В.И. Аверченков

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

2-е издание, стереотипное

Москва
Издательство «ФЛИНТА»
2011

УДК 004.732.056.5
А19

Р е ц е н з е н т ы:
кафедра «Защита информации» Воронежского
государственного технического университета;
доктор технических наук профессор *И.С. Константинов*

Аверченков В.И.
А19 Аудит информационной безопасности : учеб. пособие для вузов [электронный ресурс] / В.И. Аверченков. – 2-е изд., стереотип. – М. : ФЛИНТА, 2011. – 269 с.

ISBN 978-5-9765-1256-6

Рассмотрен комплекс вопросов, связанных с проведением аудита информационной безопасности на предприятии, даны основные понятия, показана роль анализа и управления информационными рисками. Проведено описание международных и российских стандартов информационной безопасности, изложены методологические основы применения стандартов ISO 15408 и ISO 17799 для оценки и управления безопасностью информационных технологий, дана характеристика программных средств, применяемых при аудите информационной безопасности. Особое внимание уделено практическим вопросам методики проведения аудита информационной безопасности на предприятии.

Учебное пособие предназначено для студентов, обучающихся по специальности «Организация и технология защиты информации», а также может быть полезно специалистам, занимающимся организационными вопросами защиты информации на предприятиях.

УДК 004.732.056.5

ISBN 978-5-9765-1256-6

ПРЕДИСЛОВИЕ

Аудит – форма независимого, нейтрального контроля какого-либо направления деятельности коммерческого предприятия, широко используемая в практике рыночной экономики, особенно в сфере бухгалтерского учета. Не менее важным с точки зрения общего развития предприятия является его аудит безопасности, который включает анализ рисков, связанных с возможностью осуществления угроз безопасности, особенно в отношении информационных ресурсов, оценку текущего уровня защищенности информационных систем (ИС), локализацию узких мест в системе их защиты, оценку соответствия ИС существующим стандартам в области информационной безопасности и выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Если говорить о главной цели аудита информационной безопасности, то можно ее определить как **проведение оценки уровня безопасности информационной системы предприятия для управления им в целом с учетом перспектив его развития.**

В современных условиях, когда информационные системы пронизывают все сферы деятельности предприятия, а с учетом необходимости их связи с Интернет они оказываются открытыми для реализации внутренних и внешних угроз, проблема информационной безопасности становится не менее важной, чем экономическая или физическая безопасность.

Несмотря на важность рассматриваемой проблемы для подготовки специалистов по защите информации, она до настоящего времени не была включена в виде отдельного курса в существующие учебные планы и не рассматривалась в учебниках и учебных пособиях. Это было связано с отсутствием необходимой нормативной базы, неподготовленностью специалистов и недостаточным практическим опытом в области проведения аудита информационной безопасности.

В последние годы в России наблюдается активное внедрение международных стандартов по информационной безопасности BS 7799, ISO 17799, ISO 15408, создаются отечественные стандарты, которые сегодня могут быть основой методологии проведения аудита безопасности.

Предлагаемое учебное пособие написано на основе курса лекций, читаемых студентам по специальности «Организация и технология защиты информации» и с учетом существующих требований к их подготовке и ориентировано преимущественно на рассмотрение методических и организационных основ проведения аудита информационной безопасности на предприятии. Общая структура пособия включает следующую последовательность рассматриваемых вопросов:

- описывается модель построения системы информационной безопасности (ИБ), учитывающая угрозы, уязвимости, риски и принимаемые для их снижения или предотвращения контрмеры;
- рассматриваются методы анализа и управления рисками;
- излагаются базовые понятия аудита безопасности и дается характеристика целей его проведения;
- анализируются основные международные и российские стандарты, используемые при проведении аудита ИБ;
- приводится механизм оценки безопасности информационных технологий на основе «общих критериев» (стандарт ISO 15408);
- даются конкретные рекомендации по использованию международного стандарта управления информационной безопасностью ISO 17799;
- показываются возможности использования программных средств для проведения аудита ИБ;
- даются практические рекомендации по проведению аудита ИБ на предприятии.

Выбор описанной структуры учебного пособия был сделан с целью максимальной ориентации студента на практическое использование рассматриваемого материала, во-первых, при изучении лекционного курса, во-вторых, при прохождении производственных практик (анализ состояния информационной безопасности на предприятии), в-третьих, при выполнении курсовых и дипломных работ.

Представленный материал может быть полезен руководителям и сотрудникам служб безопасности и служб защиты информации предприятия для подготовки и проведения внутреннего и обоснования необходимости внешнего аудита информационной безопасности.

Глава 1. Основы построения систем информационной безопасности

1.1. Цель и задачи информационной безопасности (ИБ)

Использование автоматизированных систем во всех сферах деятельности человека, основанных на применении современных информационно-коммуникационных технологий, выдвинуло целый ряд проблем перед разработчиками и пользователями этих систем. Одна из наиболее острых проблем – проблема информационной безопасности, которую необходимо обеспечивать, контролировать, а также создавать условия для ее управления.

Главной целью любой системы обеспечения информационной безопасности является создание условий функционирования предприятия, предотвращение угроз его безопасности, защита законных интересов предприятия от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение в рамках производственной деятельности всех подразделений предприятия.

Более детальное рассмотрение этой проблемы позволяет сформулировать основные **задачи любой системы ИБ** предприятия [10]:

- необходимость отнесения определенной информации к категории ограниченного доступа (служебной или коммерческой тайне);
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий,

способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы ИБ и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения ИБ.

1.2. Угрозы ИБ и их источники

Центральным понятием ИБ является понятие «угроза».

В соответствии с определением словаря русского языка С.И. Ожегова под угрозой понимается «намерение нанести физический, материальный или иной вред общественным или личным интересам, возможная опасность».

В современной литературе большинство авторов публикаций угрозу безопасности информации отождествляют либо с характером (видом, способом) дестабилизирующего воздействия на информацию, либо с последствиями (результатами) такого воздействия в виде ущерба, понесенного субъектом в результате нарушения его прав.

Категория «ущерб» справедлива только в том случае, когда можно доказать, что он причинен, то есть деяния, приводящие к ущербу, можно квалифицировать в терминах правовых актов как состав преступления. Поэтому при определении угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права (Уголовный кодекс РФ, 1996г.), определяющего состав преступления. В рассматриваемом случае к таким преступлениям можно отнести:

- *хищение* – совершенные с корыстной целью противоправные

безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или владельцу имущества;

- *копирование компьютерной информации* – повторение и устойчивое запечатление информации на машинном или ином носителе;
- *уничтожение* – внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводится в полную непригодность для использования по целевому назначению.
- *уничтожение компьютерной информации* – стирание ее в памяти ЭВМ;
- *повреждение* – изменение свойств имущества, при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования;
- *модификация компьютерной информации* – внесение любых изменений, связанных с адаптацией программы для ЭВМ или баз данных;
- *блокирование компьютерной информации* – искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением;
- *несанкционированное уничтожение, блокирование, модификация, копирование информации* – любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией;
- *обман (отрицание подлинности, навязывание ложной информации)* – умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество, и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью ложных сведений.

Обобщая изложенное, в дальнейшем под **угрозами будем понимать *потенциальную* или *реально существующую опасность совершения какого-либо деяния* (действия или бездействия), направленного против объекта защиты, наносящего ущерб собственнику (владельцу, пользователю) информационных ресурсов, проявляющегося в опасности искажения и/или потери информации, либо неправомерного ее использования**.

Угрозы сами по себе не проявляются. Все угрозы могут быть реализованы только при наличии каких-нибудь слабых мест – *уязвимостей,* присущих объекту информатизации.

Уязвимость – некая слабость, которую можно использовать для нарушения информационной автоматизированной системы или содержащейся в ней информации. (ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Архитектура защиты информации»).

Особое внимание при рассмотрении ИБ должно уделяться источникам угроз.

В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Причем сами источники угроз могут находиться как внутри объекта информатизации – внутренние, так и вне его – внешние.

В качестве **источников угроз** могут быть:

- действия субъекта (антропогенные источники угроз);
- технические средства (техногенные источники угрозы);
- стихийные источники.

К *антропогенным* источникам угроз относятся субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления.

К *техногенным* источникам угроз относятся источники, определяемые технократической деятельностью человека и развитием цивилизации.

К *стихийным* источникам угроз относятся стихийные бедствия или иные обстоятельства, которые невозможно или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей.

Анализ угроз ИБ показывает, что они могут быть разделены на два вида: внутренние и внешние.

Внутренние угрозы безопасности объекта защиты:

- неквалифицированная корпоративная политика по организации информационных технологий и управлению безопасностью корпорации;
- отсутствие должной квалификации персонала по обеспечению деятельности и управлению объектом защиты;
- преднамеренные и непреднамеренные действия персонала по

нарушению безопасности;

- техногенные аварии и разрушения, пожары.

Внешние угрозы безопасности объекта защиты:

- негативные воздействия недобросовестных конкурентов и государственных структур;
- преднамеренные и непреднамеренные действия заинтересованных структур и лиц (сбор информации, шантаж, искажение имиджа, угрозы физического воздействия и др.);
- утечка конфиденциальной информации из носителей информации и обусловленных каналов связи;
- несанкционированное проникновение на объект защиты;
- несанкционированный доступ к носителям информации и обусловленным каналам связи с целью хищения, искажения, уничтожения, блокирования информации;
- стихийные бедствия и другие форс-мажорные обстоятельства;
- преднамеренные и непреднамеренные действия системных интеграторов и поставщиков услуг по обеспечению безопасности, поставщиков технических и программных продуктов, кадров.

При комплексном подходе к анализу угроз ИБ объекта информатизации необходимо провести:

- описание объекта;
- классификацию источников угроз;
- классификацию уязвимостей;
- классификацию методов реализации угроз;
- ранжирование актуальных атак;
- классификацию методов парирования угроз.

Структурированное описание объекта информатизации, представленное в виде типовых структурных компонентов информационной системы и связей между ними, характеризующих направления циркуляции и параметры потоков информации в совокупности с текстовыми пояснениями, позволяет выявить точки возможного применения угроз или вскрыть существующие уязвимости.

Анализ и оценка возможностей реализации угроз должны быть основаны на построении модели угроз, классификации, анализе и оценки источников угроз, уязвимостей и методов реализации. Моделирование процессов нарушения информационной безопасности

может осуществляться на основе рассмотрения логической цепочки: *угроза – источник угрозы – метод реализации – уязвимость – последствия* (рис.1.1). Каждый компонент рассматриваемой логической цепочки целесообразно описывается с необходимой подробностью.

Угрозы классифицируются по возможности нанесения ущерба при нарушении целей информационной безопасности; *источники угроз* – по типу и местоположению носителя угрозы; *уязвимости* – по принадлежности к источнику уязвимостей, возможным проявлениям.

Классификация атак представляет собой *совокупность* возможных вариантов действий источника угроз определенными методами реализации с использованием уязвимостей, которые приводят к реализации целей атаки. Цель атаки может не совпадать с целью реализации угроз и быть направлена на получение промежуточного результата, необходимого для достижения в дальнейшем реализации угрозы. В случае несовпадения целей атаки с целью реализации угрозы сама атака рассматривается как этап подготовки к совершению действий, направленных на угрозы, то есть как «подготовка к совершению» противоправного действия.

На основе проведенной классификации, ранжирования, анализа и определения актуальных *угроз, источников угроз* и *уязвимостей* определяются варианты *возможных атак,* которые позволяют оценить состояние информационной безопасности и оптимизировать *выбор методов парирования угроз.*

Методов парирования угроз достаточно много. Наиболее важными являются следующие:

- *экономические:*
  - введение системы коэффициентов и надбавок;
  - страхование оборудования и информации;
  - возмещение убытков и компенсация ущерба.
- *организационные:*
  - физическая защита и организация охраны;
  - подбор и работа с персоналом;
  - организация инструктажа персонала;
  - выбор и работа с партнерами;
  - контроль выполнения требований по защите;
  - противопожарная охрана;
  - организация взаимодействия с компетентными органами;

Рис. 1.1. **Модель реализации угроз информационной безопасности [10]**

- *инженерно-технические:*
  - создание электрозащиты оборудования и зданий;
  - экранирование помещений;
  - применение средств визуальной защиты;
  - акустическая обработка помещений.
- *технические:*
  - резервирование технических средств обработки;
  - резервирование каналов связи;
  - использование выделенных каналов связи;
  - создание резервной копии (дублирование);
  - создание систем акустического зашумления;
  - экранирование узлов и оборудования;
  - использование источников гарантированного питания;
  - контроль каналов связи;
  - контроль отсутствия средств съема информации.
- *программно-аппаратные:*
  - ограничение доступа к средствам обработки;
  - ограничение доступа к объектам (информации, ПО);
  - разграничение доступа субъектов (пользователей);
  - управление внешними потоками информации;
  - управление внутренними потоками информации;
  - подтверждение подлинности информации;
  - преобразование информации при ее передаче и хранении;
  - мониторинг атак и разрушающих воздействий;
  - мониторинг действий субъектов и др.

1.3. Модель построения системы информационной безопасности

При выполнении работ по защите информации может быть принята следующая модель построения системы ИБ, основанная на рассмотрении угроз, уязвимости и связанного с ними риска (рис. 1.2.).

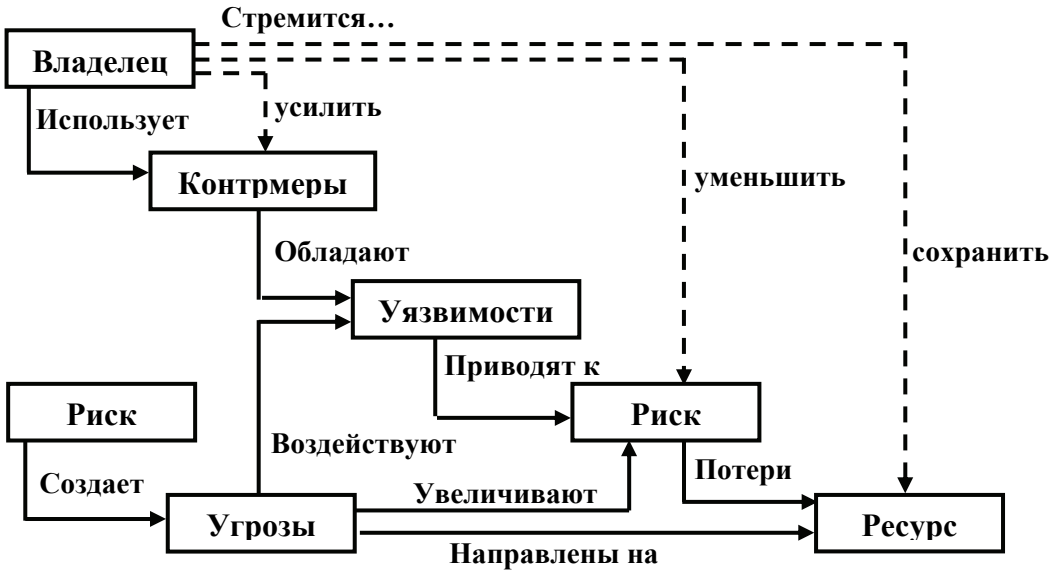

Рис. 1.2. **Модель построения системы информационной безопасности [10]:** ⟶ естественное воздействие; ⇢ управляющее воздействие

Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации и соответствующим международному стандарту ISO 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», а также стандарту ISO 17799 «Управление информационной безопасностью» и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам информационной безопасности.

Представленная модель ИБ – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Здесь рассматриваются следующие объективные факторы [10]:

- *угрозы информационной безопасности,* характеризующиеся вероятностью возникновений и вероятностью реализации;
- *уязвимости* информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- *риск* – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном

итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предприятия предполагается первоначально провести анализ информационных рисков (рассмотрено в следующей главе). Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Реализация рассмотренной модели построения системы ИБ позволяет:

- полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказать помощь в планировании и защите на всех стадиях жизненного цикла информационных систем;
- обеспечить проведение работ в сжатые сроки;
- предоставить обоснование для выбора мер противодействия;
- оценить эффективность контрмер, сравнить различные варианты контрмер.

1.4. Разработка концепции обеспечения ИБ

Современный подход к обеспечению безопасности требует создания целостной системы ИБ, включающей в себя комплекс организационных, правовых, инженерно-технических и программно-аппаратных мер защиты, использующей современные методы прогнозирования, анализа и моделирования постоянно изменяющихся ситуаций.

С этой целью для конкретного предприятия при построении системы ИБ необходима разработка **концепции обеспечения информационной безопасности** (далее **концепция**), в которой на основе анализа современного достигнутого уровня и динамики развития информационных технологий, ожидаемых угроз ИБ, источников этих угроз и факторов, способствующих их реализации, дается систематизированное изложение целей, задач и принципов достижения требуемого

уровня информационной безопасности (рис. 1.3).

Концепция должна учитывать современные тенденции развития единого информационного пространства России, сложившейся международной и внутриполитической обстановки, требования отечественных и зарубежных стандартов, законодательных актов и нормативно-методических документов по вопросам защиты информации, действующих в Российской Федерации.

Таким образом, концепция представляет собой нормативный документ, отражающий официально принятую систему взглядов на проблему обеспечения информационной безопасности и пути ее решения с учетом современных тенденций развития информатизации.

Концепция определяет генеральную линию в решении проблем информационной безопасности, а не сиюминутные, временные взгляды. Это не технический проект системы информационной безопасности, не набор конкретных средств защиты корпоративной сети, а именно изложение путей достижения поставленных целей информационной безопасности, которые должны реализовываться посредством продуманной, глубоко эшелонированной системы защиты – комплекса мер и средств, направленных на выявление, парирование и ликвидацию различных видов угроз информационной безопасности.

Концепция сама по себе не обеспечивает требуемого уровня

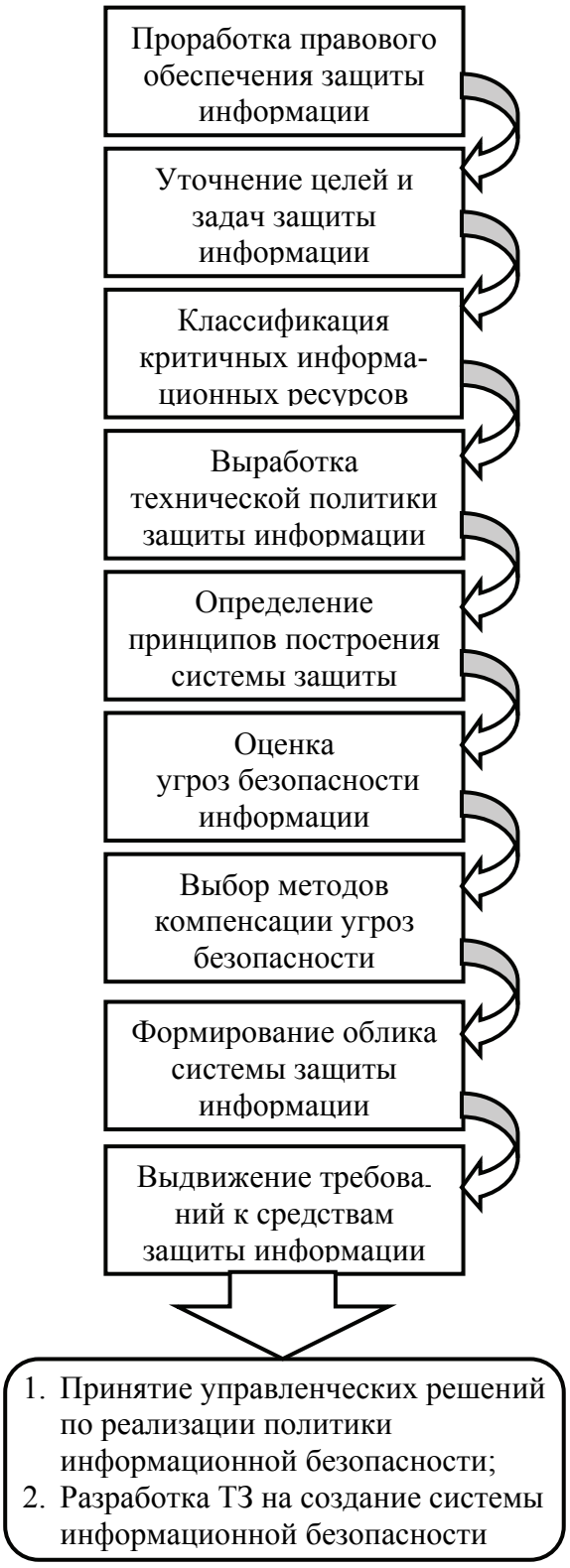

Рис. 1.3. **Структура концепции информационной безопасности**

информационной безопасности, но является методологической базой для формирования на основе определенных в ней целей, задач и возможных путей их решения единой политики в области информационной безопасности, принятия управленческих решений по реализации этой политики и выработки взаимосвязанных и согласованных мер организационного и инженерно-технического характера, координации деятельности структурных подразделений учреждения, разработки конкретных предложений по совершенствованию информационной безопасности, которые не могут свестись к простой сумме отдельных преобразований.

