (504)

Цель этого процесса состоит в выборе соответствующих мер и средств защиты. Этот процесс может быть выполнен с использованием проверки приемлемости риска.

*Это важно*

Проверка приемлемости риска рассматривается как деятельность, которая сравнивает текущую меру риска с критериями приемлемости и приводит к определению того, приемлем ли текущий уровень риска. В то время как эффективность защиты и финансовые соображения являются важными факторами, при принятии решения могут быть учтены другие факторы: политика организации, законодательство и уставы, безопасность и требования надежности, требования производительности и технические требования.

Взаимосвязь между проверкой приемлемости риска и выбором средств защиты может быть итеративной. Первоначально организация должна упорядочить уровни рисков, определенные в ходе оценки риска. Наряду с этим, организация должна принять решение о количестве остаточного риска, который желательно принять после того, как выбранные меры и средства защиты будут установлены.

Эти начальные решения по принятию риска могут внести поправки в уравнение выбора средств защиты. Когда свойства предлагаемых мер и средств защиты известны, можно повторно провести проверку приемлемости риска и определить, достигнут ли уровень остаточного риска или необходимо изменить решения относительно его приемлемости, чтобы отразить информацию о свойствах предлагаемых средств защиты.

Отбор соответствующих средств защиты является также субъективным процессом. При рассмотрении меры стоимости механизма важно, чтобы стоимость средства защиты была связана с мерой риска при определении рентабельности средства защиты.

Для вычисления отношения риск / стоимость используют меру риска и финансовую меру, связанную с каждым отношением угроза / механизм и рассчитывают отношение риска к стоимости (т.е., риск / стоимость). Отношение меньше единицы будет указывать, что стоимость механизма больше, чем риск, связанный с угрозой. Это вообще не приемлемая ситуация, но она не должна автоматически отклоняться. Предположим, что величина риска — функция меры потери и меры вероятности. Один или оба этих аргумента могут быть настолько критичны относительно ценности, что дорогостоящий механизм защиты будет оправдан.

## Этап 6 – Внедрение и тестирование средств защиты (604)

Внедрение и тестирование средств защиты должно быть выполнено структурированным способом. Цель этого процесса состоит в том, чтобы гарантировать правильность реализации средств защиты, совместимость с другими функциональными возможностями ИС и средствами защиты, и обеспечивают ожидаемую защиту.

Этот процесс начинается разработкой плана внедрения средств защиты. Этот план должен учитывать факторы, такие как доступный объем финансирования, уровень подготовки пользователей и т.д. График испытаний для каждого средства защиты также должен быть включен в этот план. График должен показывать, как каждое средство защиты взаимодействует или влияет на другие средства защиты (или функциональные возможности ИС). Ожидаемые результаты (или предположение об отсутствии конфликта) взаимодействия должны быть детализированы. Важно не только то, что средство защиты исполняет свои функции как ожидается и обеспечивают требуемую защиту, но и что средство защиты не увеличивает риск ИС из-за конфликта с другим средством защиты или функциональной возможностью.

***Каждое средство должно быть проверено независимо от других средств, чтобы гарантировать обеспечение ожидаемой защиты***. Однако это может оказаться неуместным, если средство предназначено для совместной работы с другими средствами. После независимого испытания средство должно быть проверено совместно с другими средствами, чтобы гарантировать, что оно не нарушает нормального функционирования существующих средств. План внедрения должен учесть все эти испытания и отразить проблемы или специальные условия, возникшие в результате испытания.

### Этап 7 – Одобрение остаточного риска (301)

После того, как все средства защиты реализованы, проверены и найдены приемлемыми, результаты проверки приемлемости риска должны быть повторно изучены. Риск, связанный с отношениями угроза/уязвимое место, должен теперь быть сокращен до приемлемого уровня или устранен. Если эти условия не соблюдены, то решения, принятые на предыдущих шагах, должны быть пересмотрены, чтобы определить, каковы должны быть надлежащие меры защиты.

## Методики оценки потенциально возможных угроз ИС (301)

Теоретические исследования и практический опыт защиты информации показывают, что определение точных количественных данных возможного ущерба, как правило, не представляется возможным. Поэтому широкое распространение получили приближенные оценки, основанные на обработке данных, собранных в процессе функционирования ИС и просто в процессе наблюдения над соответствующими явлениями, а также на экспертных оценках.

Краткий обзор таких методик и некоторые выводы по их использованию приведены в табл. 12.1.

### Оценка ущерба от угроз безопасности информации (301)

Одним из целесообразных вариантов определения эффективности мер ЗИ является методика, в основу которой положена процедура оценки ущерба от угроз БИ.

