РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Информационные технологии. Администрирование подсистем защиты информации

Тема 8. Оценка эффективности и надёжности функционирования подсистемы защиты информации

Вопросы:

1. *Понятие эффективности*
2. *Аудит информационной безопасности компьютерных систем*
3. *Методика проведения инструментальных проверок*

Литература

1. Митюшин Д.А. Вопросы оценки эффективности комплексов и систем с беспилотными летательными аппаратами Министерства внутренних дел // «Специальная техника», 2011. – № 5. с. 40…46
2. Оценка эффективности и анализ защищённости систем защиты информации // http://sbornik.dstu.education/articles/RU/283.pdf
3. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. Екатеринбург : УГТУ-УПИ, 2008. 248 с.
4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 е.: ил. – (Профессиональное образование).

1. Понятие эффективности

1.1. Основные термины и определения

Анализ, синтез и применение подсистем защиты информации требует оценки эффективности их применения, используя различный математический аппарат (исследование операций, теория игр, теория массового обслуживания, фрактальный анализ и т.п.) и методы моделирования.

Для начала введём основные термины и определения.

В исследовании операций под ***операцией*** [Вентцель Е.С. Введение в исследование операций. – М.: Издательство «Советское радио», 1964. – 391 с.] понимается любое мероприятие (или система действий), объединённое единым замыслом и направленное на достижение определённой цели.

Примерами операций могут служить:

- защита периметра сети;
- применение системы антивирусной защиты;
- применение межсетевого экрана;
- внедрение или модернизация подсистемы защиты информации и т.д.

1. Понятие эффективности

1.1. Основные термины и определения

Необходимо отметить, что сформулированное выше понятие «операция» не совпадает с понятием «операции», используемом, например, в военном деле, или при проведении специальных операций и в антитеррористической деятельности, а является более широким. В приведённом выше смысле примером операции, хотя и элементарным, может служить даже «блокирование процесса в памяти узла». Из подобных «мелких» элементарных операций складываются более сложные.

Каждая операция продумывается, планируется заранее, её осуществление предполагается в каких-либо условиях. Но, как правило, не все условия, в которых будет выполняться операция и которые определяют её успех, точно известны заранее. Некоторые из них содержат элемент неопределённости, случайности. Например, нельзя заранее точно предсказать: время атаки, атакуемый узел, как поведёт себя нарушитель при его обнаружении и блокировании и т.д.

Большинство операций вообще проводится в условиях, содержащих элемент случайности, иногда очень существенный. Ни для кого не секрет, что операция, задуманная определённым образом и рассчитанная на определённый результат, может окончиться совсем иначе из-за наличия случайных факторов.

1. Понятие эффективности

1.1. Основные термины и определения

В связи с этим возникают следующие две ***задачи*** [Вентцель Е.С. Введение в исследование операций. – М.: Издательство «Советское радио», 1964. – 391 с]:

- задача предсказания ожидаемого успеха операции в условиях, включающих элемент случайности;
- задача рациональной организации операции с учётом наличия и влияния случайных факторов.

Рассмотрим первую задачу. Так как успех операции зависит от заранее неизвестных, случайных факторов, точно предсказать исход каждой отдельной операции невозможно. Например, нельзя в точности предсказать, сколько радиоприёмников будет подавлено при постановке помех на определённом участке местности. Любое предсказание имеет смысл только в среднем, для большого числа однородных операций. Нельзя, например, предсказать, будет ли опасный сигнал перехвачен на расстоянии 53 м от защищаемого компьютера при однократном включении этого компьютера, но можно подсчитать средний процент включений, при котором сигнал будет перехвачен. Таким образом, чтобы предсказание имело смысл, исследуемая операция (по крайней мере, в принципе) должна обладать свойством повторяемости.

1. Понятие эффективности

1.1. Основные термины и определения

Перейдём ко второй задаче.

Организовать операцию – значит каким-либо образом ***выбрать некоторые элементы или параметры, от которых зависит её успех***. Этими элементами могут быть различные характеристики применяемых в исследуемой операции технических средств, например:

- мощность опасного сигнала от случайной антенны;
- громкость голоса человека-источника информации;
- степень совпадения сигнатуры кода с хранящейся в БД антивирусной программы и т. п.

С другой стороны, такими элементами могут быть способы осуществления операции, например:

- число участвующих в операции единиц технических средств защиты информации;
- расположение и состав программно-аппаратных средств в распоряжении злоумышленника;
- расположение технических средств охраны на объекте защиты;
- выход коммуникаций за пределы контролируемой зоны и т. п.

1. Понятие эффективности

1.1. Основные термины и определения

Условно задачи организации операций можно разделить на ***технические*** (выбор рациональных технических характеристик применяемых средств защиты информации) и ***тактические*** (выбор рациональных способов применения выбранных или заданных программно-аппаратных).

Примеры технических задач:
- выбор антивирусной программы;
- выбор системы доверенной загрузки и т. п.

Примеры тактических задач:
- выбор способа реагирования при обнаружении угрозы (если она не запрограммирована при срабатывании системы защиты);
- выбор месторасположения видеокамер систем видеонаблюдения и т. п.

Однако не всегда удаётся провести чёткую границу между техническими и тактическими задачами исследования операций. Например, сервер безопасности, предназначенная для управления процедурами разграничения доступа, может рассматриваться с двух точек зрения:
- как средство управления всеми элементами сети (включая сам сервер);
- как техническое устройство, характеристики которого должны быть выбраны рациональным образом.

1. Понятие эффективности

1.1. Основные термины и определения

В дальнейшем ***любой выбор определённого способа организации операции*** (в техническом или тактическом смысле) будем называть ***решением***.

Основная цель и содержание исследования операций [Вентцель Е.С. Введение в исследование операций. – М.: Издательство «Советское радио», 1964. – 391 с.] – количественное обоснование ***рациональных*** (иначе, ***оптимальных***) решений. Из всех возможных способов организации операции выделяется тот или те, которые оказываются по тем или иным соображениям более выгодными.