В обобщенном виде концепция ИБ должна включать в себя следующие основные разделы [10]:

Введение.

1. Правовое обеспечение вопросов защиты информации.

2. Цели и задачи защиты информации.

3. Информация, подлежащая защите.

4. Техническая политика и принципы построения защиты.

5. Модель угроз информационной безопасности.

5.1. Описание сети.

5.2. Классификация источников угроз (антропогенные, техногенные, стихийные, ранжирование).

5.3. Классификация уязвимостей (объективные, субъективные, случайнее, ранжирование).

5.4. Классификация методов реализации угроз.

5.5. Ранжирование актуальных атак.

5.6. Классификация методов парирования угроз (правовые, экономические, организационные, инженерно-технические, технические, программно-аппаратные).

6. Выбор уровней защиты.

6.1. Выбор категорий защиты объектов информатизации.

6.2. Примерный перечень объектов защиты и их категорий.

6.3. Выбор класса защищенности информационной сети.

7. Облик системы защиты информации.

7.1. Начальные условия.

7.2. Описание подсистемы защиты информации (технологический, пользовательский, локальный сегментный, сетевой внешний уровень защиты).

7.3. Структура и состав подсистемы информационной безопасности (субсистемы управления доступом, аудита и мониторинга, защиты периметра, распределения ключей, вспомогательная).

8. Защита помещений и технических средств.

8.1. Построение защищенных помещений.

8.2. Размещение технических средств.

8.3. Использование вспомогательных технических средств.

8.4. Оборудование рабочего места администратора безопасности.

9. Порядок аттестации объектов информатизации.

10. Порядок контроля эффективности защиты.

Заключение.

В качестве приложений к *Концепции* могут быть даны:

- Основные термины и определения;
- Методика оценки и анализа возможностей реализации угроз;
- Рекомендации по разработке перечня сведений ограниченного доступа;
- Примерный перечень сведений ограниченного доступа;
- Требования к программно-аппаратным средствам защиты информации;
- Требования к размещению вспомогательных технических средств;
- Программа развития и совершенствования информационной безопасности;
- Руководство по обеспечению информационной безопасности.

Приложения составляют наиболее мобильную часть концепции, которая может дополняться и изменяться (без изменения основного замысла и идеи обеспечения информационной безопасности) по мере изменения требований действующих стандартов и нормативных документов.

Контрольные вопросы

1. *Что является главной целью системы обеспечения ИБ?*
2. *Назовите основные задачи системы ИБ.*
3. *Какие виды угроз ИБ встречаются наиболее часто?*
4. *Приведите примеры источников угроз.*
5. *Опишите основные модули модели реализации угроз ИБ.*
6. *Какие существуют методы карирования угроз?*
7. *Назвать основные компоненты модели построения системы ИБ.*
8. *С какой целью разрабатывается концепция ИБ?*
9. *Какие процедуры включает в себя схемы структуры помещения ИБ?*
10. *Из каких разделов состоит концепция ИБ?*

Глава 2. Аудит безопасности и методы его проведения

2.1. Понятие аудита безопасности

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Различают внешний и внутренний аудит. **Внешний аудит** – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Рекомендуется проводить внешний аудит регулярно, а, например, для многих финансовых организаций и акционерных обществ это является обязательным требованием со стороны их учредителей и акционеров. **Внутренний аудит** представляет собой непрерывную деятельность, которая осуществляется на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка которого осуществляется подразделениями службы безопасноти и утверждается руководством организации.

Целями проведения аудита безопасности являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов;
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Аудит безопасности предприятия (фирмы, организации) должен рассматриваться как конфиденциальный инструмент управления, исключающий в целях конспирации возможность предоставления информации о результатах его деятельности сторонним лицам и организациям.

Для проведения аудита безопасности предприятия может быть рекомендована следующая последовательность действий [7].

1 . **Подготовка к проведению аудита безопасности:**

- выбор объекта аудита (фирма, отдельные здания и помещения, отдельные системы или их компоненты);
- составление команды аудиторов-экспертов;
- определение объема и масштаба аудита и установление конкретных сроков работы.

2. **Проведение аудита:**

- общий анализ состояния безопасности объекта аудита;
- регистрация, сбор и проверка статистических данных и результатов инструментальных измерений опасностей и угроз;
- оценка результатов проверки;
- составление отчета о результатах проверки по отдельным составляющим.

3. **Завершение аудита:**

- составление итогового отчета;
- разработка плана мероприятий по устранению узких мест и недостатков в обеспечении безопасности фирмы.

Для успешного проведения аудита безопасности необходимо:

- активное участие руководства фирмы в его проведении;
- объективность и независимость аудиторов (экспертов), их компетентность и высокая профессиональность;
- четко структурированная процедура проверки;
- активная реализация предложенных мер обеспечения и усиления безопасности.

Аудит безопасности, в свою очередь, является действенным инструментом оценки безопасности и управления рисками. Предотвращение угроз безопасности означает в том числе и защиту экономических, социальных и информационных интересов предприятия.

Отсюда можно сделать вывод, что аудит безопасности становится инструментом экономического менеджмента.

В зависимости от объема анализируемых объектов предприятия определяются масштабы аудита:

– аудит безопасности всего предприятия в комплексе;

– аудит безопасности отдельных зданий и помещений (выделенные помещения);

– аудит оборудования и технических средств конкретных типов и видов;

– аудит отдельных видов и направлений деятельности: экономической, экологической, информационной, финансовой и т. д.

Следует подчеркнуть, что аудит проводится не по инициативе аудитора, а по инициативе руководства предприятия, которое в данном вопросе является основной заинтересованной стороной. Поддержка руководства предприятия является необходимым условием для проведения аудита.

Аудит представляет собой комплекс мероприятий, в которых помимо самого аудитора, оказываются задействованными представители большинства структурных подразделений компании. Действия всех участников этого процесса должны быть скоординированы. Поэтому на этапе инициирования процедуры аудита должны быть решены следующие организационные вопросы:

- права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;
- аудитором должен быть подготовлен и согласован с руководством план проведения аудита;
- в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники предприятия обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

На этапе инициирования процедуры аудита должны быть определены границы проведения обследования. Если какие-то информационные подсистемы предприятия не являются достаточно критичными, их можно исключить из границ проведения обследования.

Другие подсистемы могут оказаться недоступными для аудита из-за соображений конфиденциальности.

Границы проведения обследования определяются в следующих категориях:

1. Список обследуемых физических, программных и информационных ресурсов.
2. Площадки (помещения), попадающие в границы обследования.
3. Основные виды угроз безопасности, рассматриваемые при проведении аудита.
4. Организационные (законодательные, административные и процедурные), физические, программно-технические и прочие аспекты обеспечения безопасности, которые необходимо учесть в ходе проведения обследования, и их приоритеты (в каком объеме они должны быть учтены).

План и границы проведения аудита обсуждается на рабочем собрании, в котором участвуют аудиторы, руководство компании и руководители структурных подразделений.

Для понимания аудита ИБ как комплексной системы может быть использована его концептуальная модель, показанная на рис. 2.1. Здесь выделены главные составляющие процесса:

- объект аудита;
- цель аудита;
- предъявляемые требования;
- используемые методы;
- масштаб;
- исполнители;
- порядок проведения.

С точки зрения организации работ при проведении аудита ИБ выделяют **три принципиальных этапа**:

1) сбор информации;
2) анализ данных;
3) выработка рекомендаций и подготовка отчетных документов.

Ниже более подробно рассмотрены эти этапы.

Рис. 2.1 **. Концептуальная модель аудита ИБ [7]**

2.2. Методы анализа данных при аудите ИБ

В настоящее время используются три основных метода (подхода) к проведению аудита, которые существенно различаются между собой [3].

Первый метод, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования и существующие в данной среде угрозы безопасности. Данный подход является наиболее трудоемким и требует наивысшей квалификации аудитора. На качество результатов аудита, в этом случае, сильно влияет используемая методология анализа и управления рисками и ее применимость к данному типу ИС.

Второй метод, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленности, связь и т.п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной ИС. Необходима также методика, позволяющая оценить это соответствие. Из-за своей простоты (стандартный набор требований для проведения аудита уже заранее определен стандартом) и надежности (стандарт – есть стандарт и его требования никто не попытается оспорить), описанный подход наиболее распространен на практике (особенно при проведении внешнего аудита). Он позволяет при минимальных затратах ресурсов делать обоснованные выводы о состоянии ИС.

Третий метод, наиболее эффективный, предполагает комбинирование первых двух.

Если для проведения аудита безопасности выбран подход, базирующийся на анализе рисков, то на этапе анализа данных аудита обычно выполняются следующие группы задач [3]:

1 . Анализ ресурсов ИС, включая информационные ресурсы, программные и технические средства, а также людские ресурсы.

2. Анализ групп задач, решаемых системой, и бизнес процессов.

3. Построение (неформальной) модели ресурсов ИС, определяющей взаимосвязи между информационными, программными, техническими и людскими ресурсами, их взаимное расположение и способы взаимодействия.

4. Оценка критичности информационных ресурсов, а также программных и технических средств.

5. Определение критичности ресурсов с учетом их взаимозависимостей.

6. Определение наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз.

7. Оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз.

8. Определение величины рисков для каждой тройки: угроза – группа ресурсов – уязвимость.

Перечисленный набор задач является достаточно общим. Для их решения могут использоваться различные формальные и неформальные, количественные и качественные, ручные и автоматизированные методики анализа рисков. Суть подхода от этого не меняется.

Оценка рисков может даваться с использованием различных как качественных, так и количественных шкал. Главное, чтобы существующие риски были правильно идентифицированы и проранжированы в соответствии со степенью их критичности для организации. На основе такого анализа может быть разработана система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

При проведении аудита безопасности на соответствие требованиям стандарта, аудитор, полагаясь на свой опыт, оценивает применимость требований стандарта к обследуемой ИС и ее соответствие этим

требованиям. Данные о соответствии различных областей функционирования ИС требованиям стандарта обычно представляются в табличной форме. Из таблицы видно, какие требования безопасности в системе не реализованы. Исходя из этого, делаются выводы о соответствии обследуемой ИС требованиям стандарта и даются рекомендации по реализации в системе механизмов безопасности, позволяющих обеспечить такое соответствие. Более подробно этот метод рассмотрен в главе 4,5.

2.3. Анализ информационных рисков предприятия

Анализ рисков – это то, с чего должно начинаться построение любой системы информационной безопасности и то, что необходимо для проведения аудита ИБ. Он включает в себя мероприятия по обследованию безопасности предприятия с целью определения того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам информационных систем (ИС), в случае осуществления угрозы безопасности.

Анализ рисков состоит в том, чтобы выявить существующие риски и оценить их величину (дать им качественную, либо количественную оценку). **Процесс анализа рисков** предусматривает решение следующих задач:

1. Идентификация ключевых ресурсов ИС.
2. Определение важности тех или иных ресурсов для организации.
3. Идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз.
4. Вычисление рисков, связанных с осуществлением угроз безопасности.

Ресурсы ИС можно разделить на следующие категории:

- информационные ресурсы;
- программное обеспечение;
- технические средства (серверы, рабочие станции, активное сетевое оборудование и т. п.);

- людские ресурсы.

В каждой категории ресурсы делятся на классы и подклассы. Необходимо идентифицировать только те ресурсы, которые определяют функциональность ИС и существенны с точки зрения обеспечения безопасности.

Важность (или стоимость) ресурса определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса. Обычно рассматриваются следующие **виды ущерба:**

- данные были раскрыты, изменены, удалены или стали недоступны;
- аппаратура была повреждена или разрушена;
- нарушена целостность программного обеспечения.

Ущерб может быть нанесен организации в результате успешного осуществления следующих видов угроз безопасности:

- локальные и удаленные атаки на ресурсы ИС;
- стихийные бедствия;
- ошибки, либо умышленные действия персонала ИС;
- сбои в работе ИС, вызванные ошибками в программном обеспечении или неисправностями аппаратуры.

Величина риска может быть определена на основе стоимости ресурса, вероятности осуществления угрозы и величины уязвимости по следующей формуле [17]:

$$\textit{Риск} = \frac{(\textit{стоимость ресурса} \times \textit{вероятность угрозы})}{\textit{величина уязвимости}}$$

Задача управления рисками заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины. Стоимость реализации контрмер должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть обратно пропорциональна вероятности причинения ущерба.

Подход на основе анализа информационных рисков предприятия является наиболее значимым для практики обеспечения информационной безопасности. Это объясняется тем, что анализ риска позволяет эффективно управлять ИБ предприятия. Для этого в начале

работ по анализу риска необходимо определить, что именно подлежит защите на предприятии, воздействию каких угроз это подвержено, и выработать рекомендации по практике защиты.

Анализ риска производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера.

Одной из важнейших задач в рамках защиты информации является обеспечение ее целостности и доступности. При этом следует иметь в виду, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин:

- сбоев оборудования, ведущих к потере или искажению информации;
- физических воздействии, в том числе в результате стихийных бедствий;
- ошибок в программном обеспечении (в том числе недокументированных возможностей).

Поэтому под термином «атака» более перспективно понимать не только человеческие воздействия на информационные ресурсы, но и воздействия окружающей среды, в которой функционирует система обработки информации предприятия [10].

При проведении анализа риска разрабатываются:

- общая стратегия и тактика проведения потенциальным нарушителем «наступательных операций и боевых действий»;
- возможные способы проведения атак на систему обработки и защиты информации;
- сценарий осуществления противоправных действий;
- характеристики каналов утечки информации и НСД;
- вероятности установления информационного контакта (реализации угроз);
- перечень возможных информационных инфекций;
- модель нарушителя;
- методика оценки информационной безопасности.

Кроме того, для построения надежной системы защиты информации предприятия необходимо:

- выявить все возможные угрозы безопасности информации;
- оценить последствия их проявления;

- определить необходимые меры и средства защиты с учетом требований нормативных документов, экономической целесообразности, совместимости и бесконфликтности с используемым программным обеспечением;
- оценить эффективность выбранных мер и средств защиты.

Анализ риска рекомендуется проводить согласно следующей методике по сценарию, изображенному на рис. 2.2.

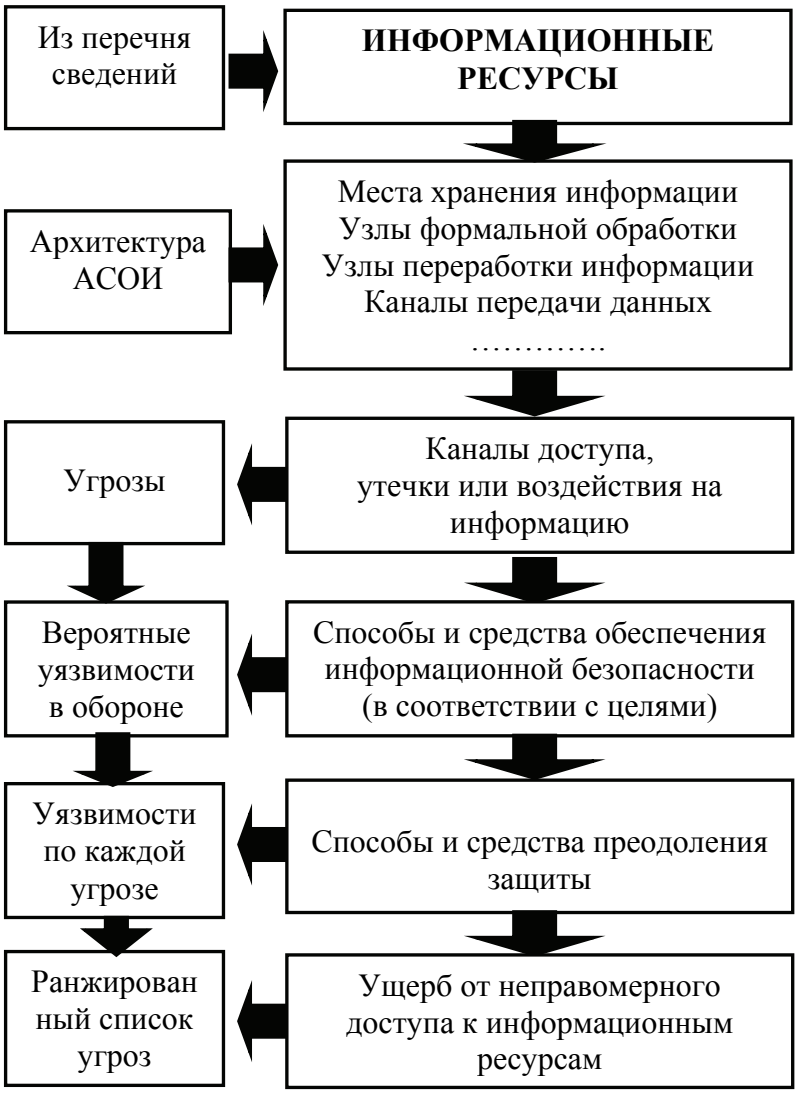

Рис. 2.2. **Сценарий анализа информационных ресурсов [10]**

Здесь представлены все 6 этапов анализа риска. На *первом* и *втором этапах* определяются сведения, которые составляют для предприятия коммерческую тайну и которые предстоит защищать. Понятно, что такие сведения хранятся в определенных местах и на конкретных носителях, передаются по каналам связи. При этом определяющим фактором в технологии обращения с информацией является архитектура ИС, которая во многом определяет защищенность информационных ресурсов предприятия.

Третий этап анализа риска – построение каналов доступа, утечки или воздействия на информационные ресурсы основных узлов ИС. Каждый канал доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они и представляют уязвимости и требуют

применения средств недопущения нежелательных воздействий на информацию.

Четвертый этап анализа способов защиты всех возможных точек атак соответствует целям защиты и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств.

На пятом этапе исходя из известных на данный момент способов и средств преодоления оборонительных рубежей определяются вероятности реализации угроз по каждой из возможных точек атак.

На заключительном, шестом, этапе оценивается ущерб организации в случае реализации каждой из атак, который вместе с оценками уязвимости позволяет получить ранжированный список угроз информационным ресурсам.

Результаты работы представляются в виде, удобном для их восприятия и выработки решений по коррекции существующей системы защиты информации. При этом каждый информационный ресурс может быть подвержен воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

Величина информационного риска по каждому ресурсу определяется как произведение вероятности нападения на ресурс, вероятности реализации и угрозы и ущерба от информационного вторжения. В этом произведении могут использоваться различные способы взвешивания составляющих.

Сложение рисков по всем ресурсам дает величину суммарного риска при принятой архитектуре ИС и внедренной в нее системы защиты информации.

Таким образом, варьируя варианты построения системы защиты информации и архитектуры ИС, становится возможным представить и рассмотреть различные значения суммарного риска за счет изменения вероятности реализации угроз. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с отобранным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение информационной безопасности к остаточному риску.

При построении систем обеспечения информационной безопасности также нужно определить стратегию управления рисками на предприятии.

На сегодня известно несколько подходов к управлению рисками. Один из наиболее распространенных – *уменьшение риска* путем использования соответствующих способов и средств защиты. Близким по сути является подход, связанный с *уклонением от риска.* Известно, что от некоторых классов рисков можно уклониться: например, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Наконец, в некоторых случаях допустимо *принятие риска.* Здесь важно определиться со следующей дилеммой: что для предприятия выгоднее – бороться с рисками или же с их последствиями. В этом случае приходится решать оптимизационную задачу.

После того как определена стратегия управления рисками, производится окончательная оценка мероприятий по обеспечению информационной безопасности с подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение включаются все материалы анализа рисков и рекомендации по их снижению.

2.4. Методы оценивания информационных рисков предприятия

На практике используются различные методы оценки и управления информационными рисками на предприятиях. При этом **оценка информационных рисков** предусматривает выполнение следующих этапов [10]:

- идентификация и количественная оценка информационных ресурсов предприятий, значимых для бизнеса;
- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании предприятия подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которой могут подвергаться компоненты корпоративной системы Internet/Intranet. При этом информационные риски компании зависят:

- от показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения ИБ.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень ИБ предприятия. При оценивании рисков учитываются ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например при определении стоимостных характеристик, так и, качественными, например учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса предприятия. При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

- привлекательностью ресурса – используется при рассмотрении угрозы от умышленного воздействия со стороны человека;
- возможностью использования ресурса для получения дохода – при рассмотрении угрозы от умышленного воздействия со стороны человека;
- техническими возможностями реализации угрозы – применяется при умышленном воздействии со стороны человека;
- степенью легкости, с которой уязвимость может быть использована.

В настоящее время известно множество табличных методов оценки информационных рисков компании. Важно, чтобы работники

службы безопасности выбрали для себя подходящий метод, который обеспечивал бы корректные и достоверные воспроизводимые результаты.