***На этапе 1*** оценивается влияние угроз БИ на ТТХ аппаратных средств обработки информации. Результатом этого этапа является оценка относительного и абсолютного ухудшения временных, энергетических, частотных, надежностных и других показателей эффективности функционирования аппаратных средств под воздействием угроз БИ с учетом вероятности осуществления этих угроз.

*Исходные данные для этого этапа:*

- перечень угроз БИ с указанием вероятности их осуществления;
- перечень ТТХ средств и предельные значения их изменения.

Кроме того, необходимо иметь аналитические отношения, позволяющие оценивать влияние угроз на ТТХ средств, или методику натурных испытаний для получения экспериментальных данных, позволяющих получить эти зависимости.

На этом же этапе оценивается влияние угроз БИ на качество программных средств и качество исходной информации. Исходные данные, используемые для оценки, содержат перечень возможных угроз и показатели качества программных средств и информации. Учет влияния угроз может осуществляться, помимо перечисленных выше методов, экспертным путем, что особенно актуально при оценке влияния угроз на качество информации, так как получить аналитические зависимости на основе математического и натурного моделирования в этом случае достаточно сложно.

***На этапе 2*** производится оценка относительного снижения эффективности процесса обработки информации, вызванного ухудшением ТТХ аппаратных средств, качества программных средств, исходной и обрабатываемой информации.

Исходными данными для этого этапа являются выходные данные этапа 1 и допустимые значения показателя, выбранного для оценки эффективности процесса обработки информации. Для проведения оценки необходимо иметь модель процесса обработки и аналитические соотношения, связывающие показатель эффективности процесса обработки с показателем качества аппаратных, программных средств, исходной и обрабатываемой информации.

***На этапе 3*** производится оценка относительного снижения эффективности решаемых на ИС частных функциональных задач вследствие ухудшения эффективности обработки информации.

Для проведения оценки необходимо иметь перечень задач, решаемых на ИС, показатели их эффективности и аналитические соотношения, позволяющие учесть влияние эффективности процесса обработки на эффективность решаемых задач.

***На этапе 4*** производится оценка относительного снижения эффективности функционирования ИС в целом в зависимости от снижения эффективности решения частных задач на объектах ИС.

Для получения более наглядных оценок на каждом из этапов производится расчет потерь, связанных с воздействием угроз на эффективность функционирования элементов ИС и процесса обработки решаемых задач.

Для расчета потерь в результате снижения эффективности функционирования объектов ИС в целом необходимо учитывать внешнее окружение объектов ИС, т.е. их назначение и область использования.

### Модель военная – значит надежная (301)

По мнению специалистов Военной академии им. Ф.Э. Дзержинского Горбунова А.Л. и Чуменко В.Н., оценка эффективности системы защиты информации относится к задачам многокритериальной оценки, поскольку столь сложную систему невозможно полно охарактеризовать с помощью единственного показателя.

**Таблица 12.1. Некоторые методики оценки угроз.**

| Источник | Показатели, по которым производится оценка и выбор | Краткая характеристика методики расчета | Выводы |
|---|---|---|---|
| ЗРЭ № 12, 1989 г., стр. 117 | Вероятность невозможности обработки данных в результате пожара, наводнения...; потери входного массива данных, отдельных записей, их искажения, несанкционированного копирования | Результаты оценки представлены в виде шкалы оценок потенциальных угроз и их последствий. Значения показателей приближенные, основанные на анализе имеющейся статистики нарушений или на экспертных оценках | Методика не может быть использована для оценки эффективности и выбора мер ЗИ, т.к. для определения (назначения) значений показателя необходим значительный объем статистического материала и, следовательно, значительное время наблюдений |
| ЗРЭ № 12, 1989 г., стр. 118 | Ожидаемый ущерб от $i$-й угрозы $R_i$ | $R_i = 10\ (S + V - 4)$, где $S$ - показатель частоты возникновения угрозы, выбирается интервале от 0 до 7: 0 - соответствует случаю, когда угроза не возникает почти никогда, 7 - тысяча раз в год; $V$ - показатель ущерба, назначается в зависимости от $S$ и принимает значения от 1 до 1 млн. дол. | Оценка весьма приближенная, ей присущи все недостатки, указанные для предыдущей методики |
| ЗРЭ № 12, 1989 г., стр. 118. Методики экспертного оценивания системы БИ | Степень обеспечения безопасности $SR$ системы $S$ | $SR_{(S,r)} = 1/n \sum_{i=1}^{n} W_i G_i$, где $W_i$ - субъективный коэффициент важности $i$-й характеристики СЗИ; $G_i$ - назначенное экспертным путем значение каждой из характеристик; $n$ - количество характеристик | Метод позволяет получить приближенную оценку эффективности системы ЗИ. Может быть использован при отсутствии необходимых исходных данных для более точной и достоверной оценки, для оценки эффективности и выбора системы ЗИ из нескольких альтернатив |
| ЗРЭ № 12, 1989 г., стр. 118. Аналитический метод оценки угроз и ущерба, вызванного ими | Для оценки угроз: $L$ - средний показатель появления анализа типа угроз (случайная величина с распределением вероятности $f(L)$). Для оценки ущерба: случайная величина $m$ со средним отклонением $v$ | $L$ - определяется на основе анализа статистики нарушений или экспертным путем; $m$ - аналогично | Для оценки ущерба необходимо иметь статистику нарушений БИ и измеренные значения ущерба в результате этих нарушений. Невозможно учесть влияние средств ЗИ на $L$ и соответственно $m$, а следовательно, и оценить эффективность мер ЗИ |