Однако само принятие решения выходит за рамки исследования операций и относится к компетенции ответственного лица, которое, опираясь на ряд известных ему данных (в том числе и на расчёты, связанные с математическими исследованиями), производит окончательный выбор того или другого варианта.

Это лицо будем называть «лицом, принимающим решение» (ЛПР). Даже в тех случаях, когда процесс управления максимально автоматизирован, это правило остаётся в силе: ЛПР нужно принять решение, например, по разумному выбору управляющего алгоритма.

1. Понятие эффективности

1.1. Основные термины и определения

Необходимо отметить, что подсистема защиты информации представляет собой некую систему. Под ***системой*** будем понимать ***совокупность (множество) объектов и процессов, называемых элементами, взаимосвязанных и взаимодействующих между собой, которые образуют единое целое, обладающее свойствами, не присущими составляющим его элементам, взятым в отдельности***.

Элемент системы – это объект (процесс), выполняющий определённые функции и не подлежащий дальнейшему разделению в рамках поставленной задачи Совокупность однородных элементов системы иногда называют ***компонентами***.

Необходимо отметить, что система может состоять из подсистем, т.е. из систем, являющимися элементами рассматриваемой системы (например, подсистемы антивирусной защиты, подсистема парольного доступа и т.д.).

Кроме того, ПЗИ решает поставленную задачу не саму по себе, а в интересах некой ***надсистемы*** (информационная система), т.е. системы, элементом которой является рассматриваемая система. Таким образом, при оценке комплексов необходимо использовать системный подход и методы системного анализа.

1. Понятие эффективности

1.1. Основные термины и определения

В тоже время следует заметить, что в теории системного анализа в качестве постулата принято следующее утверждение: любая система, вне зависимости от её природы, обладает ***основной*** и ***неосновными*** функциями – позитивными, негативными и нейтральными, преднамеренными и непреднамеренными. При этом, одна часть данных функций проявлена, а другая – скрыта как от самой системы, так и от исследователя. Чаще всего в исследуемой системе скрыты какие-либо неосновные функции, либо не ясны их связи с основной функцией. Однако нередки ситуации, когда неизвестна либо заранее неверно определена основная функция рассматриваемой системы. Поэтому любое системное исследование следует начинать с установления или уточнения основной функции исследуемой системы. В этом случае она рассматривается как некий «чёрный ящик», функционирующий в составе надсистемы, заданные характеристики которого известны на данный период времени.

Однако никакое исследование операций невозможно без ***моделирования***. Философской базой [Теоретические основы системного анализа / Новосельцев В.И. [и др.] ; под ред. В. И. Новосельцева. – М.: Майор, 2006. – 592 с] моделирования является теория отражения, точнее, исходный постулат об отражении как специфическом взаимодействии двух систем, в результате которого одна система отображается в другой.

1. Понятие эффективности

1.1. Основные термины и определения

В научных исследованиях свойство отражения приобретает форму взаимодействия реальности и человеческого сознания. Реальность через органы чувств человека воспринимается и воздействует на его сознание. В результате этого в сознании исследователя формируется ***модель*** (от фр. modèle – образец), которую он каким-либо способом воспроизводит на том или ином носителе информации. Таким образом, ***модель операции*** (***системы***) представляет собой упрощённую схему данной операции (системы).

Математически это можно выразить следующим образом.

Допустим, существует некая система-оригинал, которую обозначим как S_0. Её модель S есть некая иная система, представляющая собой образ (подобие) системы S_0. Это происходит при моделирующем отображении (соответствии подобия) оригинала, что обозначают записью: f: (S_0) → S. Круглые скобки в данной записи означают, что f – частично определённое отображение, т.е. не все черты оригинала S_0 отражаются моделью S.

1. Понятие эффективности

1.1. Основные термины и определения

Моделирующее отображение f обычно представляют в виде композиции двух отображений – огрубляющего g и гомоморфного h (от *греч.* γόμός – одинаковый и μορφή – форма):

$$g: (S_0) \rightarrow S_1;\ h: S_1 \rightarrow S;\ f = h;\ g: (S_0) \rightarrow S\ , \qquad (1)$$

где S_1 – некоторая подсистема системы S, $S_1 \subset S$.

Итак, модель представляет собой упрощённый образ оригинала. Это упрощение (огрубление) осуществляется отображением g, при котором, сознательно удаляя из системы S_0 некоторые компоненты и связи, получаем подсистему S_1. С другой стороны, модель должна верно (в определённом смысле) отражать оригинал, хотя, возможно, и огрублённо. Именно это и осуществляет гомоморфное отображение h подсистемы S_1 на модель S.

Создание (***построение***) ***модели системы*** или ***операции*** – начальный и необходимый этап исследования операций, без которого никакое исследование операций (системы) невозможно. В самом деле, каждая реальная операция имеет многочисленные связи с рядом факторов и условий, из которых некоторые являются важными, существенными, а другие побочными, второстепенными.

1. Понятие эффективности

1.1. Основные термины и определения

Попробуем разобраться с термином «эффективность». ним. Рассмотрим два определения.

Под ***эффективностью*** системы понимается количественная или качественная характеристика, позволяющая судить о степени выполнения системой присущих ей функций.
Эффективность операции – степень её приспособленности к выполнению стоящей перед ней задачи. Чем лучше организована операция, тем она эффективнее.

Оба этих определения похожи. Но есть некоторые различия. Первое определение даёт нам понятие эффективности системы, например, исследуемого СЗИ, а второе – эффективности его применения для решения определённых задач. Однако в ряде случаев первое определение может характеризовать и эффективность применения системы.

В то же время необходимо отметить следующее. Любая операция представляет собой некое мероприятие (целенаправленное действие), осуществляемая при учёте трёх факторов:
– результат;
– затрачиваемое время;

1. Понятие эффективности

1.1. Основные термины и определения

Результат – это тот эффект, который мы получаем, применяя рассматриваемую систему в рассматриваемой операции (или в нескольких операциях).