Количественные показатели информационных ресурсов рекомендуется оценивать по результатам опросов сотрудников предприятия – владельцев информации, то есть должностных лиц, которые могут определить ценность информации, ее характеристики и степень критичности, исходя из фактического положения дел. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий вплоть до рассмотрения потенциальных воздействий на бизнес-деятельность предприятия при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении ее целостности, недоступности на различные сроки, вызванных отказами в обслуживании систем обработки данных и даже физическом уничтожении. При этом процесс получения количественных показателей может дополняться соответствующими методиками оценивания других критически важных ресурсов предприятия, учитывающих [10]:

- безопасность персонала;
- разглашение частной информации;
- требования по соблюдению законодательных и нормативных положений;
- ограничения, вытекающие из законодательства;
- коммерческие и экономические интересы;
- финансовые потери и нарушения в производственной деятельности;
- общественные отношения;
- коммерческую политику и коммерческие операции;
- потерю репутации компании.

Далее количественные показатели используются там, где это допустимо и оправдано, а качественные – где количественные оценки по ряду причин затруднены. При этом наибольшее распространение получило оценивание качественных показателей при помощи специально разработанных для этих целей балльных шкал, например, с четырехбальной шкалой.

Следующей операцией является заполнение пар опросных листов, в которых по каждому из типов угроз и связанной с ним группе ресурсов оцениваются уровни угроз как вероятность реализации угроз и уровни уязвимостей как степень легкости, с которой реализованная угроза способна привести к негативному воздействию. Оценивание производится в качественных шкалах. Например, уровень угроз и уязвимостей оценивается по шкале «высокий-низкий». Необходимую информацию собирают, опрашивая TOP-менеджеров компании, сотрудников коммерческих, технических, кадровых и сервисных служб, выезжая на места и анализируя документацию компании.

Наряду с табличными методами оценки информационных рисков, могут быть использованы современные математические методы, например метод типа Дельфи, а также специальные автоматизированные системы, отдельные из которых будут рассмотрены ниже.

Общий алгоритм процесса оценивания рисков (рис. 2.3.) в этих системах включает следующие этапы.

- описание объекта и мер защиты;
- идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес);
- анализ угроз информационной безопасности;
- оценивание уязвимостей;
- оценивание существующих и предполагаемых средств обеспечения информационной безопасности;
- оценивание рисков.

2.5. Управление информационными рисками

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Его основная задача – объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность

используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности предприятия. Поэтому под термином **«управление информационными рисками»** обычно понимается системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями российской нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности.

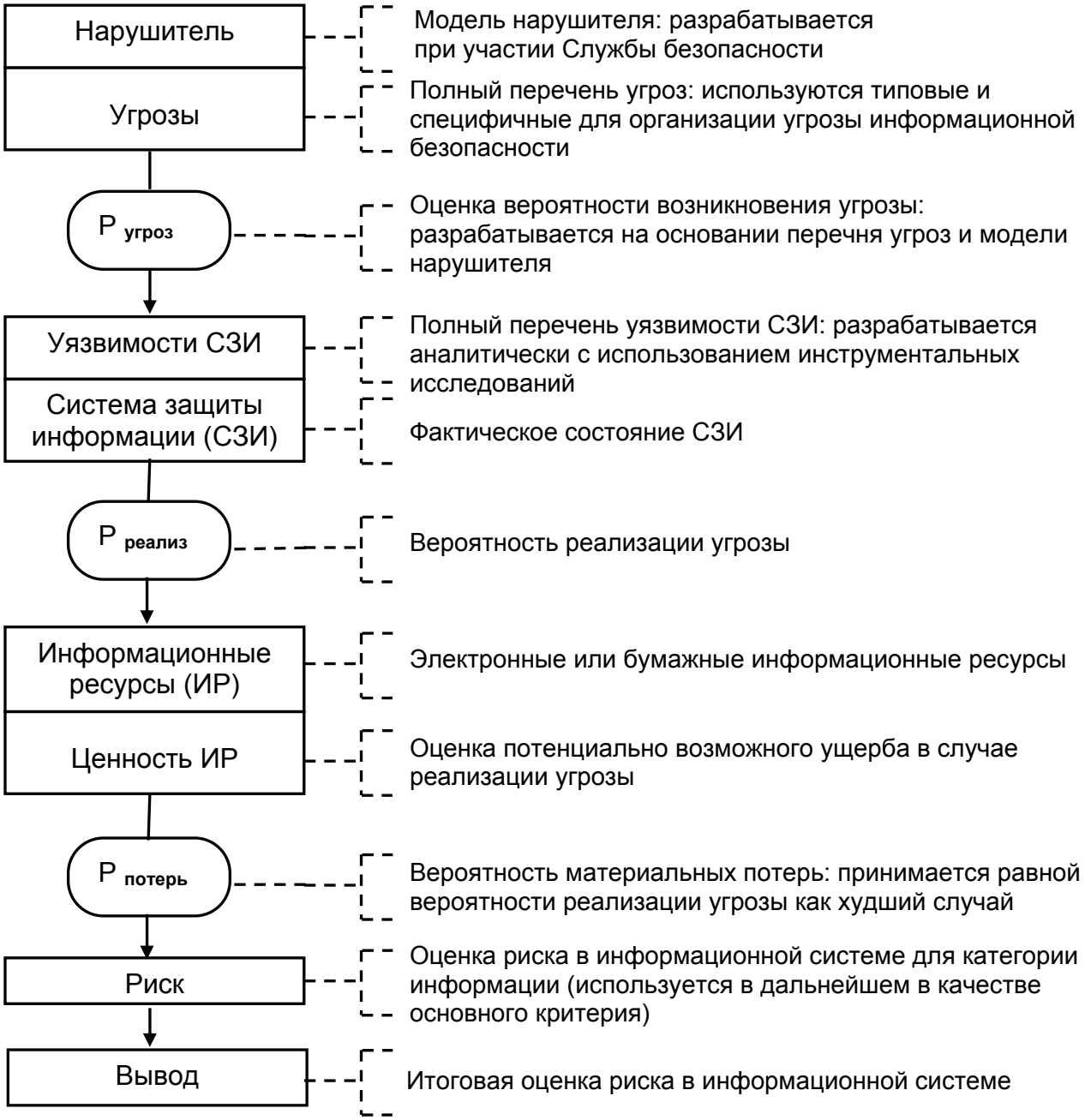

Рис. 2.3. **Алгоритм оценивания рисков [10]**

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

Суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

1) (пере)оценка (измерение) рисков;
2) выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (путем выработки плана действия в соответствующих условиях):
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.

8. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Следует отметить, что выполненная и тщательно документированная оценка может существенно упростить последующую деятельность.

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты – минимальными.

Управление рисками необходимо проводить на всех этапах жизненного цикла информационной системы: ***инициация – разработка – установка – эксплуатация – утилизация (вывод из эксплуатации)***.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе разработки знание рисков помогает выбирать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности.

На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.

При выведении системы из эксплуатации управление рисками помогает убедиться в том, что миграция данных происходит безопасным образом.

Контрольные вопросы

1. В чем отличие и особенности проведения внешнего и внутреннего аудита?

2. Назовите основные цели проведения аудита ИБ.

3. Какая последовательность действий при проведении аудита ИБ на предприятии?

4. Чем определяются масштабы аудита ИБ?

5. С какой целью проводится анализ рисков?

6. Назовите задачи, решаемые при анализе рисков.

7. Как может быть оценена величина риска?

8. Какие этапы включает сценарий анализа информационных ресурсов?

9. В чем состоит суть (подходы) управления рисками?

10. По каким показателям проводится оценивание информационных рисков?

11. Содержание алгоритма оценивания рисков.

12. Назовите этапы процесса управления рисками.

Глава 3. Стандарты информационной безопасности

3.1. Предпосылки создания стандартов ИБ

Проведение аудита информационной безопасности основывается на использовании многочисленных рекомендаций, которые изложены преимущественно в международных стандартах ИБ.

Одним из результатов проведения аудита в последнее время все чаще становится сертификат, удостоверяющий соответствие обследуемой ИС определенному признанному международному стандарту. Наличие такого сертификата позволяет организации получать конкурентные преимущества, связанные с большим доверием со стороны клиентов и партнеров.

Использование стандартов способствует решению следующих пяти задач.

Во-первых, строго определяются цели обеспечения информационной безопасности компьютерных систем. **Во-вторых**, создается эффективная система управления информационной

безопасностью. **В-третьих**, обеспечивается расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям. **В-четвертых**, создаются условия применения имеющегося инструментария (программных средств) обеспечения информационной безопасности и оценки ее текущего состояния. **В-пятых**, открывается возможность использования методик управления безопасностью с обоснованной системой метрик и мер обеспечения разработчиков информационных систем.

Начиная с начала 80-х годов были созданы десятки международных и национальных стандартов в области информационной безопасности, которые в определенной мере дополняют друг друга. Ниже будут рассмотрены наиболее известные стандарты по хронологии их создания:

1) Критерий оценки надежности компьютерных систем «Оранжевая книга» (США);
2) Гармонизированные критерии европейских стран;
3) Рекомендации X.800;
4) Германский стандарт BSI;
5) Британский стандарт BS 7799;
6) Стандарт ISO 17799;
7) Стандарт «Общие критерии» ISO 15408;
8) Стандарт COBIT

Эти стандарты можно разделить на два вида:

- Оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;
- Технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Важно отметить, что между этими видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

3.2. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем».

Данный труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о **доверенных системах**, то есть системах, которым можно оказать определенную степень доверия.

«Оранжевая книга» поясняет понятие безопасной системы, которая «*управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию*».

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В «Оранжевой книге» доверенная система определяется как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

Следует отметить, что в рассматриваемых критериях и безопасность и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности информации. При этом вопросы доступности «Оранжевая книга» не затрагивает.

Степень доверия оценивается по двум основным критериям [4].

1. **Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию**. В частности, правила определяют, в каких случаях пользователь может оперировать

конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

2. **Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС**. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Основным средством обеспечения безопасности определяется механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации. Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база – это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Рассматриваемые компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС авторы стандарта рекомендуют рассматривать только ее вычислительную базу.

Основное назначение доверенной вычислительной базы – выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (пользователями) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам

или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. **Ядро безопасности** – это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют **периметром безопасности**. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию «периметр безопасности» все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, – нет.

Согласно «Оранжевой книге», политика безопасности должна обязательно включать в себя следующие элементы [4]:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом – это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов – важное дополнение средств управления доступом, предохраняющее от

случайного или преднамеренного извлечения конфиденциальной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются **метки безопасности**. **Метка субъекта** описывает его благонадежность, **метка объекта** – степень конфиденциальности содержащейся в нем информации.

Согласно «Оранжевой книге», метки безопасности состоят из двух частей – уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, а списки категорий – неупорядоченное. Назначение последних – описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен – читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, «конфиденциальный» субъект может записывать данные в секретные файлы, но не может – в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов объектов, оказываются зафиксированными и права доступа.

Если понимать политику безопасности узко, то есть как правила разграничения доступа, то механизм подотчетности является дополнением подобной политики. Цель подотчетности - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Обычный **способ идентификации** – ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (аутентификации) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. «Оранжевая книга» предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в «Оранжевой книге» рассматривается два вида гарантированности - операционная и технологическая.

Гарантированность – это мера уверенности с которой можно утверждать, что для проведения в жизнь сформулированной политики безопасности выбран подходящий набор средств, и что каждое из этих средств правильно исполняет отведенную ему роль.

Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая – к методам построения и сопровождения. Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев.

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные «закладки».

Оформление документации является необходимым условием для подтверждения гарантии надежности системы и одновременно – инструмент проведения политики безопасности. Без документации люди не будут знать, какой политике следовать и что для этого нужно делать.

Согласно "Оранжевой книге", в комплект документации надежной системы должны входить следующие тома:

- Руководство пользователя по средствам безопасности.
- Руководство администратора по средствам безопасности.
- Тестовая документация.
- Описание архитектуры.

Разумеется, на практике требуется еще по крайней мере одна книга – письменное изложение политики безопасности данной организации.

Руководство пользователя по средствам безопасности предназначено для обычных, непривилегированных людей. Оно должно содержать сведения о механизмах безопасности и способах их использования. Руководство должно давать ответы по крайней мере на следующие вопросы:

- **Как входить в систему? Как вводить имя и пароль? Как менять пароль? Как часто это нужно делать? Как выбирать новый пароль?**
- **Как защищать файлы и другую информацию? Как задавать права доступа к файлам? Из каких соображений это нужно делать?**
- **Как импортировать и экспортировать информацию, не нарушая правил безопасности?**
- **Как уживаться с системными ограничениями? Почему эти ограничения необходимы? Какой стиль работы сделает ограничения необременительными?**

Руководство администратора по средствам безопасности предназначено и для системного администратора, и для

администратора безопасности. В Руководстве освещаются вопросы начального конфигурирования системы, перечисляются текущие обязанности администратора, анализируется соотношения между безопасностью и эффективностью функционирования.

Типичное оглавление Руководства администратора включает в себя следующие пункты:

- **Каковы основные защитные механизмы?**
- **Как администрировать средства идентификации и аутентификации? В частности, как заводить новых пользователей и удалять старых?**
- **Как администрировать средства произвольного управления доступом? Как защищать системную информацию? Как обнаруживать слабые места?**
- **Как администрировать средства протоколирования и аудита? Как выбирать регистрируемые события? Как анализировать результаты?**
- **Как администрировать средства принудительного управления доступом? Какие уровни секретности и категории выбрать? Как назначать и менять метки безопасности?**
- **Как генерировать новую, переконфигурированную надежную вычислительную базу?**
- **Как безопасно запускать систему и восстанавливать ее после сбоев и отказов? Как организовать резервное копирование?**
- **Как разделить обязанности системного администратора и оператора?**

Тестовая документация содержит описания тестов и их результаты. По идее она проста, но зачастую весьма пространна. Кроме того (вернее, перед тем), тестовая документация должна содержать план тестирования и условия, налагаемые на тестовое окружение.

- **Описание архитектуры** в данном контексте должно включать в себя по крайней мере сведения о внутреннем устройстве надежной вычислительной базы. Вообще говоря, это описание должно быть формальным, допускающим автоматическое сопоставление с политикой безопасности на предмет соответствия требованиям последней. Объем описания архитектуры может оказаться сопоставимым с объемом исходных текстов программной реализации системы.

Классы безопасности. В рассматриваемом стандарте определены подходы к ранжированию информационных систем по степени надежности. В "Оранжевой книге" рассматривается четыре уровня безопасности (надежности) — **D**, **C**, **B** и **A**.

Эти классы безопасности обозначают следующее:

D1 – неудовлетворительная безопасность;

C1, C2 – произвольное управление доступом;

B1, B2, B3 – принудительное управление доступом;

A1 – верифицированная защита.

По мере перехода от уровня **C** к **A** к надежности систем предъявляются все более жесткие требования. Уровни **C** и **B** подразделяются на классы (**C1**, **C2**, **B1**, **B2**, **B3**) с постепенным возрастанием надежности. Таким образом, всего практически используются шесть классов безопасности – **C1**, **C2**, **B1**, **B2**, **B3**, **A1**. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять приводимым ниже требованиям. Поскольку при переходе к каждому следующему классу требования только добавляются, то дополнительно вписываются только новые, что присуще данному классу, группируя требования в согласии с предшествующим изложением.

Каждый класс безопасности включает набор требований с учетом элементов политики безопасности и требований к гарантированности.

Так, для класса **C1** требования предусматривают следующее:

– С учетом политики безопасности*:*

- Надежная вычислительная база должна управлять доступом именованных пользователей к именованным объектам. Механизм управления (права для владельца/группы/прочих, списки управления доступом) должен позволять пользователям специфицировать разделение файлов между индивидами и/или группами;
- Пользователи должны идентифицировать себя прежде чем выполнять какие-либо иные действия, контролируемые надежной вычислительной базой. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;

– С учетом гарантированности*:*

- Надежная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за

ходом работы. Ресурсы, контролируемые базой, могут составлять определенное подмножество всех субъектов и объектов системы.

- Должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов надежной вычислительной базы.
- Защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты надежной вычислительной базы.
- Отдельный фрагмент документации (глава, том) должен описывать защитные механизмы, предоставляемые надежной вычислительной базой, и их взаимодействие между собой, содержать рекомендации по их использованию.
- Руководство должно содержать сведения о функциях и привилегиях, которыми управляет системный администратор посредством механизмов безопасности.
- Разработчик системы должен представить экспертному совету документ, содержащий план тестов, процедуры прогона тестов и результаты тестов.
- Должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации надежной вычислительной базы. Если база состоит из нескольких модулей, должен быть описан интерфейс между ними.

Аналогично документируются требования к каждому классу, который определяет набор конкретных оценок надежности компьютерных систем.

Однако следует отметить, что описанный подход был ориентирован на оценку отдельных программно-технических комплексов, поэтому в 1987 году Национальным центром компьютерной безопасности США была дополнительно опубликована интерпретация «Оранжевой книги» для сетевых конфигураций.

3.3. Гармонизированные критерии европейских стран

Следуя по пути интеграции, европейские страны приняли согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC), опубликованные в июне 1991 года от имени соответствующих органов четырех стран – Франции, Германии, Нидерландов и Великобритании. Выгода от использования согласованных критериев очевидна для всех – и для производителей, и для потребителей, и для самих органов сертификации.

Европейские критерии включают следующие основные составляющие информационной безопасности:

- **конфиденциальность**, то есть защиту от несанкционированного получения информации;
- **целостность**, то есть защиту от несанкционированного изменения информации;
- **доступность**, то есть защиту от несанкционированного удержания информации и ресурсов.

В критериях проводится различие между системами и продуктами. **Система** – это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. **Продукт** – это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя – обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем – например, чтобы облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин – объект оценки. В соответствующих местах делаются оговорки,

какие требования относятся исключительно к системам, а какие – только к продуктам.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций (сервисов) безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Сервисы безопасности реализуются посредством конкретных механизмов.

Чтобы объект оценки можно было признать надежным, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности в предлагаемом стандарте называется гарантированностью. **Гарантированность** может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта – эффективность и корректность средств безопасности. При проверке **эффективности** анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются **три градации** мощности – базовая, средняя и высокая.

Они определяют следующее:

***Базовый* – способность противостоять отдельным случайным атакам;**

***Средний* – способность противостоять злоумышленникам с ограниченными ресурсами и возможностями;**

***Высокий* – механизм может быть побежден только злоумышленником высокой квалификации с набором возможностей и ресурсов, выходящих за пределы практичности**.

В критериях вводят термин – корректность, под которой понимается правильность реализации функций и механизмов

безопасности. Используется семь возможных уровней гарантированности корректности – от **E0** до **E6** (в порядке возрастания). Уровень **E0** обозначает отсутствие гарантированное (аналог уровня **D** "Оранжевой книги"). При проверке корректности анализируется весь жизненный цикл объекта оценки – от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности. Теоретически эти два аспекта независимы, хотя на практике нет смысла проверять правильность реализации "по высшему разряду", если механизмы безопасности не обладают даже средней мощностью.

В европейских критериях средства, имеющие отношение к информационной безопасности, рассматриваются на трех уровнях детализации. Наиболее абстрактный взгляд касается лишь целей безопасности. На этом уровне получают ответ на вопрос, зачем нужны функции безопасности. Второй уровень содержит спецификации функций безопасности. Здесь определяется, какая функциональность на самом деле обеспечивается. Наконец, на третьем уровне содержится информация о механизмах безопасности. Таким образом, показывается декларированная функциональность анализируемой системы.

Спецификации функций безопасности – важнейшая часть описания объекта оценки. Критерии рекомендуют выделить в этих спецификациях разделы со следующими заголовками:

- Идентификация и аутентификация.
- Управление доступом.
- Точность информации.
- Надежность обслуживания.
- Обмен данными.

Под **идентификацией и аутентификацией** понимается не только проверка подлинности пользователей в узком смысле, но и функции для регистрации новых пользователей и удаления старых, а также функции для генерации, изменения и проверки аутентификационной информации, в том числе средства контроля целостности. Сюда же относятся функции для ограничения числа повторных попыток аутентификации.

Средства управления доступом также трактуются европейскими критериями достаточно широко. В этот раздел попадают, помимо прочих, функции, обеспечивающие временное ограничение доступа к совместно используемым объектам с целью поддержания целостности этих объектов – мера, типичная для систем управления базами данных. В этот же раздел попадают функции для управления распространением прав доступа и для контроля за получением информации путем логического вывода и агрегирования данных (что также типично для СУБД).

Под точностью в критериях понимается поддержание определенного соответствия между различными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникаций). Точность выступает как один из аспектов целостности информации.