Поэтому для оценки эффективности необходимо использовать счетное множество показателей: W={Wi:i=1,n}, где n — количество показателей.

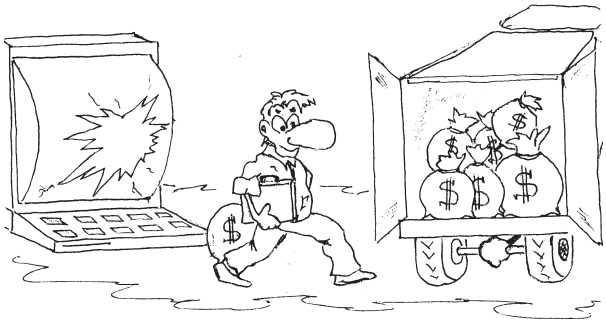
***Существуют два основных подхода к многокритериальной оценке эффективности сложных систем. Первый*** так или иначе связан со сведением множества частных показателей {Wi} к единственному интегральному показателю Wo.

***Второй*** — используется при наличии значительного числа частных показателей эффективности, приблизительно одинаково важных, и предполагает использование методов теории многокритериального выбора и принятия решений.

***Цель функционирования системы защиты информации*** — поддержание заданного уровня защищенности. Поэтому показатели эффективности должны характеризовать динамические свойства системы защиты информации и позволять оценивать ее как характеристики адаптивной системы.

Такими показателями могут быть: вероятность преодоление системы защиты информации **Pn** за время **Tn**, вероятность доставки единицы информации (например, пакета данных) от абонента к абоненту **Pд** за время **Tд** и аппаратурная сложность **S**. Значения **Pn**, **Tn**, **Pд** и **Tд** можно быть определить с помощью имитационного моделирования или аналитически. Показатель аппаратурной сложности **S** может быть определен, например, как количество типовых модулей в системе защиты информации.

Однако при анализе типов структур, различающихся, например, количеством и распределением механизмов защиты, получение аналитического выражения для показателя S практически невозможно. Это связано со



*Снижение эффективности процесса обработки информации...*

значительным различием типов механизмов защиты информации, со множеством способов их практической реализации и, следовательно, с невозможностью сведения их аппаратурной избыточности к общей единице измерения.

Поэтому целесообразно в этом случае рассматривать S как качественный показатель, а для его оценки использовать методы теории нечетких множеств. При этом количественные показатели Pn, Tn, Рд, Тд тоже можно рассматривать, как нечеткие при условии, что для них определены максимальные и минимальные допустимые значения. Функции принадлежности могут быть определены как: mP=(P-Pmin)/(Pmax-Pmin), mT=(1/T-1/Tmax)/(1/Tmin-1/Tmax).

Тогда ***задача выбора структуры и оптимизации системы защиты логически разбивается два этапа:***

- выбор структуры системы защиты информации;
- оптимизация системы защиты информации.

***На первом*** — методами теории нечетких многокритериальных задач оптимизации определяется множество Парето-оптимальных структур систем защиты информации. В общем случае множество Парето может быть как пустым, так и содержащим произвольное количество элементов. Существуют методы, позволяющие добиться, чтобы множество Парето было не пустым и содержало конечное число элементов. Среди определенного таким образом множества структур системы защиты выбирается в качестве базовой одна. Показатели эффективности на этом этапе — нечеткие.

***На втором*** этапе проводится синтез рациональной системы защиты информации в рамках выбранной на первом этапе структуры. Для этого известными методами теории численной оптимизации формируется состав протоколов, реализующих определенные на первом этапе службы и механизмы защиты информации, оптимизируется их распределение по уровням ИС.