Без времени в пространстве ничего не происходит, поэтому при исследовании операций необходимо ограничивать время на проведение операции, ибо любая операция имеет конечное время своего существования. Временной фактор может быть ограничен действующими нормативными документами, «волевым» решением ЛПР, техническими параметрами исследуемого комплекса или какими-либо внешними воздействующими факторами.

Естественно, что при выполнении какой-либо задачи расходуются ресурсы: людские, технические, финансовые и т.д. Поскольку перечисленные ресурсы имеют различную физическую и материальную природу, то их тяжело учесть в ходе оценки эффективности, используя натуральное выражение. Поэтому рациональнее всего осуществлять учёт данных ресурсов в денежной форме, так как деньги являются всеобщим эквивалентом, посредством которого выражается стоимость товаров и услуг. Кроме того, следует исходить из постулата ограниченности ресурсов, в противном случае можно создать сколь угодно сложную и беспредельно дорогую систему.

1. Понятие эффективности

1.1. Основные термины и определения

Таким образом, под ***эффективностью*** системы, будем понимать степень выполнения системой решаемых ею задач с учётом временных и экономических параметров. С другой стороны, величина, характеризующая результат деятельности безотносительно к тому, какими усилиями он достигнут, будем называть ***эффектом*** или ***результативностью***. Хотя ряд исследователей под результативностью понимают эффективность, с точки зрения автора это является некорректным, ибо результативность – достижение результата любой ценой (например, ценой гибели подразделения, выполняющего задачу).

В стандарте менеджмента качества ISO 9000:2005 приведено различие понятий эффективность и результативность:
«…3.2.14 Результативность (effectiveness)
– степень, в какой реализована запланированная деятельность и достигнуты запланированные результаты.
3.2.15 Эффективность (efficiency)
– соотношение между достигнутым результатом и использованными ресурсами.
…»

Чтобы судить об эффективности системы или операции, необходимо иметь некоторую численную величину, который будем называть ***показателем*** эффективности.

1. Понятие эффективности

1.1. Основные термины и определения

В качестве показателя эффективности при исследовании операций обычно применяется или вероятность какого-то события, или среднее значение (математическое ожидание) некоторой случайной величины. Например, показателями эффективности могут служить: вероятность обнаружения атаки на защищаемую информационную систему; средняя площадь покрытия видеокамерами контролируемой зоны и т. п.

Выбор показателя эффективности является достаточно сложной задачей. И в первую очередь при выборе показателя необходимо отталкиваться от цели исследования операций. Приведём пример неудачного выбора показателя, описываемый Ф. Морзом и Д. Кимбеллом, который стал хрестоматийным.

Во время Второй мировой войны в Англии на торговых судах для их защиты поставили зенитные средства – пулемёты и малокалиберные пушки. Проведённый через год анализ показал, что было сбито только 4 % вражеских самолётов, атаковавших вооружённые торговые суда. Так как данная цифра не велика, был сделан вывод, что зенитные средства не окупают расходов на их установку. Таким образом, по выбранному показателю эффективности – число сбитых самолётов противника – установка на торговые суда средств ПВО оказалась нецелесообразной.

1. Понятие эффективности

1.1. Основные термины и определения

Однако специалисты указали, что выбранный показатель является непредставительным, так как не отражает основной цели исследуемой операции, которая состояла в защите торговых судов от налёта авиации, а не в уничтожении самолётов противника. В данном случае представительным показателем был снижение потерь торговых судов. При анализе выяснилось, что из числа атакованных судов при наличии зенитных средств было потоплено 10 %, а при их отсутствии – 25 %. Технико-экономический анализ показал, что затраты на установку зенитных средств полностью окупались стоимостью сохранённых судов.

Рядом с понятием «показатель эффективности», находится понятие «критерий эффективности». Иногда эти два понятия смешивают, что с точки зрения автора не является верным. Под ***критерием эффективности*** понимают некоторое решающее правило, согласно которому данная система (операция) признаётся эффективной или оптимальной.

Например, выполняется оценка эффективности применения антивирусного программного комплекса на каком-либо компьютере. Тогда в качестве показателя эффективности целесообразно выбрать математическое ожидание $M_{об}$ обнаружения и обезвреживания вредоносных программ. А критерий эффективности – матожидание $M_{об}$ должно быть не меньше заданного при

1. Понятие эффективности

1.2. Эффективность защиты информации

К уровню информационной безопасности различных компаний, предприятий и организаций предъявляются высокие требования. При этом требования и задачи защиты информации могут значительно отличаться. Их формулировка и решение является сложной организационно-технической задачей, требующей комплексного подхода. Решение каждой подзадачи может иметь несколько решений, имеющих различную эффективность, сложность и стоимость реализации и поддержки. В связи с этим актуальной является проблема оценки эффективности выбранных и принятых решений защиты информации.

В настоящее время существует много работ, посвящённых проблемам защиты компьютерной безопасности в информационных системах обработки информации и сетях передачи данных.

Однако многие методологические, методические и практические аспекты защиты информации носят дискуссионный характер. Это связано с малоизученностью некоторых аспектов защиты, вызванных сложностью рассматриваемых систем, постоянно изменяющимся перечнем угроз и отсутствием единого подхода к построению и анализу систем защиты.

1. Понятие эффективности

1.2. Эффективность защиты информации

Например, в компьютерной вирусологии, несмотря на многочисленные специализированные конференции и регулярные семинары, работы множества фирм, занимающихся разработкой антивирусного программного обеспечения, до сих пор нет общеутверждённой и стандартизованной классификационной таблицы вирусов. Также недостаточно хорошо проработаны система оценки информационной безопасности и критерии защищённости, что делает поставленную задачу необходимой и актуальной.

Большинство моделей, оценивающих эффективность систем защиты информации (СЗИ) не дают численных методов определения величины защищённости и вероятности несанкционированного проникновения в информационную систему (ИС). Оценка таких показателей обычно даётся экспертами-специалистами в области информационных технологий.

Управление рисками в основном учитывает риски с высокой вероятностью появления в период эксплуатации ИС. Такие риски обычно приносят незначительный или легко устранимый ущерб (вирусные атаки), но на практике основное внимание уделяется рискам с большим ущербом и с малой вероятностью. Это зачастую ведёт к неоправданно большим затратам при построении СЗИ. Выбор оптимальной модели с точки зрения «цена-качество» представляет очень сложную задачу.