Функции **надежности обслуживания** должны гарантировать, что действия, критичные по времени, будут выполнены ровно тогда, когда нужно – не раньше и не позже, и что некритичные действия нельзя перевести в разряд критичных. Далее, должна быть гарантия, что авторизованные пользователи за разумное время получат запрашиваемые ресурсы. Сюда же относятся функции для обнаружения и нейтрализации ошибок, необходимые для минимизации простоев, а также функции планирования, позволяющие гарантировать время реакции на внешние события.

К области **обмена данными** относятся функции, обеспечивающие коммуникационную безопасность, то есть безопасность данных, передаваемых по каналам связи.

3.4. Германский стандарт BSI

В 1998 году в Германии вышло "Руководство по защите информационных технологий для базового уровня". Руководство представляет собой гипертекст объемом около 4 МБ (в формате HTML).

В дальнейшем оно было оформлено в виде германского стандарта BSI. В его основе лежит общая методология и компоненты управления информационной безопасностью:

- **Общий метод управления информационной безопасностью (организация менеджмента в области ИБ, методология использования руководства).**
- **Описания компонентов современных информационных технологий.**
- **Основные компоненты (организационный уровень ИБ, процедурный уровень, организация защиты данных, планирование действий в чрезвычайных ситуациях).**
- **Инфраструктура (здания, помещения, кабельные сети, организация удаленного доступа).**
- **Клиентские компоненты различных типов (DOS, Windows, UNIX, мобильные компоненты, прочие типы).**
- **Сети различных типов (соединения «точка-точка», сети Novell NetWare, сети с ОС ONIX и Windows, разнородные сети).**
- **Элементы систем передачи данных (электронная почта, модемы, межсетевые экраны и т.д.).**
- **Телекоммуникации (факсы, автоответчики, интегрированные системы на базе ISDN, прочие телекоммуникационные системы).**
- **Стандартное ПО.**
- **Базы данных.**
- **Описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса).**
- **Характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны).**
- **Характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение, например рабочие станции и сервера под управлением операционных систем семейства DOS, Windows и UNIX).**
- **Характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows).**
- **Характеристика активного и пассивного телекоммуникационного оборудования ведущих вендоров, например Cisco Systems.**
- **Подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).**

Все **виды угроз** в стандарте BSI разделены на следующие классы:

- Форс-мажорные обстоятельства.
- Недостатки организационных мер.
- Ошибки человека.
- Технические неисправности.
- Преднамеренные действия.

Аналогично классифицированы **контрмеры**:

- Улучшение инфраструктуры;
- Административные контрмеры;
- Процедурные контрмеры;
- Программно-технические контрмеры;
- Уменьшение уязвимости коммуникаций; планирование действий в чрезвычайных ситуациях.

Все компоненты рассматриваются и описываются по следующему плану:

1) общее описание;

2) возможные сценарии угроз безопасности (перечисляются применимые к данной компоненте угрозы из каталога угроз безопасности);

3) возможные контрмеры (перечисляются применимые к данной компоненте угрозы из каталога угроз безопасности);

3.5. Британский стандарт BS 7799

Британский институт стандартов (BSI) при участии коммерческих организаций, таких как Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica и др. разработал стандарт информационной безопасности, который в 1995 г. был принят в качестве национального стандарта BS 7799 управления информационной безопасностью организации вне зависимости от сферы деятельности компании.

В соответствии с этим стандартом любая служба безопасности, IT - отдел, руководство компании должны начинать работать согласно общему регламенту. Неважно, идет речь о защите бумажного документооборота или электронных данных. В настоящее время Британский стандарт BS 7799 поддерживается в 27 странах мира, в числе которых страны Британского Содружества, а также, например, Швеция и Нидерланды. В 2000 г. международный институт стандартов ISO на базе британского BS 7799 разработал и выпустил международный стандарт менеджмента безопасности ISO / IEC 17799.

Поэтому сегодня можно утверждать, что BS 7799 и ISO 17799 это один и тот же стандарт, имеющий на сегодняшний день мировое признание и статус международного стандарта ISO.

Вместе с тем, следует отметить первоначальное содержание стандарта BS 7799, который до настоящего времени используется в ряде стран. Он состоит из двух частей.

В **"Части 1: Практические рекомендации"** (1995г.) определяются и рассматриваются следующие аспекты ИБ:

- Политика безопасности.
- Организация защиты.
- Классификация и управление информационными ресурсами.
- Управление персоналом.
- Физическая безопасность.
- Администрирование компьютерных систем и сетей.
- Управление доступом к системам.
- Разработка и сопровождение систем.
- Планирование бесперебойной работы организации.
- Проверка системы на соответствие требованиям ИБ.

"Часть 2: Спецификации системы" (1998г) рассматривает эти же аспекты с точки зрения сертификации информационной системы на соответствие требованиям стандарта.

Она определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Дополнительные рекомендации для управления информационной безопасностью содержат руководства Британского института стандартов – British Standards Institution(BSI) http://www.bsi-giobal.com/, изданные в период 1995-2003 в виде следующей серии:

- **Введение в проблему управления информационной безопасности – Information security managment: an introduction.**
- **Возможности сертификации на требования стандарта BS 7799 - Preparing for BS 7799 sertification.**
- **Руководство BS 7799 по оценке и управлению рисками -Guide to BS 7799 risk assessment and risk management.**

- **Готовы ли вы к аудиту на требования стандарта BS 7799-Are you ready for a BS 7799 audit?**
- **Руководство для проведения аудита на требования стандарта -BS 7799Guide to BS 7799 auditing.**
- **Практические рекомендации по управлению безопасностью информационных технологий -Code of practice for IT management.**

Сегодня общими вопросами управления информационной безопасности компаний и организаций, а также развитием аудита безопасности на требования стандарта BS 7799 занимаются международный комитет Joint Technical Committee ISO/IEC JTC 1 совместно с Британским Институтом Стандартов- British Standards Institution(BSI) – (www.bsi-global.com), и в частности служба UKAS (United Kingdom Accredited Service). Названная служба производит аккредитацию организаций на право аудита информационной безопасностью в соответствии со стандартом BS ISO/IEC 7799:2000 (BS 7799-1:2000). Сертификаты, выданные этими органами, признаются во многих странах.

Отметим, что в случае сертификации компании по стандартам ISO 9001 или ISO 9002 стандарт BS ISO/IEC 7799:2000 (BS 7799-1:2000) разрешает совместить сертификацию системы информационной безопасности с сертификацией на соответствие стандартам ISO 9001 или 9002 как на первоначальном этапе, так и при контрольных проверках. Для этого необходимо выполнить условие участия в совмещенной сертификации зарегистрированного аудитора по стандарту BS ISO/IEC 7799:2000 (BS 7799-1:2000). При этом в планах совместного тестирования должны быть четко указаны процедуры проверки системы информационной безопасности, а сертифицирующие органы должны гарантировать тщательность проверки информационной безопасности.

3.6. Международный стандарт ISO 17799

Одним из наиболее развитых и широко используемых во всех странах мира стал международный стандарт ISO 17799:

Code of Practice for Information Security Management (Практические рекомендации по управлению безопасностью информации), принятом в

2000 году. ISO 17799 был разработан на основе британского стандарта BS 7799.

ISO 17799 может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Практические правила разбиты на следующие 10 разделов:

1. **Политика безопасности.**
2. **Организация защиты.**
3. **Классификация ресурсов и их контроль.**
4. **Безопасность персонала.**
5. **Физическая безопасность.**
6. **Администрирование компьютерных систем и вычислительных сетей.**
7. **Управление доступом.**
8. **Разработка и сопровождение информационных систем.**
9. **Планирование бесперебойной работы организации.**
10. **Контроль выполнения требований политики безопасности.**

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.

При использовании некоторых из средств контроля, например, шифрования данных, могут потребоваться советы специалистов по безопасности и оценка рисков, чтобы определить, нужны ли они и каким образом их следует реализовывать. Для обеспечения более высокого уровня защиты особенно ценных ресурсов или оказания противодействия особенно серьезным угрозам безопасности, в ряде случаев могут потребоваться более сильные средства контроля, которые выходят за рамки ISO 17799.

Десять ключевых средств контроля, перечисленные ниже, представляют собой либо обязательные требования, например требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования АС и составляют основу системы управления информационной безопасностью.

Ключевыми являются следующие средства контроля:

- документ о политике информационной безопасности;

- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты;
- средства защиты от вирусов;
- планирование бесперебойной работы организации;
- контроль над копированием программного обеспечения, защищенного законом об авторском праве;
- защита документации организации;
- защита данных;
- контроль соответствия политике безопасности.

Процедура аудита безопасности ИС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности ИС также является анализ и управление рисками.

Учитывая важность этого стандарта для аудита информационной безопасности, рассмотрим его ниже более подробно.

3.7. Международный стандарт ISO 15408 – «Общие критерии»

Международный стандарт ИСО/МЭК 15408-99 (исторически сложившееся название – «Общие критерии») представляет собой результат обобщения опыта различных государств по разработке и практическому использованию критериев оценки безопасности информационных технологий (ИТ). Базовые документы, которые легли в основу «Общих критериев», и связи между ними представлены на рис 3.1.

Анализ развития нормативной базы оценки безопасности ИТ позволяет понять те мотивационные посылки, которые привели к созданию «Общих критериев».

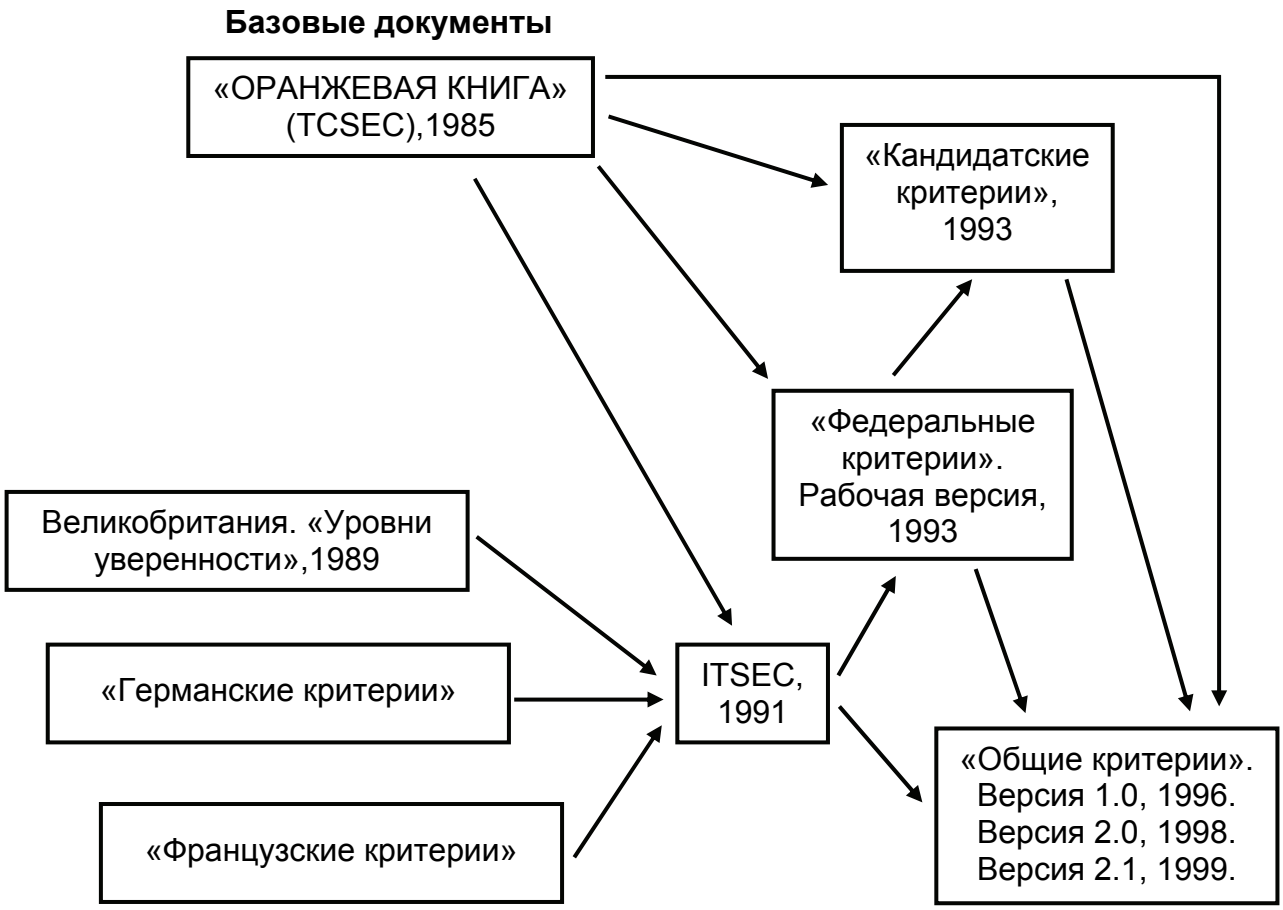

Рис. 3.1. **Предыстория «Общих критериев»**

Общие критерии оценки безопасности информационных технологий (далее «Общие критерии») определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

При проведении работ по анализу защищенности ИС, «Общие критерии» целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности ИС с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Хотя применимость «Общих критериев» ограничивается механизмами безопасности программно-технического уровня, в них содержится также определенный набор требований к механизмам безопасности организационного уровня и требований по физической

защите, которые непосредственно связаны с описываемыми функциями безопасности.

Разработка этого стандарта преследовала следующие **основные цели**:

- унификация национальных стандартов в области оценки безопасности ИТ;
- повышение уровня доверия к оценке безопасности ИТ;
- сокращение затрат на оценку безопасности ИТ на основе взаимного признания сертификатов.

Новые критерии были призваны обеспечить взаимное признание результатов стандартизованной оценки безопасности на мировом рынке ИТ.

Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во **второй части** «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в ИС функций безопасности.

Третья часть «Общих критериев», наряду с другими требованиями к адекватности реализации функций безопасности, содержит класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

- наличие побочных каналов утечки информации;
- ошибки в конфигурации, либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние;
- недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;
- наличие уязвимостей («дыр») в средствах защиты информации, позволяющих пользователям получать НСД к информации в обход существующих механизмов защиты.

При проведении работ по аудиту безопасности данные требования могут использоваться в качестве руководства и критериев для анализа уязвимостей ИС.

Основными отличительными чертами ОК являются:

- наличие определенной методологии и системы формирования требований и оценки безопасности ИТ. Системность прослеживается начиная от терминологии и уровней абстракции представления требований и кончая их использованием при оценке безопасности на всех этапах жизненного цикла изделий ИТ;
- общие критерии, которые характеризуются наиболее полной на сегодняшний день совокупностью требований безопасности ИТ;
- четкое разделение требований безопасности на функциональные требования и требования доверия к безопасности. Функциональные требования относятся к сервисам безопасности (идентификации, аутентификации, управлению доступом, аудиту и т.д.), а требования доверия – к технологии разработки, тестированию, анализу уязвимостей, эксплуатационной документации, поставке, сопровождению, то есть ко всем этапам жизненного цикла изделий ИТ;
- общие критерии, включающие шкалу доверия к безопасности (оценочные уровни доверия к безопасности), которая может использоваться для формирования различных уровней уверенности в безопасности продуктов ИТ;
- систематизация и классификация требований по иерархии «класс – семейство – компонент – элемент» с уникальными идентификаторами требований, которые обеспечивают удобство их использования;
- компоненты требований в семействах и классах, которые ранжированы по степени полноты и жесткости, а также сгруппированы в пакеты требований;
- гибкость в подходе к формированию требований безопасности для различных типов изделий ИТ и условий их применения обеспечиваемые возможностью целенаправленного формирования необходимых наборов требований в виде определенных в ОК стандартизованных структурах (профиляхй защиты и заданий по безопасности);
- общие критерии обладают открытостью для последующего наращивания совокупности требований.

По уровню систематизации, полноте и возможностям детализации требований, универсальности и гибкости в применении ОК представляют наиболее совершенный из существующих в настоящее время стандартов. Причем, что очень важно, в силу особенностей построения он имеет практически неограниченные возможности для развития, представляет собой не функциональный стандарт, а методологию задания, оценки и каталог требований безопасности ИТ, который может наращиваться и уточняться.

В определенном смысле роль функциональных стандартов выполняют профили защиты, которые формируются с учетом рекомендаций и каталога требований ОК, но могут включать и любые другие требования, которые необходимы для обеспечения безопасности конкретного изделия или типа изделий ИТ.

3.8. Стандарт COBIT

Вопросами аудита информационной безопасности в настоящее время занимаются различные аудиторные компании, фирмы организации, многие из которых входят в состав государственных и негосударственных ассоциаций. Наиболее известной международной организацией занимающейся аудитом информационных систем является ISACA, по инициативе которой была разработана концепция по управлению информационными технологиями в соответствии с требованиями ИБ.

На основе этой концепции описываются элементы информационной технологии, даются рекомендации по организации управления и обеспечению режима информационной безопасности. Концепция изложена в документе под названием COBIT 3rd Edition (Control Objectives for Information and Related Technology - Контрольные объекты информационной технологии), который состоит из четырех частей

- **часть 1** – краткое описание концепции (Executive Summary);
- **часть 2** – определения и основные понятия (Framework). Помимо требований и основных понятий, в этой части сформулированы требования к ним;
- **часть 3** – спецификации управляющих процессов и возможный инструментарий (Control Objectives);

- **часть 4** – рекомендации по выполнению аудита компьютерных информационных систем (Audit Guidelines).

Третья часть этого документа в некотором смысле аналогична международному стандарту BS 7799. Примерно так же подробно приведены практические рекомендации по управлению информационной безопасностью, но модели систем управления в сравниваемых стандартах сильно различаются. Стандарт COBIT - пакет открытых документов, первое издание которого было опубликовано в 1996 году. COBIT описывает универсальную модель управления информационной технологией, представленную на рис. 3.2 [10].

Кратко основная идея стандарта COBIT выражается следующим образом: все ресурсы информационной системы должны управляться набором естественно сгруппированных процессов для обеспечения компании необходимой и надежной информацией. В модели COBIT присутствуют ресурсы информационных технологий (IT), являющиеся источником информации, которая используется в бизнес-процессе. Информационная технология должна удовлетворять требованиям бизнес-процесса. Эти требования сгруппированы следующим образом.

Во первых, требования к качеству технологии составляют показатели качества и стоимости обработки информации, характеристики ее доставки получателю. Показатели качества подробно описывают возможные негативные аспекты, которые в обобщенном виде входят в понятия целостности и доступности. Кроме того, в эту группу включаются показатели, относящиеся к субъективным аспектам обработки информации, например: стиль, удобство интерфейсов. Характеристики доставки информации получателю – показатели, в обобщенном виде входящие в показатели доступности и частично – конфиденциальности и целостности. Рассмотренная система показателей используется при управлении рисками и оценке эффективности информационной технологии. **Во-вторых**, доверие к технологии -группа показателей, описывающих соответствие компьютерной информационной системы принятым стандартам и требованиям, достоверность обрабатываемой в системе информации, ее действенность. **В-третьих**, показатели информационной безопасности – конфиденциальность, целостность и доступность обрабатываемой в системе информации.