Показатели эффективности Pn, Tn, Рд, Тд на этом этапе — четкие. Конкретная постановка задачи оптимизации определяется задаваемым уровнем защищенности информации в зависимости от условий функционирования. ***Можно предложить следующие постановки:***

- минимизировать значения вероятности преодоления механизмов защиты Pn с учетом ограничения на вероятность доставки пакета Рд за заданное время Тд;
- максимизировать Рд при заданных ограничениях на вероятность Pn за время Tn;
- найти F*=max F(Pn, Tn, Рд, Тд), где F — функция, осуществляющая свертку частных показателей эффективности Pn, Tn,

Синтезированная на втором этапе система защиты информации будет поддерживать заданный уровень защищенности. Когда СЗИ определит, что условия функционирования изменились, она выработает новое требуемое значение уровня защищенности, и оптимизация системы защиты будет проведена заново.

Таким образом, с помощью методов теории нечеткого многокритериального выбора решений и численных методов оптимизации можно синтезировать рациональную систему защиты информации, в которой обеспечивается поддержание необходимого уровня защищенности и достигаются заданные показатели по оперативности управления и аппаратурной сложности.

## Без ущерба для "здоровья" ИС (301)

Адекватная и физически ясная оценка эффективности СЗИ может быть получена, когда в качестве интегрального показателя используется величина ущерба (потерь) вследствие воздействия различных угроз. В этом случае можно сравнить реальную опасность угроз, последствия их воздействия и достигаемый уровень безопасности в ИС.

***Разработка методов и методик оценки эффективности и выбора мер ЗИ на объектах информатики по величине предотвращенного ущерба предполагает решение двух основных задач:***

- выбор и обоснование показателей эффективности мер ЗИ;
- выбор и разработка методов и методик расчета этих показателей.

Поскольку основным назначением мер ЗИ является предотвращение угроз информации, в качестве оценки эффективности этих мер можно выбрать показатели предотвращенного ущерба объектам ИС.

Для выбора показателей, характеризующих возможный ущерб от различных угроз информации, необходимо проанализировать механизм возникновения ущерба от этих угроз.

Ущерб от нарушения информации является следствием следующих событий:

*Определение*

- воздействия угроз на технические средства обработки информации;
- воздействия угроз посредством физических полей, создаваемых основными и вспомогательными техническими средствами обработки информации и людьми – носителями информации;
- воздействия угроз информации на людей – носителей информации и/или имеющих доступ к информации в процессе ее обработки.

Воздействие угроз на аппаратные средства ИС приводит к ухудшению качества их функционирования, которое может проявляться как ухудшение их тактико-технических характеристик (временных, точностных, энергетических, частотных и других в зависимости от типа средства).

Учитывая, что аппаратные средства представляют собой материальную основу процесса обработки информации в ИС, ухудшение их тактико-технических характеристик автоматически ведет к снижению эффективности процесса обработки информации.

В качестве интегрального показателя для оценки ущерба можно выбрать показатель "**стоимость потерь в результате нарушения информации**", который в общем случае является функцией от нескольких показателей более низкого уровня, зависящих от вида нарушения (нарушение целостности, доступности и/или конфиденциальности), а также от вида потерь, среди которых можно выделить:

- затраты на восстановление аппаратных, программных средств и качества информации;
- потери в результате снижения эффективности функционирования объекта ИС.

Более конкретное содержание показателей ущерба на этом уровне зависит от конкретных условий, т.е. от того, какие показатели выбраны для оценки эффективности функционирования ИС.

Например, для ИС, в зависимости от их назначения, в качестве **показателя эффективности** может быть использовано среднее время:

- цикла управления;
- обработки информации;
- выполнения совокупности расчетов;
- доведения информации до потребителя и др.

Соответственно, как **показатели ущерба** в этом случае могут быть использованы:

- относительное или абсолютное увеличение среднего времени цикла управления или соответствующая этому событию стоимость потерь для субъектов ИС;
- относительное или абсолютное увеличение среднего времени обработки информации или соответствующая этому событию стоимость потерь для субъектов ИС и т.д.

Каждый из этих показателей в свою очередь есть функция от показателей более низкого иерархического уровня:

- эффективности решаемых объектом частных функциональных задач;
- эффективности процесса обработки информации;
- качества исходной и обрабатываемой на объекте информации;
- качества функционирования аппаратных и программных средств.

Каждый из перечисленных показателей может быть представлен системой показателей еще более низкого уровня. Например, для аппаратных средств в качестве таких показателей могут служить тактико-технические характеристики, вид и допустимые пределы изменения которых указывается в формуляре на эти средства.