1. Понятие эффективности

1.2. Эффективность защиты информации

На основании модели угроз разрабатывается наиболее выгодный (оптимальный) вариант построения СЗИ, который представляется в виде набора угроз и мероприятий по защите информации. В общем такую модель можно изобразить в виде следующей схемы, приведённой на рисунке 1.

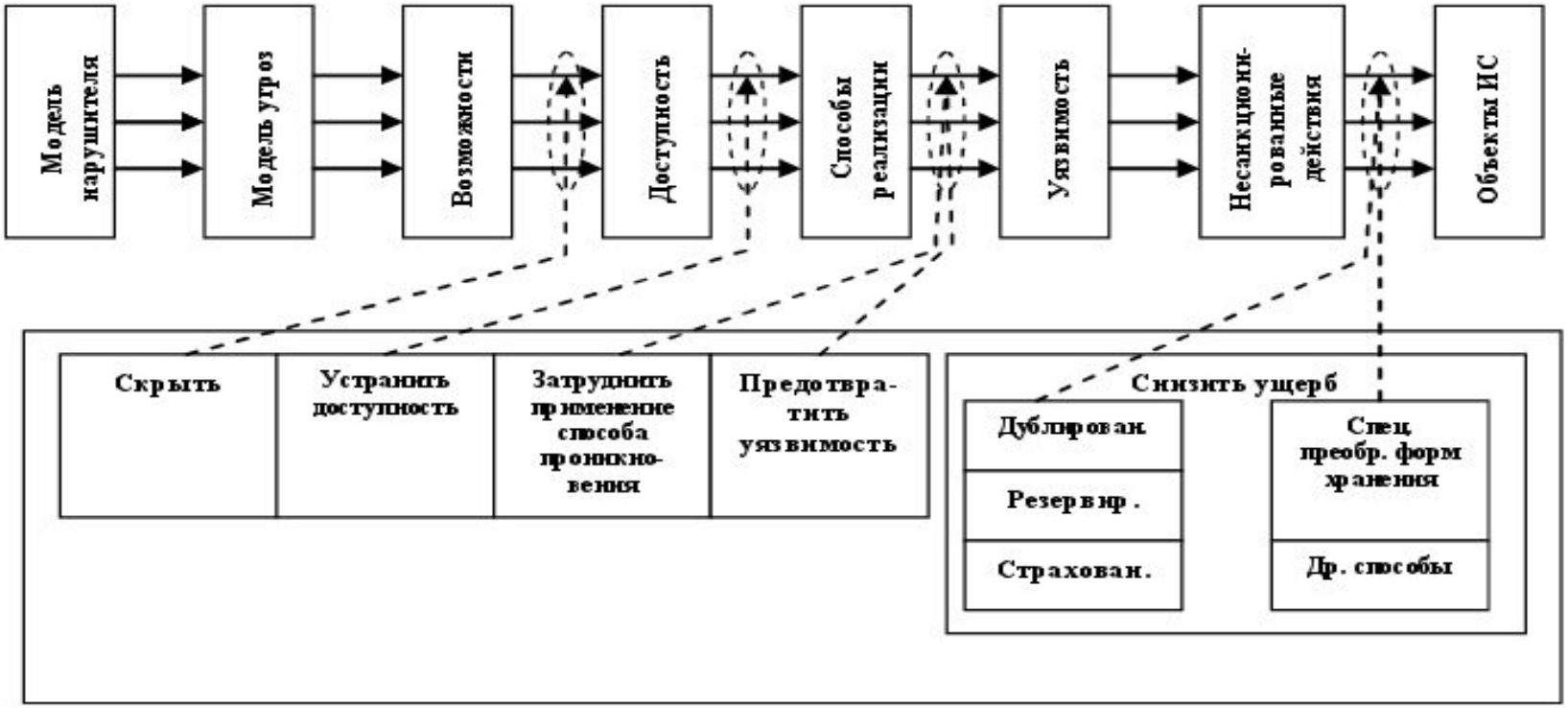

Рис. 1 Схема защиты информации в автоматизированной системе обработки информации

1. Понятие эффективности

1.2. Эффективность защиты информации

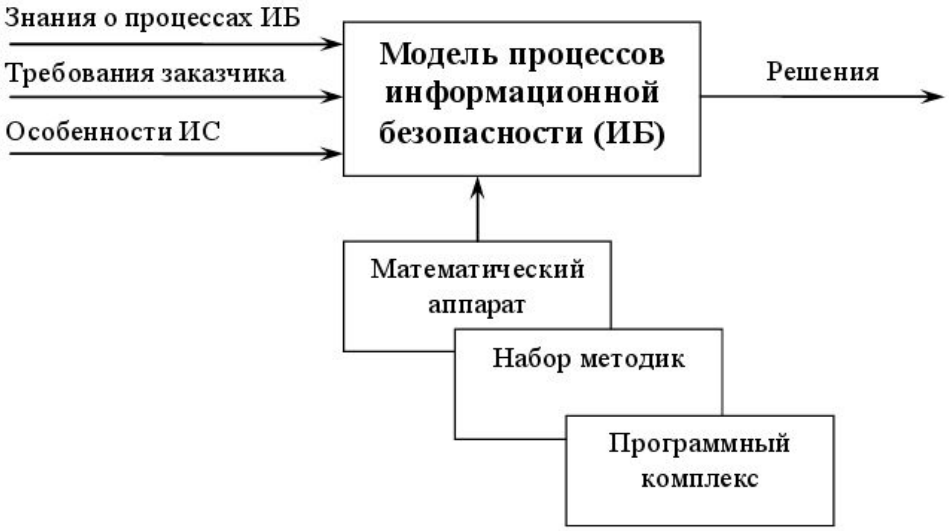

Рис. 2 Модель СЗИ

В моделях защиты информации выделяют коэффициент опасности события ($К_{оci}$) от ущерба ($У_i$), вызванного несанкционированными действиями ($Н_i$). При несанкционированных действиях ущерб наступает независимо от издержек, вложенных в создание автоматизированной системы. Таким образом, задачей создания СЗИ является нейтрализация или минимизация ущерба от несанкционированных действий.