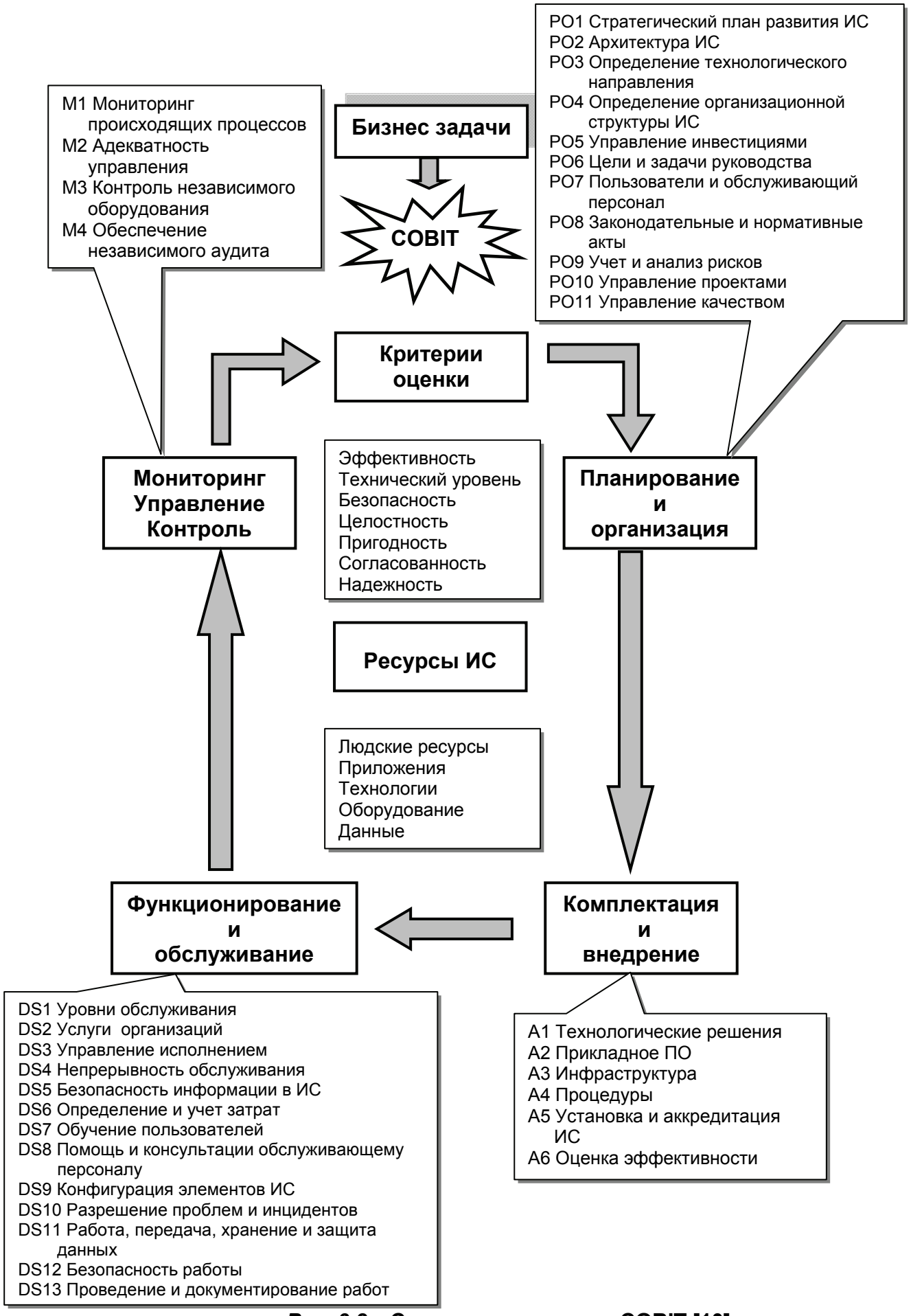

Рис. 3.2. **Структура стандарта COBIT [10]**

В стандарте COBIT выделены следующие этапы проведения аудита [10].

Подписание договорной и исходно-разрешительной документации. На этом этапе определяются ответственные лица со стороны заказчика и аудиторской компании, устанавливаются рамки проведения аудита, указываются контролируемые элементы информационной системы, составляется и согласовывается необходимая документация. По результатам предварительного аудита всей информационной системы проводится углубленная проверка подозрительных с точки зрения проводимых аудитом компонентов системы.

Сбор информации с применением стандарта COBIT, который в данном случае регламентирует состав объектов контроля исследуемой системы. Степень детализации описания объектов контроля определяется на этапе разработки исходно-разрешительной документации. При этом стараются добиться оптимального соотношения между временными, стоимостными и прочими затратами на получение исходных данных и их важностью для целей исследования. Диапазон представления исходных данных изменяется от бинарных ответов типа ДА/НЕТ до развернутых отчетов. Основное требование, предъявляемое к информации, – это ее полезность, то есть информация должна быть понятной, уместной (относящейся к делу) и достоверной (надежной).

Анализ исходных данных проводится только с учетом достоверных исходных данных. Требования к проведению анализа определяются на этапе сбора исходных данных. Стандарт COBIT рекомендует применять описанные в стандарте методики анализа данных, но при необходимости допускается использование разрешенных ISACA разработок других членов ассоциации. На этапе анализа возможен возврат к этапу сбора информации для получения недостающих исходных данных.

Выработка рекомендаций. Полученные в результате проведенного анализа рекомендации после предварительного согласования с заказчиком обязательно должны быть проверены на выполнимость и актуальность с учетом рисков внедрения. Стандарт COBIT рекомендует оформлять рекомендации отчетом о текущем состоянии информационных систем, техническом задании на внесение изменений, отчетом о проведенном аудите. Результаты проведения аудита можно разделить на три условные группы: *организационные, технические и*

методологические. Каждая из названных групп направлена на улучшение организационного, технического или методологического обеспечения информационной системы. К **организационной группе** относятся оценки стратегического планирования, общего управления и инвестиций в информационную систему, рекомендации, способствующие повышению конкурентоспособности компании, снижению затрат на обслуживание информационной системы, результаты проверки соответствия информационной системы решаемым бизнес-задачам, снижение стоимости эксплуатации информационной системы, управление рисками, проектами, выполняемыми в рамках информационных систем и некоторые другие. **Техническая группа** результатов позволяет лучше понять проблемы информационных систем и разработать пути их решения с минимальными затратами, оценить технологические решения, реализовать весь потенциал новых технологий, системно решить вопросы безопасности, осуществить профессиональный прогноз функционирования и необходимости модернизации информационных систем, повысить эффективность функционирования информационной системы, определить уровень обслуживания информационных систем. **Методологические результаты** позволяют предоставить апробированные подходы к стратегическому планированию и прогнозированию, оптимизации документооборота, повышению трудовой дисциплины, обучению администраторов и пользователей информационных систем, получению своевременной и объективной информации о текущем состоянии информационной системы компании.

Контроль за выполнением рекомендаций подразумевает постоянное отслеживание аудиторской компанией выполнения заказчиком рекомендацией.

Подписание отчетных актов приемки работы с планом-графиком проведения последующих проверок, разработкой такой дополнительной документации, как долгосрочные и краткосрочные планы развития ИС, план восстановления информационной системы в чрезвычайных ситуациях, порядок действий при нарушении защиты, концепция политики безопасности. Постоянное проведение аудита гарантирует работоспособность системы, поэтому создание плана-графика проведения последующих проверок является одним из условий проведения профессионального аудита.

Любая работающая информационная технология в модели COBIT проходит следующие **стадии жизненного цикла**:

Планирование и организация работы. На этой стадии определяется стратегия и тактика развития информационных технологий в интересах достижения основных целей бизнеса, а затем решаются вопросы реализации: построение архитектуры системы, решение технологических и организационных задач, обеспечение финансирования и т.д. Всего на этой стадии выделяется 11 основных задач [10].

Приобретение и ввод в действие. Выбранные на этой стадии решения должны быть документально оформлены и спланированы. Выделяется 6 основных задач, решаемых на данной стадии.

Поставка и поддержка. Выделяется 13 основных задач данной стадии, предназначенных обеспечить эксплуатацию информационной технологии [10].

Мониторинг. За процессами информационной технологии необходимо наблюдать и контролировать соответствие их параметров выдвинутым требованиям. Выделяется 4 основные задачи, решаемые на данной стадии.

Всего в стандарте COBIT выделяется 34 задачи верхнего уровня обработки информации (рис. 3.2).

Кроме традиционных свойств информации – конфиденциальности, целостности и доступности, – в модели дополнительно используются еще 4 свойства – **действенность**, **эффективность**, **соответствие формальным требованиям** и **достоверность**. Эти свойства не являются независимыми, поскольку частично связаны с первыми тремя. Но их использование объясняется соображениями удобства интерпретации результатов.

Применение стандарта COBIT возможно как для проведения аудита ИС организации, так и для изначального проектирования ИС. Обычный вариант прямой и обратной задач. Если в первом случае – это соответствие текущего состояния ИС лучшей практике аналогичных организаций и предприятий, то в другом – изначально верный проект и, как следствие, по окончании проектирования – ИС, стремящаяся к идеалу.

На базовой блок-схеме COBIT (рис. 3.2.) отражена последовательность, состав и взаимосвязь базовых групп. Бизнес-процессы (в верхней части схемы) предъявляют свои требования к ресурсам ИС, которые анализируются с использованием критериев оценки COBIT на всех этапах построения и проведения аудита.

Четыре базовые группы (домена) содержат в себе тридцать четыре подгруппы, которые, в свою очередь, состоят из трехсот двух объектов контроля (в данной работе не рассматриваются). Объекты контроля предоставляют аудитору всю достоверную и актуальную информацию о текущем состоянии ИС.

Отличительные черты COBIT:

1. Большая зона охвата (все задачи от стратегического планирования и основополагающих документов до анализа работы отдельных элементов ИС).
2. Перекрестный аудит (перекрывающиеся зоны проверки критически важных элементов).
3. Адаптируемый, наращиваемый стандарт.

Основными преимуществами COBIT перед другими аналогичными стандартами является то, что он позволяет использовать любые разработки производителей аппаратно-программного обеспечения и анализировать полученные данные, не изменяя общие подходы и собственную структуру.

Представленная на рис 3.3 блок-схема отражает, хотя и не в деталях, ключевые точки проведения аудита ИС с использованием стандарта COBIT. Рассмотрим их подробнее.

На этапе подготовки и подписания исходно-разрешительной документации определяются границы проведения аудита:

- Границы аудита определяются критическими точками ИС (элементами ИС), в которых наиболее часто возникают проблемные ситуации.
- На основании результатов предварительного аудита всей ИС (в первом приближении) проводится углубленный аудит выявленных проблем.

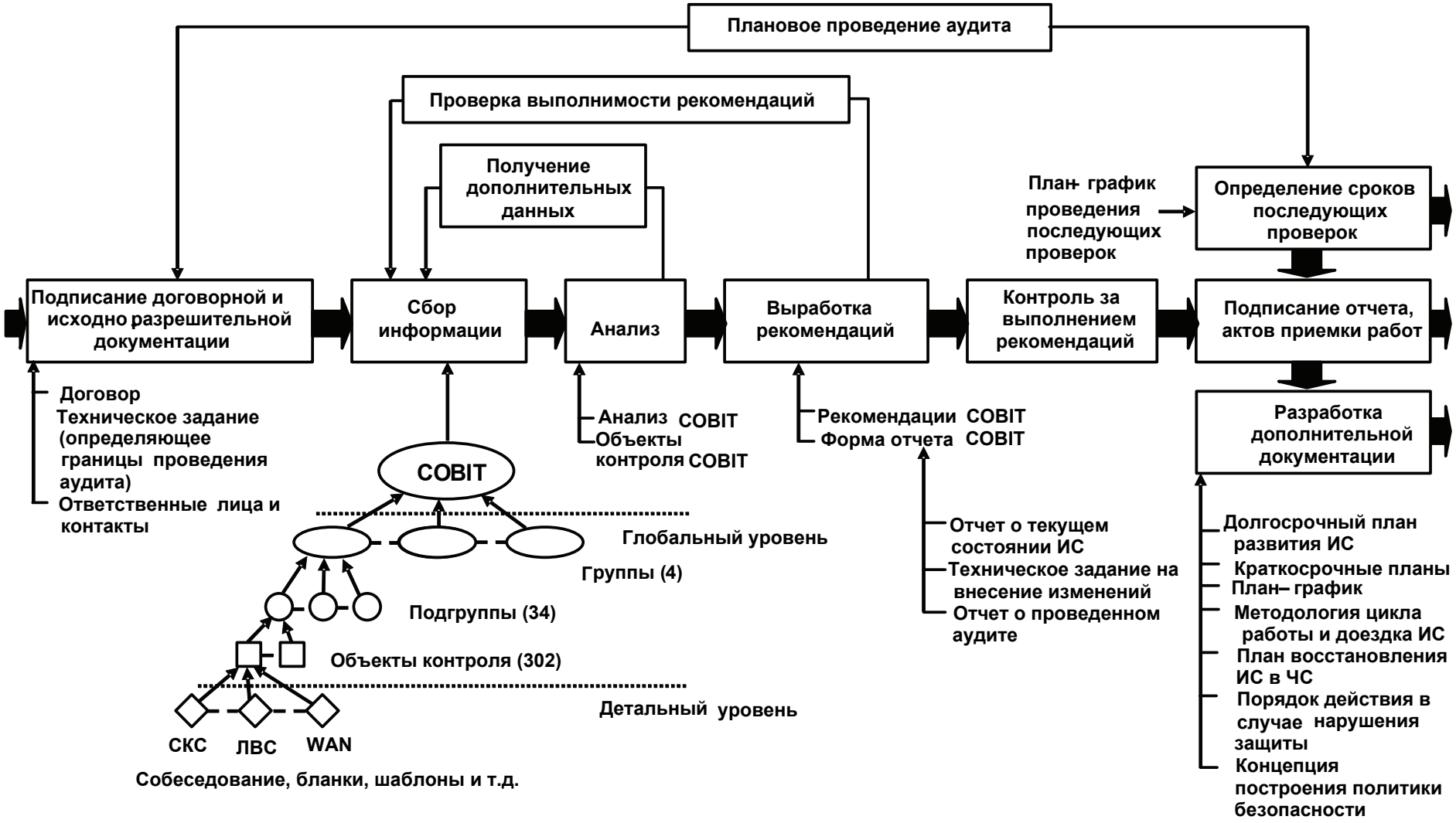

Рис. 3.3. **Общая последовательность проведения аудита**

В это же время создается команда проведения аудита, определяются ответственные лица со стороны заказчика. Создается и согласовывается необходимая документация.

Далее проводится сбор информации о текущем состоянии ИС с применением стандарта COBIT, объекты контроля которого получают информацию обо всех нюансах функционирования ИС как в двоичной форме (Да/Нет), так и форме развернутых отчетов. Детальность информации определяется на этапе разработки исходно-разрешительной документации. Существует определенный оптимум между затратами (временными, стоимостными и т.д.) на получение информации и ее важностью и актуальностью.

Проведение анализа – наиболее ответственная часть проведения аудита ИС. Использование при анализе недостоверных, устаревших данных недопустимо, поэтому необходимо уточнение данных, углубленный сбор информации. Требования к проведению анализа определяются на этапе сбора информации. Методики анализа информации существуют в стандарте COBIT, но если их не хватает не возбраняется использовать разрешенные ISACA разработки других компаний.

Результаты проведенного анализа являются базой для выработки рекомендаций, которые после предварительного согласования с заказчиком должны быть проверены на выполнимость и актуальность с учетом рисков внедрения.

Контроль выполнения рекомендаций – немаловажный этап, требующий непрерывного отслеживания представителями консалтинговой компании хода выполнения рекомендаций.

На этапе разработки дополнительной документации проводится работа, направленная на создание документов, отсутствие или недочеты в которых могут вызвать сбои в работе ИС. Например, отдельное углубленное рассмотрение вопросов обеспечения безопасности ИС.

Постоянное проведение аудита гарантирует стабильность функционирования ИС, поэтому создание план-графика проведения последующих проверок является одним из результатов профессионального аудита.

3.9. Стандарты по безопасности информационных технологий в России

Среди различных стандартов по безопасности информационных технологий, существующих в нашей стране, следует выделить ряд документов, регламентирующих защиту взаимосвязи открытых систем (табл.3.1, строки 1-3). К ним можно добавить нормативные документы по средствам, системам и критериям оценки защищенности средств вычислительной техники и автоматизированных систем (табл. 3.1, строки 4-8). Последняя группа документов, также как и многие ранее созданные зарубежные стандарты, ориентирована преимущественно на защиту государственной тайны.

Таблица 3.1

№ п/п	Номер документа	Описание
1	ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. архитектура защиты информации.
2	ГОСТ Р ИСО/МЭК 9594-8-98	Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. основы аутентификации.
3	ГОСТ Р ИСО/МЭК 9594-9-95	Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 9. Дублирование.
4	Руководящий документ	Руководящий документ Гостехкомиссии «РД.СВТ Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1997).
5	ГОСТ Р 50739-95	«Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
6	ГОСТ 28147-89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
7	ГОСТ Р 34.10-94	Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе ассиметричного криптографического алгоритма.
8	ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования.

Кроме названных ГОСТов, начиная с 1992г. Гостехкомиссией при президенте РФ был разработан ряд документов, посвященных проблеме защиты от несанкционированного доступа к информации, в основу которых была положена концепция, предусматривающая существование

двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД. Это направление, связанное со средствами вычислительной техники (СВТ), и направление, связанное с автоматизированными системами (АС).

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации, при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Существуют различные способы покушения на информационную безопасность – радиотехнические, акустические, программные и т.п. Среди них главным образом выделяются такие, которые приводят к нарушению установленных правил разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В концепции формулируются следующие основные принципы **защиты от НСД к информации**:

- Защита СВТ обеспечивается комплексом программно-технических средств.
- Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
- Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
- Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

- Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.
- Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Концепция ориентируется на физически защищенную среду, проникновение в которую посторонних лиц считается невозможным, поэтому нарушитель определяется как субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель считается специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты.

В качестве главного средства защиты от НСД к информации в Концепции рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. **Основными функциями СРД** являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Кроме того, концепция предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Мы видим, что функции системы разграничения доступа и обеспечивающих средств, предлагаемые в концепции по сути близки к

аналогичным положениям "Оранжевой книги". Это вполне естественно, поскольку близки и исходные посылки – защита от несанкционированного доступа к информации в условиях физически безопасного окружения.

Технические средства защиты от НСД, согласно Концепции, должны оцениваться по следующим основным параметрам:

- степень полноты охвата ПРД реализованной СРД и ее качество;
- состав и качество обеспечивающих средств для СРД;
- гарантии правильности функционирования СРД и обеспечивающих ее средств.

Классификация средств вычислительной техники по уровню защищенности от НСД

Переходя к рассмотрению предлагаемой Гостехкомиссией при Президенте РФ классификации средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации, отметим ее близость к классификации "Оранжевой книги". Процитируем соответствующий руководящий документ:

Устанавливается **семь классов защищенности СВТ от НСД** к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

Приведем сводную таблицу распределения показателей защищенности по шести классам СВТ (табл. 3.2).

Таблица 3.2

Распределение показателей защищенности по классам СВТ

Показатель	Класс защищенности					
	6	**5**	**4**	**3**	**2**	**1**
1. Дискреционный принцип контроля доступа	+	+	+	=	+	=
2. Мандатный принцип контроля доступа	-	-	+	=	=	=
3. Очистка памяти	-	+	+	+	=	=
4. Изоляция модулей	-	-	+	=	+	=
5. Маркировка документов	-	-	+	=	=	=
6. Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
7. Сопоставление пользователя с устройством	-	-	+	=	=	=
8. Идентификация и аутентификация	+	=	+	=	=	=
9. Гарантии проектирования	-	+	+	+	+	+
10. Регистрация	-	+	+	+	=	=
11. Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12. Надежное восстановление	-	-	-	+	=	=
13. Целостность КСЗ	-	+	+	+	=	=
14. Контроль модификации	-	-	-	-	+	=
15. Контроль дистрибуции	-	-	-	-	+	=
16. Гарантии архитектуры	-	-	-	-	-	+
17. Тестирование	+	+	+	+	+	=
18. Руководство пользователя	+	=	=	=	=	=
19. Руководство по КСЗ	+	+	=	+	+	=
20. Текстовая документация	+	+	+	+	+	=
21. Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения: «-» – нет требований к данному классу; «+» – новые или дополнительные требования; «=» – требования совпадают с требованиями к СВТ предыдущего класса; «КСЗ» – комплекс средств защиты.

Классификация автоматизированных систем по уровню защищенности от НСД

Классификация автоматизированных систем устроена иначе. Снова обратимся к соответствующему руководящему документу.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – **3Б** и **3А**.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности.

Группа содержит два класса – **2Б** и **2А**.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС.

Группа содержит пять классов – **1Д**, **1Г**, **1В**, **1Б** и **1А**.

Сведем в таблицу требования ко всем девяти классам защищенности АС (табл.3.3).

Таблица 3.3

Требования к защищенности автоматизированных систем

Подсистемы и требования	**Классы**								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистемы управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+

Продолжение табл. 3.3

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
к программам				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов		+		+		+	+	+	+
запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
доступа программ субъектов к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи				+		+	+	+	+
доступа программ субъектов, доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
изменения полномочий субъектов доступа							+	+	+
создаваемых защищаемых объектов доступа				+			+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей		+		+		+	+	+	+
2.4. Сигнализация попыток нарушения защиты							+	+	+

Окончание табл. 3.3

Подсистемы и требования	Классы								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах									+
3.3. Использование аттестованных (сертифицированных) криптографических средств				+				+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС				+			+	+	+
4.4. Периодическое тестирование СЗИ НСД									
4.5. Наличие средств восстановления СЗИ НСД									
4.6. Использование сертифицированных средств защиты		+		+			+	+	+

Приведем для примера изложение требований к достаточно представительному классу защищенности – **1В**.

Требования к классу защищенности **1 В**:

- **Подсистема управления доступом**:

– должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

– должна осуществляться идентификация:
  - терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и/или адресам;
  - программ, томов, каталогов, файлов, записей, полей записей по именам;

А также должен контролироваться доступ субъектов к защищаемым ресурсам в соответствии с матрицей доступа; должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

- **Подсистема регистрации и учета**:
  – должна осуществляться регистрация:
    - входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова; должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию;
    - запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов;
    - попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;
    - изменений полномочий субъектов доступа и статуса объектов доступа;
  – должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

– должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки;

– должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. При двукратной произвольной записи в любую освобождаемую область памяти, использованную для хранения защищаемой информации; должна осуществляться сигнализация попыток нарушения защиты.