### Показатели предотвращенного ущерба

Выбор показателей определяется:

- назначением методик;
- технологией оценки эффективности и выбора мер ЗИ;
- целевым назначением мер ЗИ, которое заключается в предотвращении ущерба субъектам информационных отношений от угроз нарушения безопасности информации.

Исходя из назначения методик и общей технологии оценки эффективности и выбора мер ЗИ можно сформулировать некоторые *требования к показателям*:

*Определение*

- должны выбираться с учетом системного подхода к исследованию вопросов оценки эффективности и выбора мер ЗИ, т.е. с учетом задач, решаемых в процессе анализа и синтеза;
- на этапе анализа для оценки степени опасности угроз БИ желательно, чтобы показатели эффективности могли принимать абсолютные значения;
- на этапе синтеза показатели эффективности должны обеспечивать возможность проведения сравнительной оценки различных по характеру и способам реализации мер ЗИ, поэтому желательно, чтобы указанные показатели могли измеряться в относительных единицах.

Поскольку целевым назначением СЗИ является предотвращение угроз БИ, в качестве показателей эффективности могут быть выбраны показатели предотвращенного ущерба субъектам ИС.

*Показатель предотвращенного ущерба*

***В качестве субъектов информационных отношений рассматриваются:***

- пользователи информации;
- лица, о которых информация накапливается и обрабатывается;
- собственники информации или уполномоченные ими органы и организации с правом владения и распоряжения;
- собственники, владельцы и пользователи ИС;
- органы управления, администрация ИС.

Для выбора показателей, характеризующих возможный ущерб от различных угроз информации, необходимо проанализировать механизм возникновения ущерба от этих угроз.

Схема, иллюстрирующая механизм возникновения ущерба, представлена на рис. 19.1.

***Ущерб от нарушения БИ на типовой ИС является следствием следующих событий:***

- воздействия угроз на технические средства обработки информации;
- воздействия угроз посредством физических полей, создаваемых основными и вспомогательными техническими средствами обработки информации и людьми — носителями информации;
- воздействия угроз на людей — носителей информации и/или имеющих доступ к информации в процессе ее обработки.

Для установления причинно-следственных связей, описывающих процесс возникновения ущерба субъектам ИС в результате нарушения безопасности информации, рассмотрим более подробно последствия воздействия угроз БИ на элементы объекта информатики.

Воздействие угроз на аппаратные средства ИС приводит к ухудшению качества их функционирования, которое может проявляться как ухудшение их тактико-технических характеристик (временных, точностных, энергетических, частотных и прочих в зависимости от типа средства).

Учитывая, что аппаратные средства представляют собой материальную основу процесса обработки информации в ИС, ухудшение их тактико-технических характеристик (ТТХ) автоматически ведет к снижению эффективности процесса обработки информации и далее, через снижение эффективности решаемых объектом ИС частных функциональных задач — к снижению эффективности функционирования объекта ИС в целом. В свою очередь ***это приводит к потерям, издержкам, которые несут субъекты ИС, вид и масштаб которых определяются:***

- содержанием информации, обрабатываемой в ИС;
- областью применения (использования) результатов обработки информации (выходной информации);
- степенью и видом нарушения БИ;
- видом источника угроз БИ и целью его деятельности.

Аналогичные последствия возникают при воздействии угроз БИ на программные средства, используемые в процессе обработки информации на ИС, а также при воздействии угроз БИ на физическое поле — носители информации и на людей — носителей информации и/или участников процесса обработки информации (персонал, пользователи ИС, источники информации).

Результаты приведенного анализа позволяют сформировать иерархию видов ущерба от угроз БИ и соответствующих показателей для их оценки.

Виды и показатели ущерба представлены на рис. 19.2 и 19.3.

Примерный перечень показателей для оценки качества информации и соответствующих им показателей ущерба, связанных с ухудшением качества информации под воздействием угроз БИ, приведен в табл. 19.2.

Для выбора проблемно-ориентированной системы показателей, т.е. системы показателей, оценивающих конкретные условия ИС, необходимо, основываясь на приведенных выше рекомендациях, ***сформировать свою систему показателей эффективности мер ЗИ, привязав ее к конкретным условиям эксплуатации ИС с учетом:***

- назначения, области использования ИС;
- задач, решаемых в ИС;
- наиболее вероятных видов и источников угроз БИ;
- показателей, принятых для оценки эффективности ИС и решаемых в ИС частных функциональных задач;
- структуры и состава ИС;
- модели процесса обработки информации в ИС;
- содержания информации, обрабатываемой в ИС.