Задача обеспечения информационной безопасности состоит в разработке модели представления системы мер, которые позволили бы решать задачи создания, использования и оценки эффективности СЗИ. В упрощённом виде модель СЗИ

1. Понятие эффективности

1.2. Эффективность защиты информации

Основной задачей модели является обеспечение процесса создания системы информационной безопасности за счёт правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Специфическими особенностями решения задачи создания систем защиты являются:

- неполнота и неопределённость исходной информации о составе ИС и характерных угрозах;
- многокритериальность задачи, связанная с необходимостью учёта большого числа частных показателей (требований) СЗИ;
- наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ.

Такая модель должна удовлетворять целый ряд требований.

1 Использоваться в качестве:

– руководства по созданию СЗИ;

– методики формирования показателей и требований к СЗИ;

– инструмента для оценки СЗИ.

1. Понятие эффективности

1.2. Эффективность защиты информации

2 Обладать свойствами:
– универсальность;
– комплексность;
– простота использования;
– наглядность.
3 Позволять:
– задавать различные уровни защиты;
– получать количественные оценки;
– контролировать состояние СЗИ.

Эффективность СЗИ выражается в отношении полезных результатов её функционирования к затраченным ресурсам на её создание. Основным показателем эффективности СЗИ является коэффициент эффективности $К_{эф}$, как показатель её приближения к предельным издержкам на СЗИ:

$$К_{эф} = \frac{С_{СЗИ}}{М_{СЗИ}} \quad (1)$$

где $С_{СЗИ}$ – затраты на создание СЗИ;
$М_{СЗИ}$ – предельные издержки на СЗИ.

1. Понятие эффективности

1.2. Эффективность защиты информации

Коэффициент $К_{эф}$ применяется для расчётов «эффективность-стоимость». Для систем защиты информации не имеющих коммерческий характер, эффективность зависит от показателя «ущерб-стоимость», т.е. с помощью СЗИ увеличиваются затраты злоумышленника и его риски на взлом информации. Таким образом, эффективней будет та система защиты, в которой при наименьших затратах на её создание требуются наибольшие затраты на её взлом.

Сформулируем общие подходы к количественной оценке эффективности СЗИ.

В соответствии с современной теорией оценки эффективности систем, качество любого объекта, в том числе и СЗИ, проявляется лишь в процессе его использования по назначению (целевое функционирование), поэтому наиболее объективным является оценивание по эффективности применения.
Проектирование, организация и применение СЗИ фактически связаны с неизвестными событиями в будущем и поэтому всегда содержат элементы неопределённости. Кроме того, присутствуют и другие причины неоднозначности, такие как недостаточно полная информация для принятия управленческих решений или социально-психологические факторы. Поэтому, например, этапу проектирования СЗИ естественным образом сопутствует значительная неопределённость. По мере реализации проекта её уровень

1. Понятие эффективности

1.2. Эффективность защиты информации

Процедуры испытаний, сертификации или лицензирования не устраняют полностью неопределённость свойств СЗИ или её отдельных элементов и не учитывают случайный характер атак. Поэтому объективной характеристикой качества СЗИ – степенью её приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов, может служить только вероятность, характеризующая степень возможностей конкретной СЗИ при заданном комплексе условий.

В общей теории систем такая характеристика называется вероятностью достижения цели операции или вероятностью выполнения задачи системой. Данная вероятность должна быть положена в основу комплекса показателей и критериев оценки эффективности СЗИ.

При этом критериями оценки служат понятия пригодности и оптимальности. Пригодность означает выполнение всех установленных к СЗИ требований, а оптимальность – достижение одной из характеристик экстремального значения при соблюдении ограничений и условий на другие свойства системы. При выборе конкретного критерия необходимо его согласование с целью, возлагаемой на СЗИ.

1. Понятие эффективности

1.2. Эффективность защиты информации

Обычно при синтезе системы возникает проблема решения задачи с многокритериальным показателем. Некоторые авторы рассматривают показатели эффективности, которые предназначены при решении задачи сравнения различных структур СЗИ. Предлагается также использовать показатели эффективности вероятностно-временного характера, имеющие смысл функций распределения. В частности, к ним относятся вероятность преодоления системы защиты информации за некоторое время.

Оценку гарантий защиты также необходимо сформулировать в количественной форме.

В современных нормативных документах по информационной безопасности, используется, как известно, классификационный подход. Гораздо более конструктивными являются вероятностные методы, нашедшие широкое распространение в практике обеспечения безопасности в других прикладных областях. В соответствии с этими методами уровни гарантий безопасности СЗИ трансформируются в доверительные вероятности соответствующих оценок показателей. Для решения данной задачи можно рекомендовать теорию статистических решений, позволяющую находить оптимальные уровни гарантий безопасности.

1. Понятие эффективности

1.2. Эффективность защиты информации

Во-первых, оценка оптимального уровня гарантий безопасности в определяющей степени зависит от ущерба, связанного с ошибкой в выборе конкретного значения показателя эффективности. Во-вторых, для получения численных оценок риска необходимо знать распределения ряда случайных величин.

Это, конечно, в определённой степени ограничивает количественное исследование уровней гарантий безопасности, предоставляемых СЗИ, но, тем не менее, во многих практических случаях такие оценки можно получить, например, с помощью имитационного моделирования или по результатам активного аудита СЗИ.

Обобщённые данные о возможных показателях эффективности приведены в таблице 1, а критериев – в таблице 2.