- **Подсистема обеспечения целостности**:

– должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды, при этом:

– целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ, целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;

– должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и

– специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

– должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

– должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;

– должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;

– должны использоваться сертифицированные средства защиты.

Рассмотренный пример определяет необходимый минимум требований, которым надо следовать, чтобы обеспечить конфиденциальность защищаемой информации.

Контрольные вопросы

1. С какой целью разрабатывались международные стандарты ИБ?

2. Назовите основные международные стандарты ИБ.

3. Какие критерии определяют степень доверия в стандарте «Оранжевая книга»?

4. Определите назначения и виды классов безопасности в «Оранжевой книге».

5. Как определяются составляющие ИБ в гармозированных критериях Европейских стран.

6. Приведите составляющие германского стандарта BSI.

7. Почему Британский стандарт BS 7799 используется наиболее часто?

8. В чем отличие применения международных стандартов ISO 15408 и ISO 17799?

9. Назовите основные этапы проведения аудита ИБ при использовании стандарта CoBiT.

10. Какие стандарты, разработанные в России, используются при оценке защищенности информационных технологий?

11. Как проводится оценка защищенности автоматизированных систем (по рекомендации ГосТехкомиссии)?

Глава 4. Оценка безопасности информационных технологий на основе «Общих критериев». Стандарт ISO 15408

4.1. Предпосылки введения международного стандарта ISO 15408

Следуя по пути интеграции, в 1990 г. Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (TEC) составили специализированную систему мировой стандартизации, а ISO начала создавать международные стандарты по критериям оценки безопасности информационных технологий для общего использования, названные Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий) или просто Common Criteria (общие критерии). В их разработке участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Нидерланды), Органы исполнения программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция).

В дальнейшем «Общие критерии» неоднократно редактировались. В результате 8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий» (ОК).

Общие критерии обобщили содержание и опыт использования «Оранжевой книги», развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК – полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Использование методик данного стандарта позволяет определить для компании те критерии, которые могут быть использованы в качестве основы для выработки оценок защитных свойств продуктов и систем информационной технологии. Кроме того, эти методики позволяют проводить наиболее полное сравнение результатов оценки защитных свойств корпоративных информационных систем с помощью общего перечня (набора) требований для функций защиты продуктов и систем, а также методов точных измерений, которые проводятся во время получения оценок защиты. Основываясь на этих требованиях, в процессе выработки оценки уровня защиты устанавливается уровень доверия.

Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы.

Вместе с тем, в ОК главное внимание уделено защите от несанкционированного доступа (НСД). Модификации или потери доступа к информации в результате случайных или преднамеренных действий и ряд других аспектов информационной безопасности остался не рассмотренным. Например, оценка административных мер безопасности, оценка безопасности от побочных электромагнитных излучений, методики оценки различных средств и мер безопасности, критерии для оценки криптографических методов защиты информации.

На основе рассматриваемого стандарта в РФ был принят в 1999 г. аналогичный стандарт, состоящий из трех частей.

ISO 15408-1:1999 – Информационные технологии. Методы защиты. Критерии оценки для информационных технологий. **Часть 1. Введение и общая модель**.

ISO 15408-2:1999 – **Часть 2. Функциональные требования безопасности**.

ISO 15408-3:1999 – **Часть 3. Требования к обеспечению защиты**.

Первая часть определяет концепцию всего стандарта, **вторая,** самая большая часть, формализует методы и требования к **информационной безопасности,** а **третья часть** полностью посвящена процессам обеспечения **доверия – (качества) компонентов** информационных систем (ИС), реализующих функции их безопасности. По существу рассматривается регламентирование технологии и процессов обеспечения жизненного цикла программных средств, создаваемых для обеспечения безопасности функционирования и применения систем. При этом акцент документа сосредоточен на **информационной безопасности** сложных программных средств ИС. В тоже время основные положения этой части стандарта практически полностью применимы к технологии и процессам создания программных средств (ПС) и обеспечению их функциональной безопасности. Поэтому ниже в данном разделе многие положения этой части стандарта трактуются с позиции обеспечения функциональной безопасности, а **термин – доверие** применяется как понятие **качество или уверенность выполнения требования безопасности.**

4.2. Основные понятия общих критериев

Основная концепция ISO 15408 – обеспечение доверия, основанное на оценке качества (активном исследовании реализации функции) продукта или системы. Нарушения безопасности ПС возникают вследствие преднамеренного использования или случайной активизации уязвимостей при применении систем и ПС. Рекомендуется ряд шагов для предотвращения уязвимостей, возникающих в продуктах и системах. Уязвимости могут возникать **вследствие недостатков [23]:**

- **требований** к продукту или системе, которые могут обладать требуемыми от них функциями и свойствами, но все же содержать

определенные уязвимости, делающие их непригодными или неэффективными в части безопасности применения;

- **проектирования** продукта или системы, которые не отвечают спецификации по уязвимостями, что являются следствием некачественных стандартов проектирования или неправильных проектных решений;
- **эксплуатации** продукта или системы, которые должны быть разработаны в полном соответствии с корректными спецификациями, но уязвимости возникают как результат неадекватного управления при эксплуатации.

Оценка и утверждение **целей функциональной безопасности** требуется для демонстрации заказчику или пользователю, что установленные цели проекта адекватны проблеме его безопасности. Существуют цели и функции безопасности для объекта или ПС и цели безопасности для среды. Рекомендуется сопоставлять эти цели безопасности с идентифицированными угрозами, которым они противостоят, и/или с политикой и предположениями, которым они должны соответствовать. Не все цели безопасности могут быть реализованы соответствующим объектом, так как некоторые могут зависеть от требований безопасности системы, выполняемых ее средой. В этом случае требования безопасности, относящиеся к внешней среде, необходимо ясно изложить и оценить в контексте требований к системе.

Доверие – основа для уверенности в том, что продукт или система отвечают целям и требованиям безопасности. Активное исследование доверия – это оценка процесса функционирования системы для определения его свойств безопасности. Методы оценки могут, в частности, включать в себя [22]:

- анализ и проверку выполнения процессов и процедур;
- проверку того, что процессы и процедуры действительно применяются;
- анализ соответствия реализации каждого положения проекта требованиям;
- верификацию доказательств правильности реализации функций;
- анализ руководств применения;
- анализ разработанных функциональных тестов и полученных результатов;

- независимое функциональное тестирование ПС и системы;
- анализ уязвимостей, включающий предположения о дефектах и ошибках.

В стандарте применяется иерархия детализации требований к безопасности и качеству систем и ПС с использованием специфических терминов: **класс** – наиболее общая характеристика качества, которая структурируется **семейством** – субхарактеристиками. Каждое семейство может иметь несколько **компонентов** – атрибутов, состоящих из **элементов** качества. Семейство доверия (качества) в стандарте может содержать один или несколько компонентов доверия. Этот подраздел семейства доверия включает описание имеющихся компонентов и объяснение их содержания и разграничения. Подраздел идентификации компонента содержит описательную информацию, необходимую для категорирования, регистрации и ссылок на компонент. Каждый элемент представляет собой требование для выполнения. Формулировки этих требований к ПС должны быть четкими, краткими и однозначными. Поэтому каждое требование рекомендуется излагать как отдельный элемент. Структура процессов жизненного цикла систем и программных средств, обеспечивающих информационную и функциональную безопасность применения в соответствии с классами и семействами стандарта, представлена на рис. 4.1.

Рассмотрим основные виды используемых классов, как наиболее общих характеристик качества ПС.

1. **Класс управление конфигурацией ПС** обеспечивает сохранение целостности объектов, устанавливая и контролируя определенный порядок процессов корректировки, модификации и предоставления связанной с ними информации. Этот класс предотвращает несанкционированную модификацию, добавление или уничтожение составляющих объектов, обеспечивая тем самым качество и документацию компонентов, которые подготовлены к распространению. *Управления конфигурацией* устанавливает уровень автоматизации, используемый для изменения элементов конфигурации. *Возможности управления* определяют характеристики системы УК. Область управления указывает на те элементы объектов, для которых необходим контроль со стороны системы управления конфигурацией.

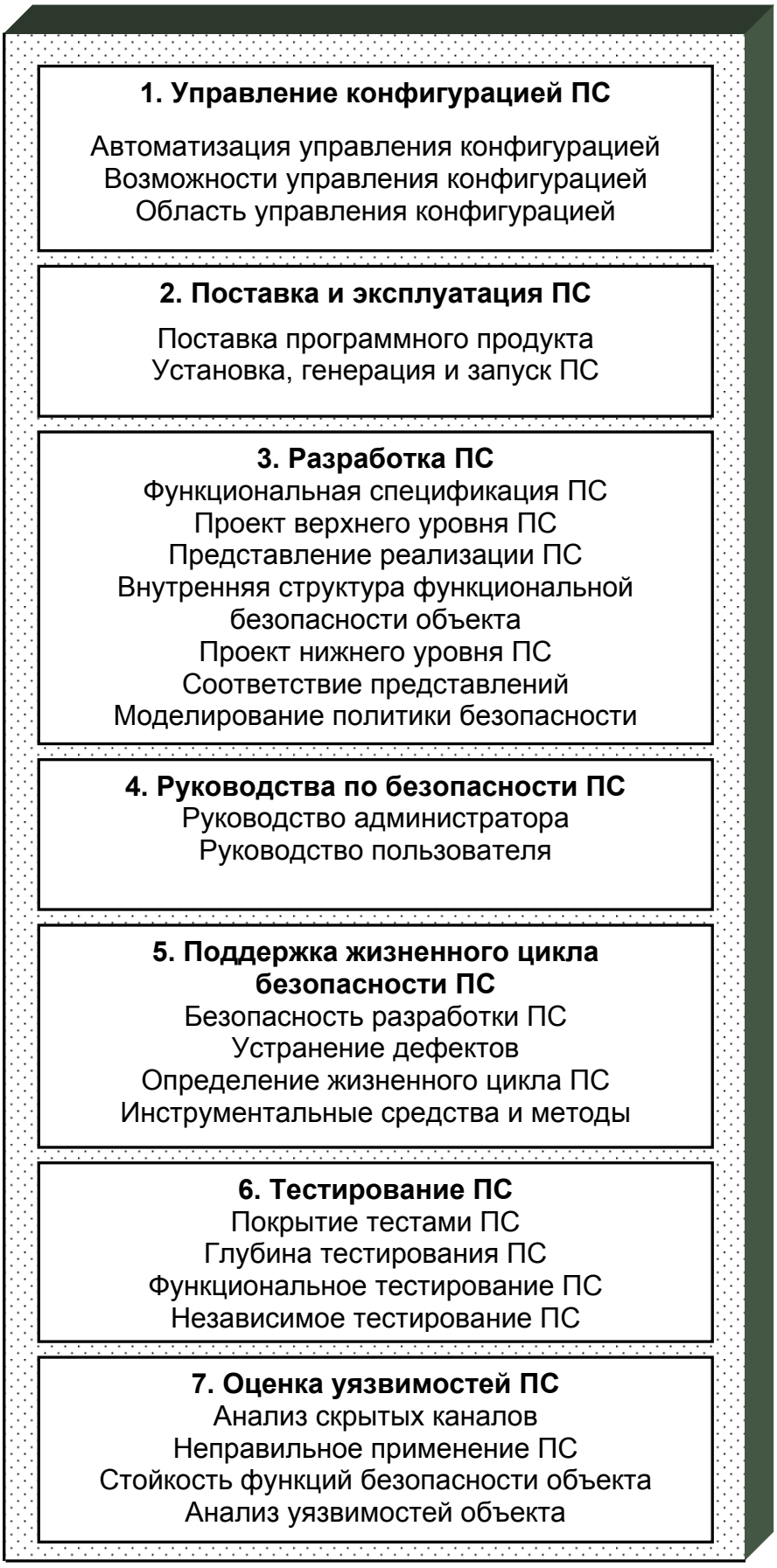

Рис. 4.1. **Управление информационной и функциональной безопасностью программных средств (ПС) в процессе их жизненного цикла [6]**

2. **Класс поставка и эксплуатация ПС** определяет требования к мерам, процедурам и стандартам, применяемым для безопасной поставки, установки и эксплуатации ПС, обеспечивая, чтобы безопасность объектов не нарушалась во время его распространения, внедрения и эксплуатации. *Поставка распространяется* на процедуры, используемые для поддержки безопасности во время передачи объекта пользователю при первоначальной поставке и последующих модификациях. Она включает в себя специальные процедуры, необходимые для демонстрации подлинности поставленного объекта. *Установка, генерация* и *запуск* предусматривает, чтобы копия объекта была конфигурирована и активизирована администратором так, чтобы показать те же самые свойства безопасности, что и у оригинала.

3. **Класс разработка ПС** определяет требования для пошагового уточнения функциональной безопасности, начиная с краткой спецификации объекта в задании на безопасность и вплоть до фактической реализации. Каждое из получаемых представлений содержит информацию, помогающую оценщику решить, были ли выполнены функциональные требования к безопасности. *Функциональная спецификация* описывает функции безопасности, и необходимо, чтобы она была полным и точным отображением требований безопасности объекта. Функциональная спецификация также детализирует его внешний интерфейс. Предполагается, что пользователи и заказчики объекта взаимодействуют с функциональной безопасностью через этот интерфейс.

Проект верхнего уровня – проектная спецификация самого высокого уровня, которая уточняет функциональную спецификацию безопасности системы в основных составляющих частях. Она идентифицирует базовую структуру функциональной безопасности, а также основные элементы аппаратных, программных и программно-аппаратных средств. *Представление реализации* – наименее абстрактное отражение функциональной безопасности. Оно фиксирует ее детализированное внутреннее содержание на уровне исходного текста, аппаратных схем и т.д. Требования к *внутренней структуре* определяют необходимое структурирование функций безопасности.

Проект нижнего уровня – детализированная проектная спецификация, уточняющая проект верхнего уровня до необходимой детализации, которая может быть использована как основа для

программирования и/или проектирования аппаратуры и программных компонентов. *Соответствие представлений* – демонстрация отображения между всеми смежными парами имеющихся представлений функций безопасности, от краткой спецификации объекта до наименее абстрактного из имеющихся представлений.

Модели политики безопасности – структурные представления методов, используемые для обеспечения повышенного доверия, что функциональная спецификация соответствует принятой политике безопасности и, в конечном счете, функциональным требованиям безопасности системы. Это достигается посредством определения соответствия между функциональной спецификацией, моделью политики безопасности и моделируемыми методами обеспечения безопасности ПС.

4. **Класс руководства по безопасности ПС** определяет требования, направленные на обеспечение понятности, достаточности и законченности эксплуатационной документации, представляемой разработчиком. Эта документация, которая содержит две категории информации (для пользователей и администраторов), является важным фактором безопасной эксплуатации объекта и ПС.

Требования к *руководству администратора* должны обеспечивать отражения ограничений среды, которые будут поняты администраторами и операторами. Руководство администратора – основной документ, имеющийся в распоряжении разработчика, для предоставления администраторам объекта детальной и точной информации о том, как осуществлять администрирование безопасным способом и эффективно использовать доступные процедуры обеспечения безопасности.

Требования к *руководству пользователя* должны обеспечивать возможность эксплуатировать объект безопасным способом. Руководство – основной документ, имеющийся в распоряжении разработчика, для предоставления пользователям необходимой общей и специфической информации о том, как правильно использовать функции безопасности. В руководстве необходимо осветить два аспекта. Во-первых, требуется объяснить, что делают доступные пользователю процедуры безопасности, и как они будут использоваться, чтобы пользователи имели возможность последовательно и действенно

защищать свою систему. Во-вторых, требуется разъяснить роль пользователя в поддержании безопасности системы и ПС.

5. **Класс поддержка жизненного цикла ПС** определяет требования для реализации всех этапов разработки четко определенной модели, включая политику и процедуры устранения недостатков и дефектов, правильное использование инструментальных средств и методов, а также меры безопасности для защиты среды разработки.

Безопасность разработки охватывает физические, процедурные, относящиеся к персоналу и другие меры безопасности, используемые применительно к среде разработки. Она также содержит требования к физической безопасности местоположения разработки и к контролю за отбором и наймом персонала разработчиков. *Устранение дефектов* обеспечивает, чтобы недостатки, обнаруженные потребителями, отслеживались и исправлялись, пока объект сопровождается разработчиком. Несмотря на то, что при оценке объекта не может быть принято решение о потенциальном соответствии требованиям устранения недостатков, можно оценить политику и процедуры, которые разработчик предусмотрел для выявления и устранения дефектов и распространения исправлений потребителям.

Определение жизненного цикла ПС устанавливает, что технология разработки, используемая разработчиком для создания объекта, включает в себя положения и действия, указанные в требованиях к процессу разработки и поддержке эксплуатации. Уверенность в соответствии объекта требованиям больше, когда анализ безопасности и подготовка свидетельств осуществляются на регулярной основе, как неотъемлемая часть процесса разработки и поддержки эксплуатации всей системы и ПС. *Инструментальные средства* и методы связаны с необходимостью определения средств разработки, используемых для анализа и создания объекта и ПС. Сюда включены требования, относящиеся к инструментальным средствам разработки и опциям этих инструментальных средств, зависящим от их реализации.

6. **Класс тестирование ПС** устанавливает требования, которые должны демонстрировать, что реализованные функции удовлетворяют функциональным требованиям безопасности системы. *Покрытие* тестами определяет их полноту и функциональность, выполненных разработчиком для анализа качества системы и ПС. Оно связано со степенью тестирования функций безопасности. *Глубина тестирования*

характеризуется уровнем детализации, на котором разработчик проверяет программы. Тестирование функций безопасности основано на последовательно увеличивающейся глубине информации, получаемой из анализа представлений безопасности.

Функциональное тестирование ПС должно устанавливать, что функции безопасности действительно демонстрируют свойства, необходимые для удовлетворения требований спецификации. Функциональное тестирование обеспечивает доверие, что функции удовлетворяют, по меньшей мере, требованиям выбранных функциональных компонентов. Эти процедуры сосредоточены на функциональном тестировании, выполняемом разработчиком. *Независимое тестирование* определяет степень выполнения функционального тестирования третьей стороной, кроме разработчика и заказчика. Эти процедуры повышают ценность тестирования добавлением тестов, которые расширяют тесты разработчика.

7. **Класс оценка уязвимости ПС** определяет требования, направленные на идентификацию уязвимостей, которые могут проявиться и быть активизированы. Особое внимание должно быть уделено уязвимостям, которые вносятся при проектировании, эксплуатации, неправильном применении или неверной конфигурации объекта. *Анализ скрытых каналов* направлен на выявление и анализ непредусмотренных коммуникационных каналов, которые могут применяться при нарушениях предписанных функций безопасности. Анализ *неправильного применения* позволяет выяснить, способен ли администратор или пользователь, используя руководства, определить, что система или ПС конфигурированы или эксплуатируются небезопасным способом.

Анализ стойкости функций безопасности объекта направлен на их определение с помощью вероятностного или перестановочного механизма. Даже если такие функции нельзя обойти, отключить или исказить, не исключено, что их все же можно преодолеть прямой атакой. Может быть заявлен уровень или специальная метрика стойкости для каждой из этих функций. Анализ *стойкости функций* выполняют для принятия решения, отвечают ли такие функции сделанным заявлениям. *Анализ уязвимостей* заключается в идентификации недостатков, которые могли быть внесены на различных этапах разработки. Эти потенциальные уязвимости оцениваются посредством тестирования

проникновения, позволяющим сделать заключение, могут ли они в действительности быть использованы для нарушения безопасности системы и ПС.

Для систематичного применения приведенных на рис. 4.1 классов и семейств требований в стандарте используется основное понятие **профиль защиты (ПЗ).**

> **Профиль защиты (ПЗ)** – независимая от реализации совокупность требований безопасности для некоторой категории объектов, отвечающая специфическим требованиям проекта и потребителя.

Цель разработки и оценки ПЗ – показать, что он является полным, непротиворечивым, технически правильным и поэтому пригоден для изложения конкретных требований к одному или нескольким типам объектов. Оцененный ПЗ пригоден в качестве основы для разработки задания по безопасности. Для принятия решения о достаточности требований безопасности в составе ПЗ важно, чтобы решаемая задача безопасности ясно понималась всеми участниками оценки.

Вторым основополагающим понятием является **задание по безопасности** (ЗП).

> **Задание по безопасности (ЗБ)** – совокупность требований и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта.

Цель оценки ЗБ – показать, что оно является полным, непротиворечивым, технически правильным и поэтому пригодно для использования в качестве основы при оценке уровня безопасности соответствующей системы.

4.3. Методология оценки безопасности информационных технологий по общим критериям

Центральными понятиями ОК являются: «**Функция безопасности**» (Security Function), которая определяется как «часть или части объекта оценки (ОО), обеспечивающие выполнение подмножества

взаимосвязанных правил политики безопасности ОО» и «Функции безопасности ОО» (TOE Security Functions), которые определяются как «совокупность всех аппаратных, программных и программно-аппаратных средств ОО, обеспечивающих адекватное осуществление политики безопасности ОО». В российских нормативных документах по защите информации от несанкционированного доступа для аналогичных понятий используются термины «средство защиты» и «комплекс средств защиты». Однако следует учитывать, что понятие «функция безопасности» имеет в ОК более общую и широкую трактовку, чем понятие «средство защиты».