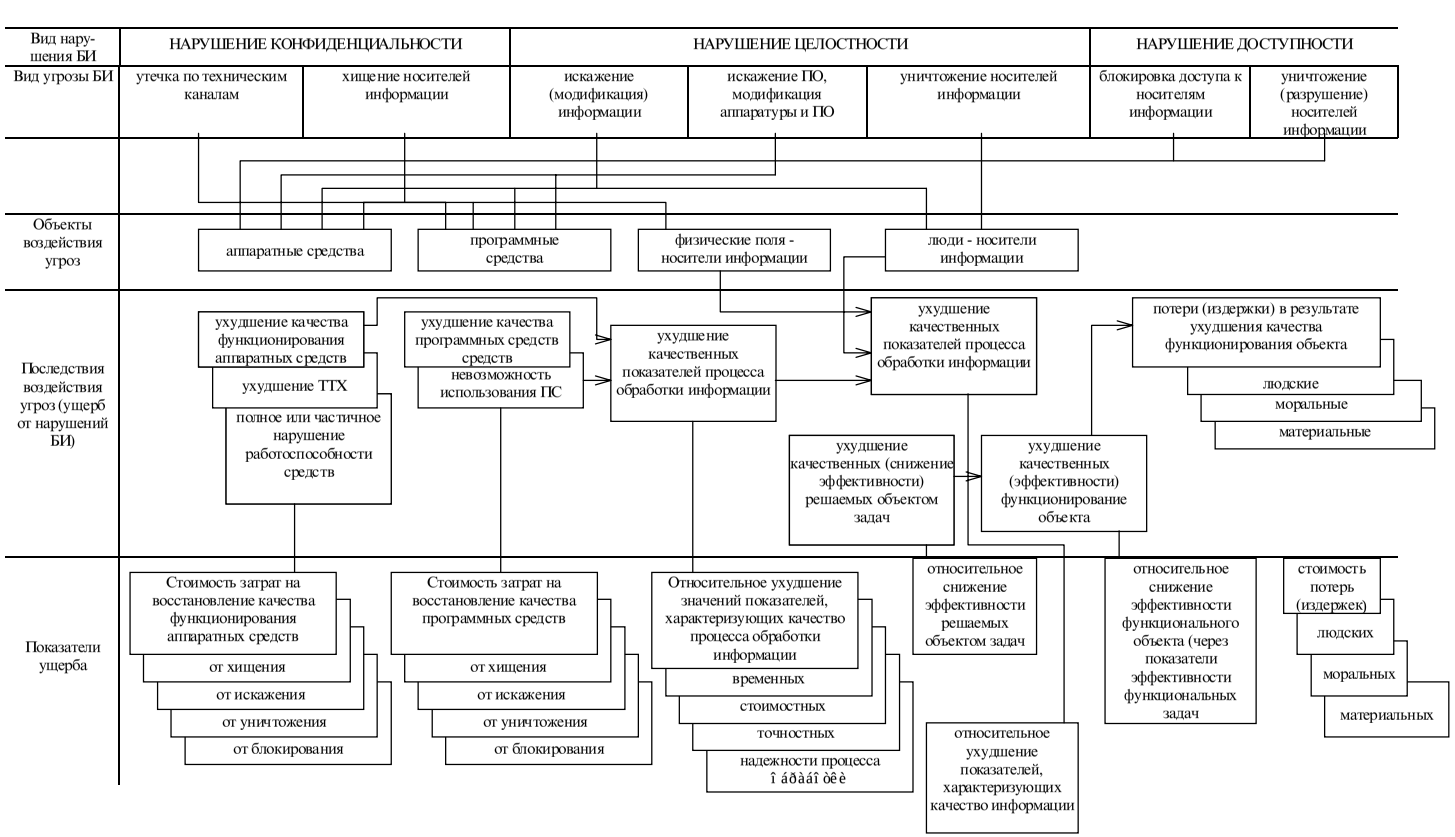



**РИСУНОК 19.1.** *Структурная схема механизма возникновения ущерба от угроз безопасности информации.*

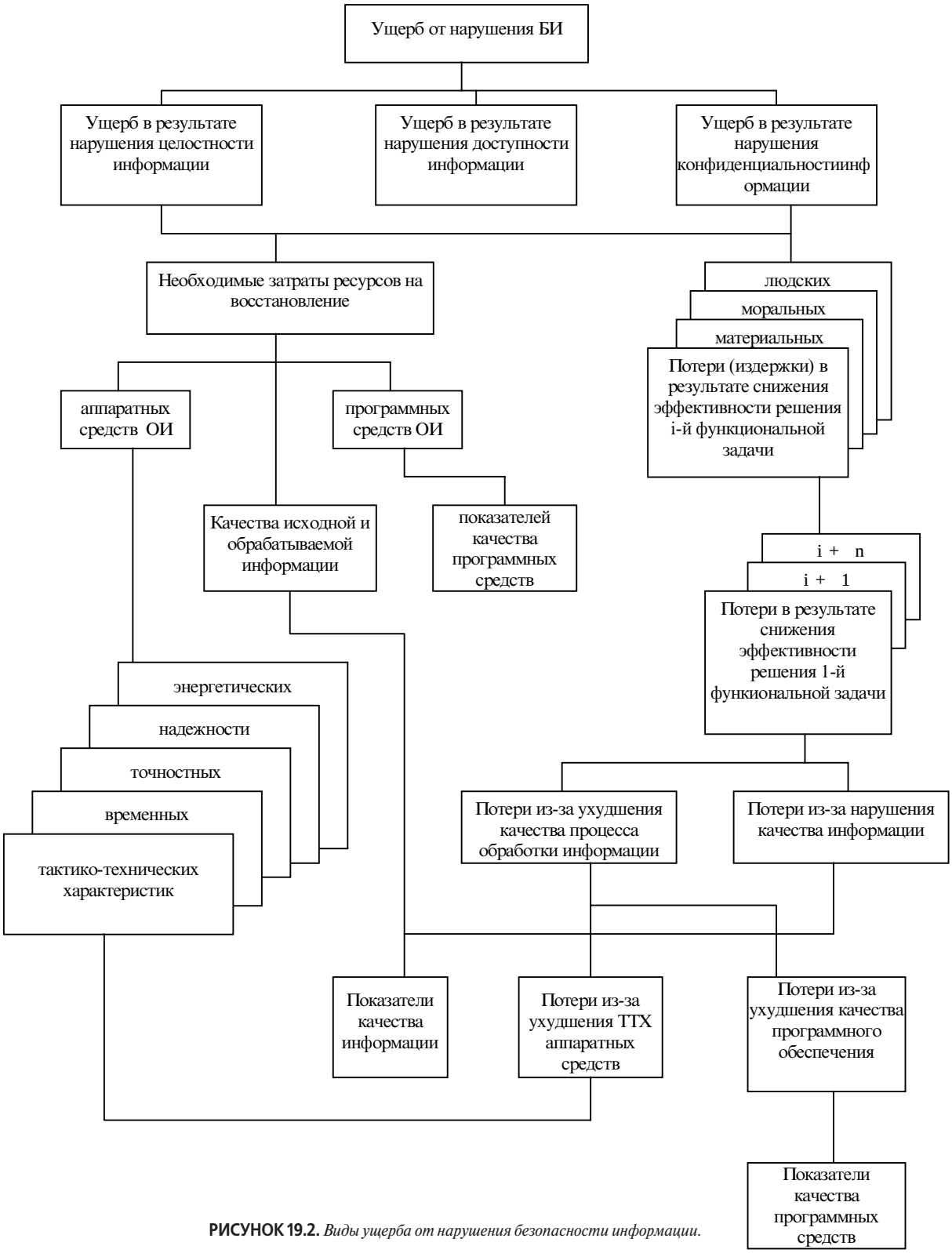



**РИСУНОК 19.2.** *Виды ущерба от нарушения безопасности информации.*

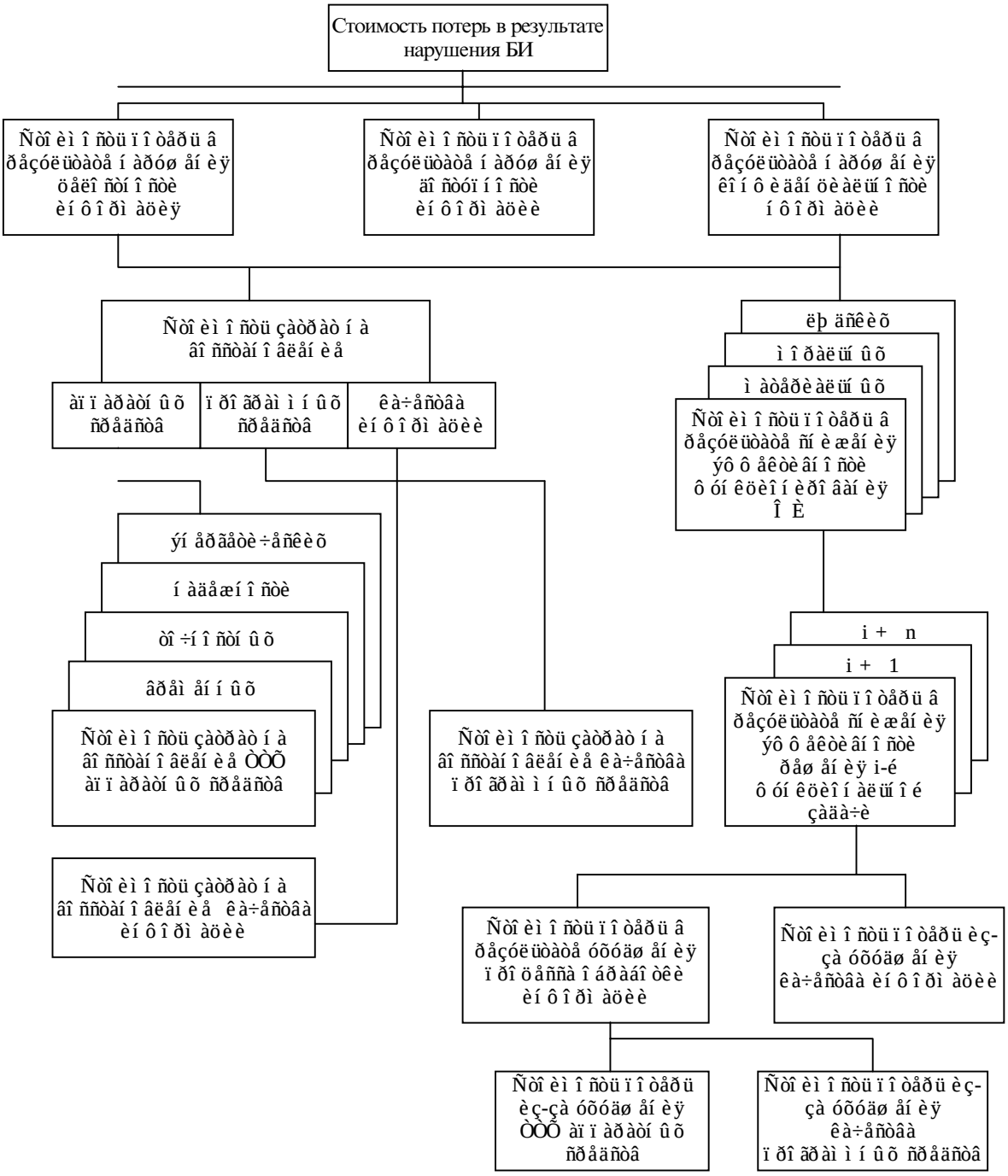



**РИСУНОК 19.3.** *Система показателей ущерба от нарушения безопастности информации.*

## Резюме

Оценка рисков производится с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящие потенциальную угрозу в разряд реально опасных и, следовательно, требующие принятия дополнительных защитных мер.

Как правило, для каждой подобной угрозы существует несколько решений по ее нейтрализации. При оценке их стоимости и эффективности следует учитывать не только расходы на закупку оборудования и программных средств, но и такие обстоятельства, как возможность