1. Понятие эффективности

1.2. Эффективность защиты информации

Таблица 1 - Возможные показатели эффективности СЗИ

Требования к СЗИ	Вид показателя эффективности СЗИ
Наступление или отсутствие события	Вероятность события
Достижение требуемых характеристик	Вероятность достижения события не ниже требуемого уровня
Отклонение от заданных характеристик	Среднеквадратичное отклонение от требуемого результата

Таблица 2 - Возможные критерии эффективности СЗИ

Концепция эффективности СЗИ	Критерии эффективности
Пригодность	1. Приемлемый результат
	2. Допустимая гарантия
Оптимальность	1. Наилучший результат
	2. Наилучший средний результат
	3. Наибольший гарантированный результат

1. Понятие эффективности

1.2. Эффективность защиты информации

Для наглядного представления текущего состояния эффективности СЗИ целесообразно использовать лепестковую диаграмму, изображённую на рисунке 3. Маркеры отображающие значение защищённых параметров в процентах.

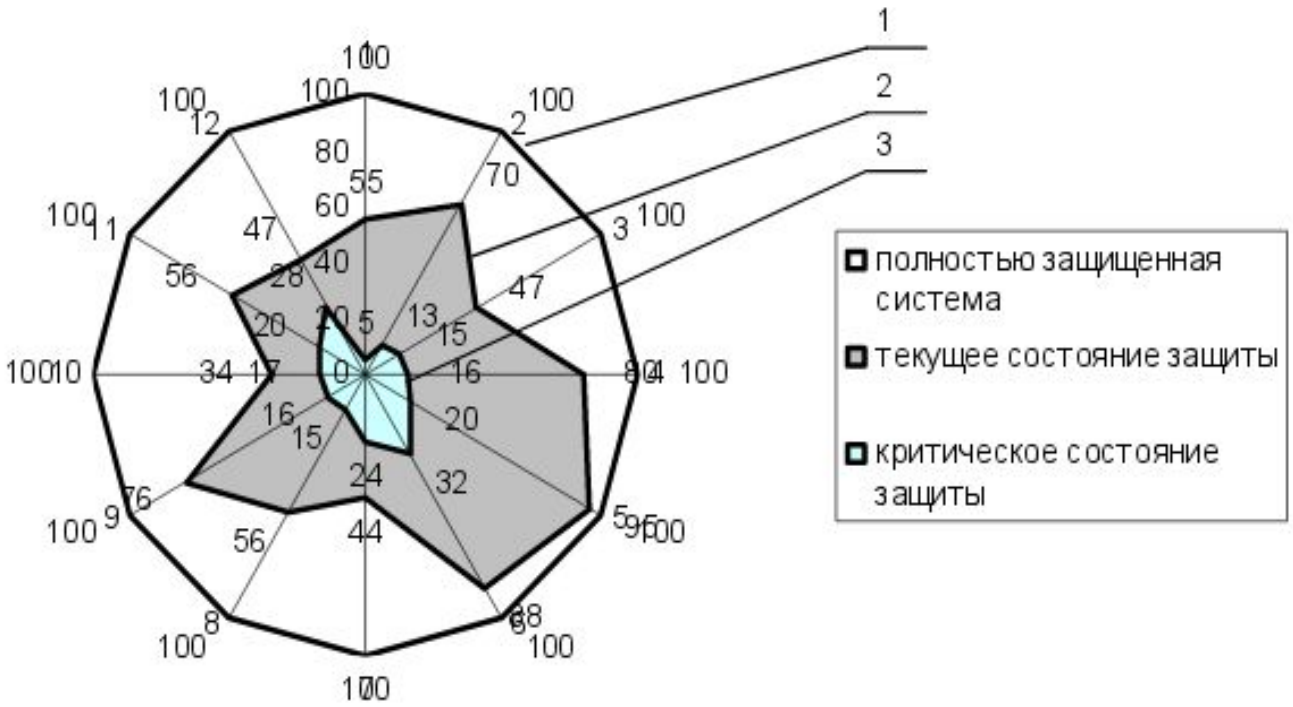

Рисунок 3 – Лепестковая диаграмма оценки защищённости СЗИ:
1 – полностью защищённый параметр системы;
2 – текущее состояние защищённости параметра системы;
3 – критическое состояние защищённости параметра системы

1. Понятие эффективности

1.2. Эффективность защиты информации

Из приведённой диаграммы видно, что СЗИ работает эффективно, так как текущее состояние всех параметров защищённости больше соответствующих критических. Средневзвешенный нормированный показатель степени защищённости ИС равен 62%, что больше на 44% соответствующего среднего критического параметра системы. Важно также отметить максимальную и минимальную разность между текущим и критическим параметром системы.

Максимальная разность составляет 75% по 5 параметру, а минимальная 17% по 10 параметру. Таким образом можно оценить избыточные и недостаточные меры защиты. Такой анализ позволяет более оптимально использовать выделенные ресурсы, особенной при использовании критерия «эффективность – стоимость».

Многочисленные методы оценки эффективности и защищённости СЗИ имеют некоторые недостатки. Для решения данной задачи можно воспользоваться несколькими критериями, а затем усреднить количественные показатели с различными коэффициентами доверия для разных методов. Ещё одним вариантом решения может быть использование методов нечёткой логики, как для усреднения разных методов оценки, так и для перевода нечёткого лингвистического мнения эксперта в количественную величину.

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

Аудит информационной безопасности (ИБ) представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области безопасности КС и вызывает постоянный интерес специалистов. Его основная задача – объективно оценить текущее состояние ИБ организации, а также её адекватность поставленным целям и задачам бизнеса.

Под аудитом ИБ понимается системный процесс получения объективных качественных и количественных оценок текущего состояния ИБ организации в соответствии с определёнными критериями и показателями на всех основных уровнях обеспечения безопасности: нормативно-методологическом, организационно-управленческом, процедурном и программно-техническом.

Результаты квалифицированно выполненного аудита ИБ организации позволяют построить оптимальную по эффективности и затратам систему обеспечения информационной безопасности (СОИБ), представляющую собой комплекс технических средств, а также процедурных, организационных и правовых мер, объединённых на основе модели управления ИБ.

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

В результате проведения аудита могут быть получены как качественные, так и количественные оценки. При качественном оценивании, например, может быть приведён перечень уязвимостей в программно-аппаратном обеспечении с их классификацией по трёхуровневой шкале опасности: высокая, средняя и низкая. Количественные оценки чаще всего применяются при оценке риска для активов организации, создаваемого угрозами безопасности. В качестве количественных оценок могут выступать, например, цена риска, вероятность риска, размер риска и т. п.