Другим важнейшим понятием ОК является понятие «**доверие к безопасности**», выражаемое термином «assurance», которое в ОК определяется как «основание для уверенности в том, что сущность отвечает своим целям безопасности». В российской нормативной базе близкое к этому понятие определялось термином «гарантии проектирования».

Термин «Security Policy» в РД Гостехкомиссии России трактуется как «правила разграничения доступа». В ОК это понятие используется в более широком смысле. В частности, термин «TOE Security Policy» определяется как «совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО». Поэтому в отношении термина «Security Policy» используется перевод «политика безопасности».

Безопасность информационных технологий (ИТ) рассматривается в ОК с позиций предотвращения и уменьшения опасностей типа нежелательного или неоправданного распространения, изменения или потери информации или им подобных.

Безопасность связана с защитой активов от угроз, где угрозы классифицируются на основе потенциала злоупотребления защищаемыми активами. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека, преднамеренными или иными.

ОК применимы к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Объектами обеспечения безопасности могут выступать как отдельные продукты, так и законченные системы ИТ.

Продукт ИТ – это совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная как для непосредственного использования, так и для включения в различные системы ИТ.

Система ИТ – это конкретная реализация ИТ с определенными назначением и условиями эксплуатации, предназначенная для решения задач автоматизации в определенной области применения.

Продукт или система ИТ и соответствующая им документация руководств администратора и пользователя, являющиеся предметом оценки и сертификации по требованиям безопасности, называются *объектом оценки (ОО).*

К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателем (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Нарушения безопасности ИТ возникают вследствие преднамеренного использования или случайной активизации уязвимостей при применении ИТ по назначению.

Уязвимости могут возникать из-за недостатков в:

- требованиях – то есть ОО может обладать всеми требуемыми функциями и свойствами, но все же содержать уязвимости, которые делают его несоответствующим или неэффективным в части безопасности;
- проектировании – то есть ОО не удовлетворяет спецификации, и/или уязвимости являются следствием плохих технологий проектирования, неправильных проектных решений или внесенных дефектов;
- эксплуатации – то есть ОО разработан в полном соответствии с корректными спецификациями, но уязвимости возникают как результат неадекватного использования при эксплуатации.

Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности, составляет *политику безопасности организации.*

Безопасность ИТ составляет область интересов трех категорий лиц: *потребителей, разработчиков* и *оценщиков ОО.*

Потребители (заказчики) заинтересованы в формулировании обоснованных требований к безопасности ИТ, исходя из принятой ими политики безопасности и возможных угроз безопасности ИТ, и получении объективных оценок безопасности ОО, которые предназначены для защиты их информационных ресурсов. Потребители могут также использовать результаты оценки для сравнения различных продуктов и систем ИТ.

Разработчики должны осуществлять обоснованный выбор требований к безопасности продуктов и систем ИТ. Они должны также обеспечивать необходимый уровень доверия к реализации требований безопасности на основе выработки и соблюдения необходимых организационных и технологических мер при проектировании, разработке и оценке ОО.

Оценщики должны производить независимую оценку ОО на предмет их соответствия предъявленным требованиям безопасности.

Существенно, чтобы требования безопасности, налагаемые на ОО, эффективно содействовали достижению целей безопасности, установленных потребителями. Если соответствующие требования не установлены до начала процесса разработки, то даже хорошо спроектированный конечный продукт может не отвечать целям потребителей. Общая схема формирования требований к безопасности ОО представлена на рис. 4.2.

4.4. Оценка уровня доверия функциональной безопасности информационной технологии

Не все перечисленные выше классы и семейства процессов обеспечения функциональной безопасности систем и ПС целесообразно применять в каждом проекте. В зависимости от сложности и критичности требования к безопасности функционирования системы и доступных ресурсов для ее реализации, стандартом рекомендуется выбирать набор классов и семейств процессов, достаточных для обеспечения необходимого качества комплекса функциональной безопасности проекта – **оценочный уровень доверия**. Оценочные уровни доверия (ОУД) образуют возрастающую шкалу достигаемого качества безопасности, которая позволяет соотнести получаемый уровень качества с трудоемкостью его реализации и возможностью достижения этой степени доверия.

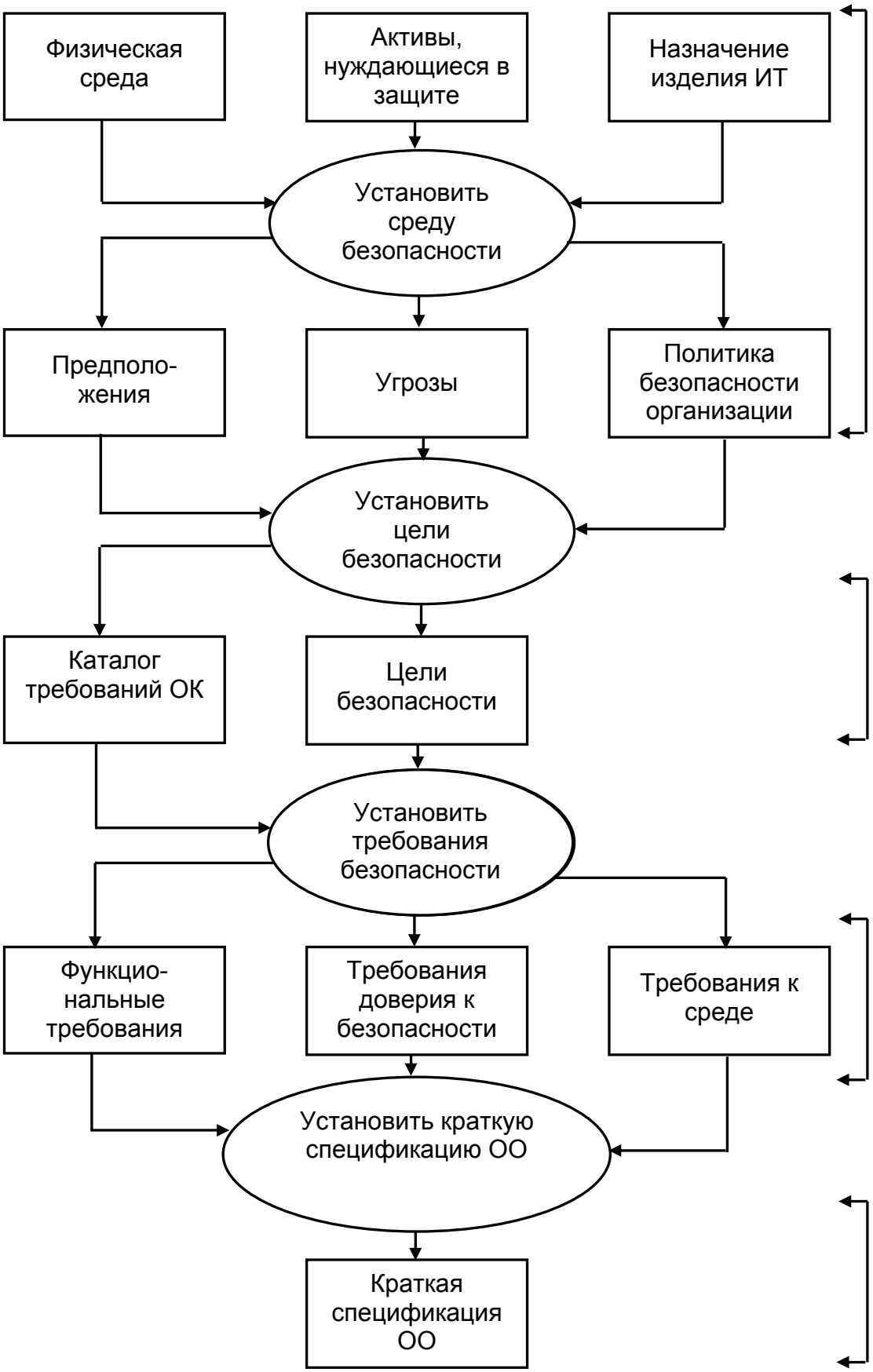

Рис. 4.2. **Формирование требований к безопасности ОО**

Не все классы и семейства настоящего стандарта включены в каждый из перечисленных ниже оценочных уровней доверия. Эти семейства рекомендуется использовать для повышения уровней доверия в тех ПЗ и ЗБ, для которых они действительно полезны и необходимы. Определены семь иерархически упорядоченных оценочных уровней доверия для ранжирования при выборе доверия к безопасности объектов оценки. (Они, в некоторой степени, подобны пяти уровням зрелости технологий в стандарте **ISO 15504**). Каждый последующий ОУД представляет более высокое доверие (гарантированное качество), чем любой из предыдущих. Связь уровней доверия с классами и семействами технологических процессов обеспечения ЖЦ безопасности систем и программных средств в стандарте иллюстрированы семью таблицами. В каждой из них выделены и отмечены обязательные (белые) и рекомендуемые (остальные) классы и семейства процессов, обеспечивающие определенный уровень доверия при создании и применении методов и средств соответствующей безопасности. Эти таблицы помогают выбирать технологии в соответствии с требованиями к безопасности системы и ПС с учетом доступных ресурсов.

Ниже для примера при рассмотрении классов доверия 3 и 7 приведены табл. 4.1, 4.2, характеризующих их содержание.

Оценочный уровень доверия 1 (ОУД1) – предусматривает функциональное тестирование и применим, когда требуется некоторая уверенность в правильном функционировании системы, а угрозы безопасности не рассматривают как серьезные. Он полезен там, где требуется, чтобы было уделено должное внимание безопасности, путем независимого тестирования на соответствие спецификации и экспертизы представленной документации. Предполагается, что оценка может успешно проводиться без помощи разработчика и с минимальными затратами, посредством анализа экспертами заданных функций безопасности с использованием функциональной спецификации, спецификации интерфейсов и руководств.

Оценочный уровень доверия 2 (ОУД2) – включает структурное тестирование, содержит требование сотрудничества с разработчиком для получения информации о проекте и результатах тестирования. Он применим в тех случаях, когда разработчикам или пользователям требуется независимо подтверждаемый уровень доверия (от невысокого до умеренного), при отсутствии доступа к полной документации при разработке. Такая ситуация может возникать при обеспечении безопасности разработанных ранее (наследуемых) систем или при

ограниченной доступности к ним разработчика. ОУД2 обеспечивает доверие посредством анализа применяемых функций безопасности с использованием функциональной спецификации, спецификации интерфейсов, руководств и проекта верхнего уровня. Этот уровень требует тестирования и анализа уязвимостей разработчиком, основанного на более детализированных спецификациях.

Оценочный уровень доверия 3 (ОУД3) – предусматривает методическое тестирование и проверку, позволяет разработчику достичь доверия путем применения проектирования безопасности без значительного изменения существующей технологии качественной разработки всей системы (табл. 4.1). ОУД3 применим в тех случаях, когда разработчикам или пользователям требуется независимо подтверждаемый умеренный уровень доверия на основе исследования системы и процесса ее разработки без существенных затрат на изменение технологии. Этот уровень представляет значимое увеличение доверия, требуя более полного покрытия тестированием функций и процедур безопасности.

Таблица 4.1

Класс доверия 3	Компоненты доверия
Управление конфигурацией	Средства контроля авторизации Охват УК объекта оценки
Поставка и эксплуатация	Процедуры поставки Процедуры установки, генерации и запуска
Разработка	Неформальная функциональная спецификация Детализация вопросов безопасности в проекте верхнего уровня Неформальная демонстрация соответствия
Руководства	Руководство администратора Руководство пользователя
Поддержка жизненного цикла	Идентификация мер безопасности
Тестирование	Анализ покрытия Тестирование: проект верхнего уровня Функциональное тестирование Выборочное независимое тестирование
Оценка уязвимостей	Экспертиза руководств Оценка стойкости функции безопасности Анализ уязвимостей разработчиком

Оценочный уровень доверия 4 (ОУД4) – предусматривает методическое проектирование, тестирование и углубленную проверку, что позволяет разработчику достичь максимального качества, основанного на регламентированной технологии разработки, которая не требует глубоких специальных знаний, навыков и других ресурсов. ОУД4 – самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться при оценке уже существующих продуктов. Анализ поддержан независимым тестированием, свидетельством разработчика об испытаниях, основанных на функциональной спецификации и проекте верхнего уровня, подтверждением результатов тестирования разработчиком и независимым анализом уязвимостей. Уровень также обеспечивает доверие посредством использования контроля среды разработки и дополнительного управления конфигурацией системы и ПС.

Оценочный уровень доверия 5 (ОУД5) – позволяет разработчику достичь максимального качества путем систематического проектирования безопасности, основанного на строгой технологии разработки, поддержанной умеренным применением узко специализированных методов, не влекущих излишних затрат на методы проектирования безопасности. Доверие достигается применением формальной модели политики безопасности и полуформального представления функциональной спецификации и проекта верхнего уровня системы, а также полуформальной демонстрации соответствия между ними. Кроме этого, требуется модульное проектирование системы. Анализ поддержан независимым свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проектах верхнего и нижнего уровня, независимым подтверждением результатов тестирования разработчиком и независимым анализом уязвимостей. ОУД5 также обеспечивает качество посредством использования контроля среды разработки и управления конфигурацией системы, требуя соблюдать структурированную архитектуру системы.

Оценочный уровень доверия 6 (ОУД6) – позволяет разработчикам достичь высокой безопасности путем полуформальной

верификации всего проекта и тестирования, применением специальных методов проектирования безопасности в строго контролируемой среде разработки с целью получения высокой безопасности системы и защиты активов от значительных рисков, где ценность защищаемых активов оправдывает дополнительные затраты. ОУД6 также обеспечивает повышение доверия посредством использования структурированного процесса разработки, контроля среды разработки и управления конфигурацией системы, включая полную автоматизацию, и свидетельства безопасности процедур поставки. Этот уровень представляет значительное увеличение доверия по сравнению с предыдущим, требует всестороннего анализа, структурированное представление реализации, более стройную структуру системы, всесторонний независимый анализ уязвимостей, систематическую идентификацию скрытых каналов, улучшенное управление конфигурацией и глубокий контроль среды разработки.

Оценочный уровень доверия 7 (ОУД7) – применим при разработке безопасных систем для использования в ситуациях чрезвычайно высокого риска и/или там, где высокая ценность активов или систем оправдывает максимальные затраты на их безопасность (табл. 4.2.). Практическое применение уровня ограничено системами, которые строго ориентированы на реализацию полных функциональных возможностей безопасности, для которых возможен и целесообразен подробный формальный анализ. Уровень обеспечивает качество посредством использования всех представленных выше классов и семейств, а также процессов предшествующих уровней, структурированного процесса разработки, средств контроля среды разработки и всестороннего управления конфигурацией системы, включая полную автоматизацию, и свидетельства безопасных процедур поставки. Этот уровень представляет значительное увеличение доверия, требует всестороннего анализа, использующего формальные представления и формальное соответствие, а также всестороннее независимое тестирование.

Таблица 4.2

Класс доверия 7	Компоненты доверия
Управление конфигурацией	Полная автоматизация УК Расширенная поддержка Охват УК инструментальных средств разработки
Поставка и эксплуатация	Предотвращение модификации Процедуры установки, генерации и запуска
Разработка	Формальная функциональная спецификация Формальный проект верхнего уровня Структурированная реализация функциональной безопасности Минимизация сложности Полуформальный проект нижнего уровня Формальная демонстрация соответствия Формальная модель политики безопасности
Руководства	Руководство администратора Руководство пользователя
Поддержка жизненного цикла	Достаточность мер безопасности Измеримая модель жизненного цикла Соответствие всех частей объекта оценки стандартам реализации
Тестирование	Строгий анализ покрытия Тестирование на уровне реализации Упорядоченное функциональное тестирование Полное независимое тестирование
Оценка уязвимостей	Систематический анализ скрытых каналов Анализ и тестирование опасных состояний Оценка стойкости функции безопасности Высокостойкий

4.5. Обзор классов и семейств ОК

Классы и семейства функциональных требований в рассматриваемом стандарте ISO 15408 сгруппированы на основе определенной функции или цели и представлены в ОК в алфавитном

порядке. Всего в разделе "Требования к функциям безопасности" ОК **девять** классов, **76** семейств, **184** компонента и **380** элементов. Назовем эти классы [6].

Класс FAU. (*Аудит Безопасности*) состоит из 12 семейств, содержащих требования по распознаванию, регистрации, хранению и анализу информации, связанной с действиями, относящимися к безопасности ОО.

Класс FCO. (*Связь*) включает два семейства, связанных с определением идентичности сторон, участвующих в обмене данными: идентичности отправителя информации и идентичности получателя переданной информации.

Класс FDP. (*Защита Данных Пользователя*) включает 15 семейств, определяющих требования для функций безопасности ОО и политики функции безопасности ОО, связанной с защитой данных пользователя. Класс FDP подразделен на пять групп семейств, которые адресованы защите данных пользователя в пределах ОО в процессе ввода, вывода и хранения информации.

Класс FIA. (*Идентификация и Аутентификация*) включает девять семейств. Семейства в этом классе содержат требования для функций, предназначенных для установления и проверки требуемой идентичности пользователя. Эффективность других классов требований (например, Защита Данных Пользователя, Аудит Безопасности) зависит от правильной идентификации и аутентификации пользователей.

Класс FPR. (*Секретность*) включает четыре семейства и содержит требования секретности, обеспечивающие защиту пользователя от раскрытия и неправильного употребления его идентификаторов другими пользователями.

Класс FPT. (*Защита Функций Безопасности*) включает 22 семейства функциональных требований, которые касаются целостности и контроля механизмов, обеспечивающих функции безопасности (ФБ), и целостности и контроля данных ФБ. Может показаться, что семейства в этом классе дублируют компоненты в **к**лассе FDP (Защита Данных Пользователя); они могут даже быть реализованы, используя те же самые механизмы. Однако, класс FDP сосредотачивается на защите данных пользователя, в то время как класс FPT – на защите данных ФБ. Фактически, компоненты от класса FPT необходимы даже при

отсутствии любой защиты данных пользователя, обеспечивая доверие осуществлению политики, определенной в ПЗ/ЗБ.

Класс FRU. (*Использование Ресурса*) включает три семейства, которые определяют готовность требуемых ресурсов к обработке и/или хранению информации.

Класс FTA. (*Доступ к ОО*) включает семь семейств, которые определяют функциональные требования, сверх требований идентификации и аутентификации, для управления сеансом работы пользователя.

Класс FTP. (*Надежный Маршрут/Канал*) включает два семейства, которые содержат требования по обеспечению надежного маршрута связи между пользователями и ФБ и надежного канала связи между ФБ, имеющих следующие общие характеристики:

- маршрут коммуникаций построен с использованием внутренних и внешних каналов коммуникаций, которые изолируют идентифицированный поднабор данных и команд ФБ от других частей ФБ и данных пользователя;
- использование маршрута коммуникаций может быть инициализировано пользователем и/или ФБ;
- маршрут коммуникаций способен обеспечить гарантии того, что пользователь сообщается с нужной ФБ и что ФБ сообщается с нужным пользователем, то есть обеспечивается надежная идентификация конечных пунктов.

Требования доверия безопасности, по сравнению с функциональными, представляются более проработанными, поскольку для них определены удобные на практике оценочные уровни доверия (ОУД).

Для большинства областей применения достаточно третьего уровня доверия; с другой стороны, этот уровень достижим при разумных затратах на разработку, так что его можно считать типовым.

В число требований доверия третьего оценочного уровня входят:

- анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации;
- независимое тестирование;
- наличие проекта верхнего уровня;
- анализ стойкости функций безопасности;
- поиск разработчиком явных уязвимостей;

- контроль среды разработки;
- управление конфигурацией.

В принципе достижим и четвертый оценочный уровень, который можно рекомендовать для конфигураций повышенной защищенности. В число дополнительных требований этого уровня входят:

- полная спецификация интерфейсов;
- наличие проектов нижнего уровня;
- анализ подмножества реализации;
- применение неформальной модели политики безопасности;
- независимый анализ уязвимостей;
- автоматизация управления конфигурацией.

Вероятно это самый высокий уровень, который можно достичь при существующей технологии программирования и разумных затратах материальных и временных ресурсов.

Последовательность проведения оценки безопасности ИТ на основе ОК может показана в виде схемы (рис. 4.3.)

Результатом оценки должен быть общий вывод, в котором описана степень соответствия объекта оценки функциональным требованиям и требованиям гарантированности.

После оценки изделия ИТ, предназначенного для широкого использования, результаты оценки могут быть включены в каталог оцененных изделий, чтобы они стали доступными более широкому кругу потребителей.