экранирования одним сервисом безопасности нескольких прикладных, его совместимость с аппаратно-программной структурой организации, стоимость обучения персонала для работы с ним.

Когда намеченные меры приняты, необходимо проверить их действенность, например, произвести автономное и комплексное тестирование программно-технического механизма защиты. Если проверка показывает, что в результате проделанной работы остаточные риски снизились до приемлемого уровня, то можно намечать дату ближайшей переоценки, если нет, следует проанализировать допущенные ошибки и провести повторную оценку рисков.

***Цель оценки риска*** состоит в том, чтобы определить риск для ИС. Процесс оценки риска проводится в два шага. На первом шаге определяют границы ИС для анализа, требуемую степень детализации описания ИС при оценке и методологию, которая будет использоваться. На втором шаге проводится анализ риска. Анализ риска может быть разбит на идентификацию ценностей, угроз и уязвимых мест, оценку вероятностей, и измерение риска.

***Цель минимизации риска*** состоит в том, чтобы применить эффективные меры защиты таким образом, чтобы остаточный риск в ИС стал приемлем. Минимизация риска состоит из трех частей: определения тех областей, где риск является недопустимо большим; выбора наиболее эффективных средств защиты; оценивания мер защиты и определения , приемлем ли остаточный риск в ИС.

Процесс управления риском включает следующие этапы:

1. Определение степени детализации, границ анализа и методологии.
2. Идентификация и оценка ценностей.
3. Идентификация угроз и определение вероятности.
4. Измерение риска.
5. Выбор соответствующих средств защиты.
6. Внедрение и испытания средств защиты.
7. Проверка остаточного риска.