Объективность аудита обеспечивается, в частности, тем, что оценка состояния ИБ производится специалистами на основе определённой методики, позволяющей объективно проанализировать все составляющие СОИБ.

Аудит ИБ может представлять собой услугу, которую предлагают специализированные фирмы, тем не менее в организации должен проводиться внутренний аудит ИБ, выполняемый, например, администраторами безопасности.

Традиционно выделяют три типа аудита ИБ, которые различаются перечнем анализируемых компонентов СОИБ и получаемыми результатами:

− активный аудит;

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

Активный аудит

Активный аудит представляет собой обследование состояния защищённости определённых подсистем информационной безопасности (ПИБ), относящихся к программно-техническому уровню.

Например, вариант активного аудита, называемый тестом на проникновение (Penetration test), предполагает обследование подсистемы защиты сетевых взаимодействий. Активный аудит включает:

- анализ текущей архитектуры и настроек элементов ПИБ;
- интервьюирование ответственных и заинтересованных лиц;
- проведение инструментальных проверок, охватывающих определённые ПИБ.

Анализ архитектуры и настроек элементов ПИБ проводится специалистами, обладающими знаниями по конкретным подсистемам, представленным в обследуемой системе (например, могут требоваться специалисты по активному сетевому оборудованию фирмы Cisco или по ОС семейства Microsoft), а также системными аналитиками, которые выявляют возможные изъяны в организации подсистем. Результатом этого анализа является набор опросных листов и инструментальных тестов.

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

Опросные листы используются в процессе интервьюирования лиц, отвечающих за администрирование АИС, для получения субъективных характеристик АИС, для уточнения полученных исходных данных и для идентификации некоторых мер, реализованных в рамках СОИБ. Например, опросные листы могут включать вопросы, связанные с политикой смены и назначения паролей, жизненным циклом АИС и степенью критичности отдельных её подсистем для АИС и бизнес-процессов организации в целом.

Параллельно с интервьюированием проводятся инструментальные проверки (тесты), которые могут включать следующие мероприятия:

- визуальный осмотр помещений, обследование системы контроля доступа в помещения;
- получение конфигураций и версий устройств и ПО;
- проверка соответствия реальных конфигураций предоставленным исходным данным;
- получение карты сети специализированным ПО;
- использование сканеров защищённости (как универсальных, так и специализированных);
- моделирование атак, использующих уязвимости системы;
- проверка наличия реакции на действия, выявляемые механизмами обнаружения и реагирования на атаки.

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

Аудитор может исходить из следующих моделей, описывающих степень его знания исследуемой АИС (модель знания):

- модель «чёрного ящика» – аудитор не обладает никакими априорными знаниями об исследуемой АИС. Например, при проведении внешнего активного аудита (то есть в ситуации, когда моделируются действия злоумышленника, находящегося вне исследуемой сети), аудитор может, зная только имя или IP-адрес web-сервера, пытаться найти уязвимости в его защите;
- модель «белого ящика» – аудитор обладает полным знанием о структуре исследуемой сети. Например, аудитор может обладать картами и диаграммами сегментов исследуемой сети, списками ОС и приложений. Применение данной модели не в полной мере имитирует реальные действия злоумышленника, но позволяет, тем не менее, представить «худший» сценарий, когда атакующий обладает полным знанием о сети. Кроме того, это позволяет построить сценарий активного аудита таким образом, чтобы инструментальные тесты имели минимальные последствия для АИС и не нарушали её нормальной работы;
- модель «серого ящика» или «хрустального ящика» – аудитор имитирует действия внутреннего пользователя АИС, обладающего учётной записью доступа в сеть с определённым уровнем полномочий. Данная модель позволяет оценить риски, связанные с внутренними угрозами, например, от

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

Аудиторы должны согласовывать каждый тест, модель знания, применяемую в тесте, и возможные негативные последствия теста с лицами, заинтересованными в непрерывной работе АИС (руководителями, администраторами системы и др.).

По результатам инструментальной проверки проводится пересмотр результатов предварительного анализа и, возможно, организуется дополнительное обследование (рис. 4).

Рис. 4. Схема проведения активного аудита ИБ

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

По результатам активного аудита создаётся аналитический отчёт, состоящий из описания текущего состояния технической части СОИБ, списка найденных уязвимостей АИС со степенью их критичности и результатов упрощённой оценки рисков, включающей модель нарушителя и модель угроз.

Дополнительно может быть разработан план работ по модернизации технической части СОИБ, состоящий из перечня рекомендаций по обработке рисков.

Экспертный аудит

Экспертный аудит предназначен для оценивания текущего состояния ИБ на нормативно-методологическом, организационно-управленческом и процедурном уровнях. Экспертный аудит проводится преимущественно внешними аудиторами, его выполняют силами специалистов по системному управлению. Сотрудники организации-аудитора совместно с представителями заказчика проводят следующие виды работ:

- сбор исходных данных об АИС, её функциях и особенностях, используемых технологиях автоматизированной обработки и передачи информации (с учётом ближайших перспектив развития);
- сбор информации об имеющихся организационно-распорядительных

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

- определение защищаемых активов, ролей и процессов СОИБ.

Важнейшим инструментом экспертной оценки является сбор данных об АИС путём интервьюирования технических специалистов и руководства заказчика.

Основные цели интервьюирования руководящего состава организации:
- определение политики и стратегии руководства в вопросах обеспечения ИБ;
- выявление целей, которые ставятся перед СОИБ;
- выяснение требований, которые предъявляются к СОИБ;
- получение оценок критичности тех или иных подсистем обработки информации, оценок финансовых потерь при возникновении тех или иных инцидентов.

Основные цели интервьюирования технических специалистов:
- сбор информации о функционировании АИС;
- получение схемы информационных потоков в АИС;
- получение информации о технической части СОИБ;
- оценка эффективности работы СОИБ.

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

В рамках экспертного аудита проводится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты, различного рода положения и инструкции. Организационно-распорядительные документы оцениваются на предмет достаточности и непротиворечивости декларируемым целям и мерам ИБ, а также на предмет соответствия стратегической политике руководства в вопросах ИБ.

Результаты экспертного аудита могут содержать рекомендации по совершенствованию нормативно-методологических, организационно-управленческих и процедурных компонентов СОИБ.

2. Аудит информационной безопасности компьютерных систем

2.1. Понятие аудита информационной безопасности

Аудит на соответствие стандартам ИБ

В ряде случаев проводится аудит на соответствие стандартам ИБ. Специально уполномоченные организации-аудиторы по результатам аудита принимают решение и выдают документальное подтверждение о соответствии СОИБ тому или иному эталонному стандарту (проводят сертификацию). Сертификация является показателем качества СОИБ и поднимает престиж и уровень доверия к организации.

Аудит на соответствие стандартам чаще всего подразумевает проведение активного и экспертного аудита. По результатам могут быть подготовлены отчёты, содержащие следующую информацию:

- степень соответствия проверяемой ИС выбранным стандартам;
- количество и категории полученных несоответствий и замечаний;
- рекомендации по построению или модификации СОИБ, позволяющие привести её в соответствие с требованиями рассматриваемого стандарта.

3. Методика проведения инструментальных проверок

Инструментальные проверки (ИП) выполняются в процессе активного аудита ИБ. Как уже было отмечено, ИП состоят из набора заранее согласованных тестов, направленных на получение характеристик об уровне защищённости выбранных ПИБ. Для проведения инструментальных проверок может быть предложена следующая методика, предполагающая тестирование возможности несанкционированного доступа (НСД) к информации, обрабатываемой или хранящейся в АИС, как изнутри организации, так и из внешних сетей. Методика включает три этапа: анализ структуры АИС, внутренний аудит, внешний аудит.

На этапе анализа структуры АИС с позиций ИБ производится анализ инвентаризация информационных ресурсов и СВТ:

- формируется перечень защищаемых сведений;
- описываются информационные потоки, структура и состав АИС;
- проводится категорирование ресурсов, подлежащих защите.

На втором этапе осуществляется внутренний аудит АИС, включающий анализ настроек АИС с точки зрения ИБ. На данном этапе с учётом известных изъянов ОС и специализированных СЗИ осуществляется анализ защищённости от опасных внутренних воздействий. Исследуется возможность несанкционированных действий легальных пользователей компьютерной сети, которые могут привести к модификации, копированию или разрушению конфиденциальных данных.

3. Методика проведения инструментальных проверок

Анализ осуществляется путём детального изучения настроек безопасности средств защиты с использованием как общеупотребимых (в том числе входящих в арсенал хакеров), так и специально разработанных автоматизированных средств исследования уязвимости АИС. Анализируются следующие компоненты АИС:

- средства защиты ПК – возможность отключения программно-аппаратных систем защиты при физическом доступе к выключенным станциям; использование и надёжность встроенных средств парольной защиты BIOS;
- состояние антивирусной защиты – наличие в АИС вредоносных программ, возможность их внедрения через машинные носители, сеть Интернет;
- ОС – наличие требуемых настроек безопасности;
- парольная защита в ОС – возможность получения файлов с зашифрованными паролями и их последующего дешифрования; возможность подключения с пустыми паролями, подбора паролей, в том числе по сети;
- система разграничения доступа пользователей АИС к ресурсам – формирование матрицы доступа; анализ дублирования и избыточности в предоставлении прав доступа; определение наиболее осведомлённых пользователей и уровней защищённости конкретных ресурсов; оптимальность формирования рабочих групп;
- сетевая инфраструктура – возможность подключения к сетевому оборудованию для получения защищаемой информации путём перехвата и анализа сетевого трафика; настройки сетевых протоколов и служб;
- аудит событий безопасности – настройка и реализация политики аудита;

3. Методика проведения инструментальных проверок

- прикладное ПО – надёжность элементов защиты используемых АРМ; возможные каналы утечки информации; анализ версий используемого программного обеспечения на наличие уязвимых мест;
- СЗИ: надёжность и функциональность используемых СЗИ; наличие уязвимых мест в защите; настройка СЗИ.

На третьем этапе осуществляется внешний аудит АИС, оценивающий состояние защищённости информационных ресурсов организации от НСД, осуществляемого из внешних сетей, в том числе из Интернет.

Последовательно анализируются следующие возможности проникновения извне:

- получение данных о внутренней структуре АИС – наличие на web-серверах информации конфиденциального характера; выявление настроек DNS- и почтового серверов, позволяющих получить информацию о внутренней структуре АИС;
- выявление компьютеров, подключённых к сети и достижимых из Интернет – сканирование по протоколам ICMP, TCP, UDP; определение степени доступности информации об используемом в АИС ПО и его версиях; выявление активных сетевых служб; определение типа и версии ОС, сетевых приложений и служб;
- получение информации об учётных записях, зарегистрированных в АИС с применением утилит, специфичных для конкретной ОС.

3. Методика проведения инструментальных проверок

- использование известных уязвимостей в программном обеспечении МЭ, выявление неверной конфигурации МЭ.
- выявление версий ОС и сетевых приложений, подверженных атакам типа «отказ в обслуживании»;
- тестирование возможности атак на сетевые приложения – анализ защищённости web-серверов, тестирование стойкости систем удалённого управления, анализ возможности проникновения через имеющиеся модемные соединения.

По результатам тестирования оформляется экспертное заключение, описывающее реальное состояние защищённости АИС от внутренних и внешних угроз, содержащее перечень найденных изъянов в настройках систем безопасности. На основании полученного заключения разрабатываются рекомендации по повышению степени защищённости АИС, по администрированию систем, по применению СЗИ.

Реализация методики требует постоянного обновления знаний об обнаруживаемых изъянах в системах защиты. Не все этапы методики могут быть автоматизированы. Во многих случаях требуется участие эксперта, обладающего соответствующей квалификацией.