ОК поддерживают выбор и оценку безопасности объекта ИТ. ОК полезны при разработке изделий или систем ИТ с функциями безопасности и при приобретении коммерческих изделий и систем с такими функциями. ОК дают основу для оценки объекта, чтобы установить уровень доверия к безопасности ИТ.

К таким объектам относятся, например, операционные системы, сети компьютеров, распределенные системы, прикладные программы.

Аспекты безопасности ИТ включают защиту информации от несанкционированного раскрытия, модификации или потери возможности использования при воздействии угроз, являющихся результатом преднамеренных или непреднамеренных действий человека. Защищенность от этих трех типов угроз обычно называют конфиденциальностью, целостностью и доступностью.

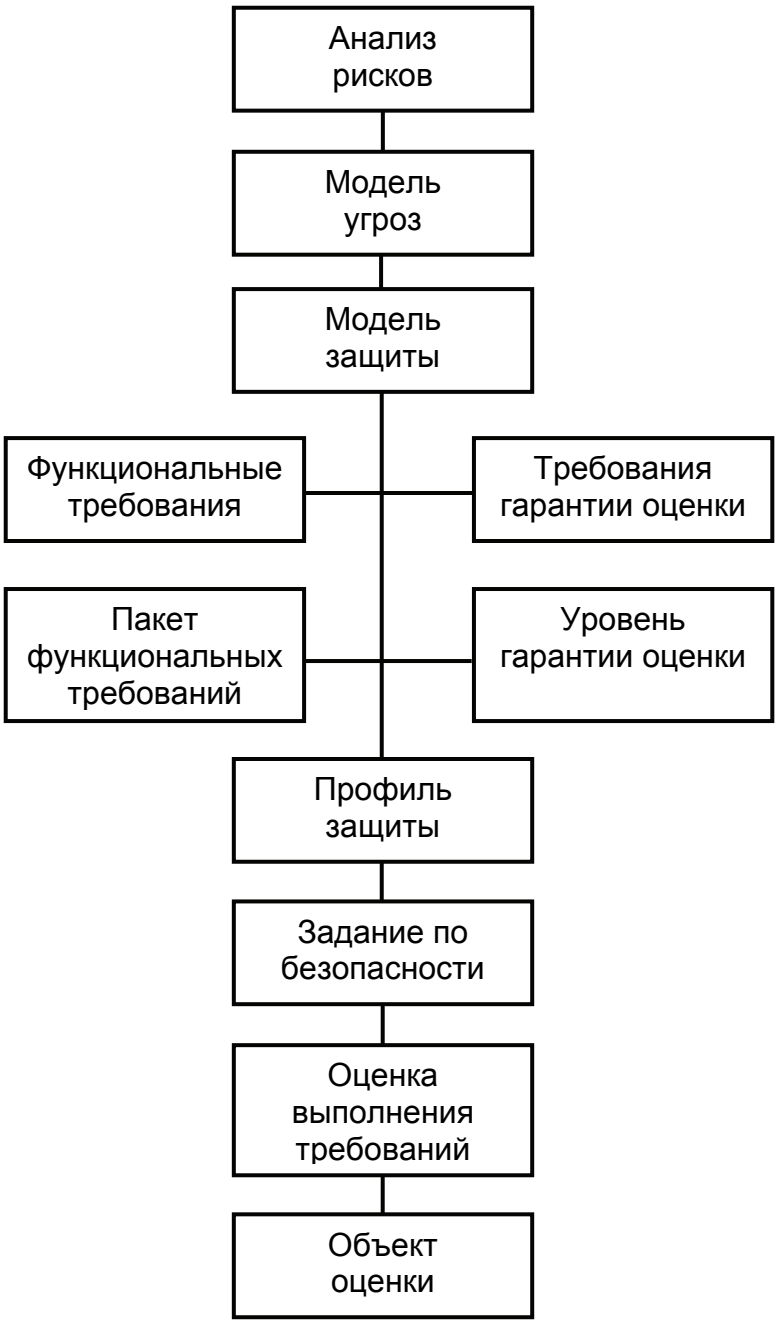

Рис. 4.3. **Общая схема оценки безопасности ИТ на основе общих критериев**

ОК могут быть также применимы и к другим аспектам безопасности ИТ.

ОК применимы при оценке безопасности ИТ, включая как аппаратные средства, так и программное обеспечение.

Некоторые аспекты безопасности ИТ находятся вне рамок ОК. К ним относятся следующие:

1. ОК не охватывают оценку административных мер безопасности. Административные меры безопасности в окружающей среде объекта оценки рассматриваются только в той части, где они могут влиять на способность ИТ противостоять идентифицированным угрозам.

2. В ОК не рассматривается оценка технических аспектов безопасности ИТ типа электромагнитного излучения.

3. ОК формулируют только критерии оценки и не содержат методик самой оценки, а также административных структур, которые должны их использовать. Однако ожидается, что ОК будут использоваться для оценки такими структурами и в таких методиках.

4. Вне рамок ОК процедуры для использования результатов оценки при приеме системы в эксплуатацию, так как это уже административный процесс.

5. В ОК не входят критерии для оценки специфических качеств криптографических методов и алгоритмов защиты информации.

Контрольные вопросы

1. Опишите статус стандарта ISO 15408 в РФ.

2. Что включает в себя понятие «доверие» в рамках стандарта ISO15408?

3. Какие классы и семейства используются для оценки безопасности ПС?

4. Дайте определение понятиям «профиль защиты» и «Задание по безопасности».

5. Что определяет оценочный уровень доверия (ОУД)?

6. Какой оценочный уровень доверия является типовым (наиболее используемым) и почему?

7. Изложите общую схему оценки безопасности ИТ на основе общих критериев.

Глава 5. Международный стандарт управления информационной безопасностью ISO 17799

5.1. Назначение стандарта ISO 17799 для управления информационной безопасностью

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте **ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной**

безопасностью), принятом в 2000 году. ISO 17799 является ни чем иным, как международной версией британского стандарта BS 7799, принятого в 1995г. и поддерживаемого в настоящее время в 27 странах мира.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Этот стандарт стал основой для организации аудита ИБ. Стандарт ISO 17799 включает 10 разделов.

1. **Политика безопасности**
2. **Организационные меры по обеспечению безопасности**
   - Организация и управления информационной безопасностью
   - Безопасность доступа сторонних организаций
   - Условия безопасности в контрактах, заключенных со сторонними организациями
3. **Классификация ресурсов и их контроль**
   - Инвентаризация ресурсов
   - Классификация ресурсов
4. **Безопасность персонала**
   - Безопасность при выборе и работе с персоналом
   - Обучение персонала
   - Реагирование на события, угрозу безопасности
5. **Физическая безопасность**
   - Защищенные области
   - Защита оборудования
6. **Администрирование компьютерных систем и вычислительных сетей**
   - Рабочие процедуры и ответственность
   - Планирование работы систем и их приемка
   - Защита от вредоносного программного обеспечения
   - Обслуживание систем
   - Сетевое администрирование
   - Оперирование с носителями информации и их защита
   - Обмен данными и программами

7. **Управление доступом к системам**
   - Производственные требования к управлению и системам
   - Управление доступом пользователей
   - Обязанности пользователей
   - Управление доступом к сети
   - Управление доступом к компьютерам
   - Управление доступом к приложениям
   - Слежение за доступом к системам и их использование
8. **Разработка и сопровождение информационных систем**
   - Требования к безопасности систем
   - Безопасность в прикладных системах
   - Защита файлов прикладных программ
   - Безопасность в среде разработки и рабочей среде
9. **Планирование бесперебойной работы организации**
   - Вопросы планирования бесперебойной работы организации
   - Тестирование планов обеспечения бесперебойной работы организации
10. **Соответствие системы основным требованиям**
    - Выполнение правовых требований
    - Проверка безопасности информационных систем
    - Аудит систем

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Одними из наиболее важных понятий при управлении информационной безопасностью на основе стандарта ISO 17799 являются ключевые средства контроля. **Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.**

Выделено десять ключевых средств контроля, которые представляют собой либо обязательные требования, например, требования действующего законодательства, либо считаются основными структурными элементами информационной безопасности, например, обучение правилам безопасности. Эти средства контроля актуальны для всех организаций и сред функционирования

автоматизированных систем (АС) и составляют основу системы управления информационной безопасностью. Они служат в качестве основного руководства для организаций, приступающих к реализации средств управления информационной безопасностью.

Ключевыми являются следующие **десять средств контроля**:

- **Документ о политике информационной безопасности.**
- **Распределение обязанностей по обеспечению информационной безопасности.**
- **Обучение и подготовка персонала к поддержанию режима информационной безопасности.**
- **Уведомление о случаях нарушения защиты.**
- **Средства защиты от вирусов.**
- **Планирование бесперебойной работы организации.**
- **Контроль над копированием программного обеспечения, защищенного законом об авторском праве.**
- **Защита документации организации.**
- **Защита данных.**
- **Контроль соответствия политике безопасности.**

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования.

Одной из основных целей проведения аудита ИБ с использованием стандарта ISO 17799 является получение соответствующих сертификатов. Это дает предприятию или фирме ряд преимуществ. Прежде всего, после проведения аудита информационная система "компании" становится «прозрачнее» для менеджмента, выявляются основные угрозы безопасности для бизнес-процессов, вырабатываются рекомендации по повышению текущего уровня защищенности для защиты от обнаруженных угроз и по устранению недостатков в системе безопасности и управления. В результате компании предлагается комплексный план внесения изменений в систему управления информационной безопасностью, как для повышения реального уровня защищенности, так и для соответствия стандарту.

Сертификация на соответствие стандарту ISO 17799 (BS 7799) позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании налажено эффективное управление информационной безопасностью. Это обеспечивает компании дополнительное конкурентное преимущество.

Кроме того, говоря о сертификации по ISO 17799, стоит принять во внимание согласованную с ВТО процедуру принятия России в данную организацию. Эта процедура потребует адекватной реакции от наиболее значимых в экономике России структур и адаптации стратегии развития в области информационных технологий с учетом международных стандартов безопасности, таких как ISO 17799.

5.2. Практика прохождения аудита и получения сертификата ISO 17799

Для получения сертификата соответствия ISO 17799 компания должна пройти процедуру аудита информационной безопасности, провести подготовку информационной системы на соответствие требованиям стандарта, внедрить изменения и провести окончательную проверку соответствия стандарту. Данную работу целесообразно разбить на несколько этапов.

Предварительный этап заключается в проведении аудита, на основании которого производится подготовка необходимых изменений системы управления информационной безопасностью. Его может выполнить специализированная компания, имеющая опыт в проведение подобных работ.

Затем, после подготовки комплекта необходимых документов и внесения изменений в систему, необходимо провести итоговую проверку соответствия стандарту ISO 17799, для чего требуется участие специалистов одной из консалтинговых компаний, которые владеют эксклюзивным правом выдачи данного сертификата и имеют аккредитацию при United Kingdom Accreditation Service (UKAS), уполномоченном государственном органе Великобритании. Также, отметим, что в настоящее время до выхода 2-й части ISO 17799 — требования к аудиторам, которая намечена на 2004 год, официальная

сертификация возможно только по BS 7799. Однако между ISO и UKAS существует соглашение, согласно которому после принятия второй части ISO 17799 все сертификаты BS 7799 автоматически получат статус ISO 17799.

Для подготовки к проведению аудита необходимо проанализировать состояние информационной безопасности предприятия по всем рассмотренным выше 10 разделам стандарта ISO 17799.

Ниже приведена характеристика содержания этих разделов [8].

5.3. Раздел 1. Политика безопасности

Цель: сформулировать и обеспечить поддержку информационной безопасности руководством организации.

Высшее руководство должно поставить четкую цель и всестороннее оказывать свою поддержку информационной безопасности посредством распространения политики безопасности среди сотрудников организации.

Необходимость разработанной соответствующей политики безопасности на сегодняшний день является очевидным фактом для любой, даже достаточно небольшой компании.

Политика безопасности в целом – это совокупность программных, аппаратных, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, четко регламентирующих все аспекты деятельности компании, включая информационную систему, и обеспечивающих их безопасность.

Политика безопасности является одним из важнейших, жизненно важных документов компании. Кроме своего прямого назначения, разработка политики безопасности дает дополнительный эффект: в результате анализа информационных потоков, инвентаризации информационных ресурсов и ранжирования обрабатываемой информации по степени ценности руководство организации получает целостную картину одного из самых сложных объектов управления - информационной системы, что положительно влияет на качество управления бизнеса в целом, и, как следствие, улучшает его прибыльность и эффективность.

Основные положения политики обеспечения информационной безопасности включают:

А. Определение информационной безопасности, перечень ее составляющих.

Б. Положение о целях управления - поддержка целей и принципов информационной безопасности.

В. Краткое разъяснение политики безопасности, принципов ее построения и стандартов в этой области.

Соответствие политики требованиям, имеющим особое значение для организации:

1) соответствие положений политики местному и международному законодательству;

2) обучение персонала по вопросам безопасности;

3) обнаружение и блокирование вирусов и других вредоносных программ;

4) непрерывность ведения бизнеса;

5) последствия нарушения политики безопасности

Г. Включение в должностные обязанности руководителей ответственности за обеспечение информационной безопасности, включая отчеты об инцидентах

Д. Подробный перечень документов, которые должны быть изданы вместе с политикой безопасности (положения, инструкции, регламенты и т.п.)

В результате выполнения работ на этом этапе формируется письменный документ о политике безопасности, который должен быть доступен всем сотрудникам, отвечающим за обеспечение режима информационной безопасности.

Высшее руководство должно предоставить задокументированную политику информационной безопасности всем подразделениям организации. Этот документ должен содержать следующие вопросы.

1. Определение информационной безопасности, ее основные цели и область ее применения, а также ее значение как механизма, позволяющего коллективно использовать информацию.

2. Изложение позиции руководства по вопросам реализации целей и принципов информационной безопасности.

3. Разъяснение конкретных вариантов политики безопасности, принципов, стандартов и требований к ее соблюдению, включая:

- **выполнение правовых и договорных требований;**

- **требования к обучению персонала правилам безопасности;**
- **политика предупреждения и обнаружения вирусов;**
- **политика обеспечения бесперебойной работы организации.**

4. Определение общих и конкретных обязанностей по обеспечению режима информационной безопасности.

5. Разъяснение процесса уведомления о событиях, таящих угрозу безопасности.

Необходимо разработать процесс проверки, определить обязанности и даты проверок для соблюдения требований документа о политике безопасности.

Прежде всего, обратим внимание на требование стандарта перечислить все объекты информационной инфраструктуры, подлежащие защите. Это не просто сделать даже в средних компаниях, не говоря уже о крупных. Зачастую эта задача решается с привлечением внешней аудиторской фирмы, специализирующейся на вопросах информационной безопасности.

Поэтому при разработке политики безопасности чрезвычайно важно учесть специфику существующего законодательства. Для этого необходимо привлекать юристов, хорошо владеющих вопросами права в области информационных технологий, телекоммуникаций и информационной безопасности.

Последствия в случае нарушений политики безопасности. Этот раздел требует особого внимания. Зачастую компании забывают четко проработать моменты, связанные с наступлением той или иной ответственности в случае нарушения политики безопасности. В связи с этим, злоумышленники могут остаться безнаказанными даже в случае их обнаружения, выявления и доказательства умышленности их злонамеренных действий. В зависимости от наступивших последствий и юридического статуса нарушителя к нему могут быть применены дисциплинарные, административные или уголовные меры воздействия.

Определение ответственности за обеспечение информационной безопасности – это то, о чем необходимо всегда помнить и это то, что должно проходить единым стержнем через всю политику безопасности. Определение ответственности - это краеугольный камень политики безопасности и это то, что о чем так часто забывают при ее разработке [8].

По сложившейся практике за все аспекты деятельности компании персональную ответственность несет руководитель. Очевидно, однако,

что он не может лично обеспечивать информационную безопасность, поэтому без конкретизации, без точного определения, кто именно и за что именно несет ответственность в компании, никакая, даже самая совершенная система защиты работать соответствующим образом не будет. Поэтому необходима детальная проработка вопросов, связанных с распределением обязанностей и разграничением ответственности.

5.4. Раздел 2. Организационные меры по обеспечению информационной безопасности

5.4.1. Организация управления информационной безопасностью

Цель: Управлять информационной безопасностью в организации.

Чтобы инициировать и контролировать процесс обеспечения информационной безопасности, необходимо создать в организации соответствующую структуру управления.

В организации должны проводиться регулярные совещания руководства для разработки и утверждения политики безопасности, распределения обязанностей по обеспечению защиты и координации действий по поддержанию режима безопасности. В случае необходимости следует привлечь специалистов по вопросам защиты информации для консультаций. Необходимо вступать в контакты со специалистами других организаций, чтобы быть в курсе современных направлений и промышленных стандартов, а также, чтобы установить соответствующие деловые отношения для рассмотрении случаев нарушения защиты. Следует всячески поощрять комплексный подход к проблемам информационной безопасности, например, совместную работу аудиторов, пользователей и администраторов для эффективного решения проблем.

Ответственность за обеспечение информационной безопасности несут все члены руководящей группы. Поэтому руководству организации необходимо регулярно проводить совещания, посвященные проблемам защиты информации, чтобы вырабатывать четкие указания по этому вопросу, а также оказывать административную поддержку инициативам по обеспечению безопасности.

Обычно на подобных совещаниях рассматриваются следующие вопросы:

а) анализ и утверждение политики информационной безопасности и распределение общих обязанностей;

б) отслеживание основных угроз, которым подвергаются информационные ресурсы;

в) анализ и слежение за инцидентами в системе безопасности;

г) утверждение основных инициатив, направленных на усиление защиты информации.

Рекомендуется, чтобы один из членов руководящей группы взял на себя основную ответственность за координацию действий по проведению политики безопасности в жизнь.

Координация действий по защите информации

В крупной организации возможно потребуется координация мер по обеспечению информационной безопасности посредством проведения совещания, в котором будут участвовать руководители разных подразделений.

Такое совещание, в работе которого принимают участие представители руководства каждого из подразделений организации, зачастую необходимо для того, чтобы координировать действия по реализации защитных мер. Обычно на таком совещании:

а) согласовываются конкретные функции и обязанности по обеспечению информационной безопасности в организации;

б) согласовываются конкретные методики и процессы защиты информации, например, оценка рисков, система классификации средств защиты;

в) согласовывается и оказывается поддержка инициативам по защите информации в организации, например, программе обучения персонала правилам безопасности;

г) обеспечивается включение защитных мер в процесс планирования использования информации;

д) координируются действия по реализации конкретных мер по обеспечению информационной безопасности новых систем или сервисов;

е) создаются благоприятные условия для информационной безопасности во всей организации.

Необходимо четко определить обязанности по защите отдельных ресурсов и выполнению конкретных процессов обеспечения безопасности. Политика информационной безопасности должна давать общие рекомендации по распределению функций и обязанностей по защите информации. Там, где необходимо, следует дополнить эти рекомендации более подробными разъяснениями, касающимися конкретных систем или сервисов; в этих дополнениях нужно четко определить ответственных за конкретные ресурсы (как физические, так и информационные) и за процессы обеспечения защиты, например, за планирование бесперебойной работы организации.

Защита информационной системы должна быть обязанностью ее владельца. Владельцы информационных систем могут делегировать свои полномочия по защите отдельным пользователям-администраторам или поставщикам услуг. Тем не менее, владельцы все равно несут ответственность за обеспечение безопасности системы.

Чтобы избежать каких-либо недоразумений, касающихся отдельных обязанностей, крайне важно четко определить **зоны ответственности каждого администратора** и, в частности, следующее:

1. Различные ресурсы и процессы обеспечения безопасности, связанные с каждой системой, необходимо идентифицировать и четко определить.

2. Кандидатура администратора, отвечающего за каждый ресурс или процесс обеспечения защиты, должна быть согласована, а его обязанности задокументированы.

3. Уровни полномочий необходимо четко определить и задокументировать.

Следует определить процедуру утверждения новых информационных систем руководством.

Необходимо рассмотреть два уровня полномочий по их утверждению:

1. У т в е р ж д е н и е р у к о в о д с т в о м . Каждая установка систем должен быть утверждена соответствующим руководством, которое дает разрешение на ее проведение. Необходимо также получить разрешение от администратора, отвечающего за поддержание режима локальной информационной безопасности; это гарантирует, что

установка систем будут соответствовать политике безопасности и требованиям к ней.

2. Техническое утверждение. В случае необходимости проверить, все ли устройства, подключенные к коммуникационным сетям, или сопровождаемые конкретным поставщиком услуг имеют тип, который был утвержден.

Следует поощрять контакты специалистов по защите информации из штата организации со специалистами из других организаций (промышленных или правительственных) по их усмотрению. Такое взаимодействие дает возможность обмена опытом и оценками угроз режиму безопасности, а также способствует разработке согласованных правил в промышленности, что помогает устранить препятствия на пути установления деловых отношений между организациями.

Важно также поддерживать соответствующие контакты с правоохранительными органами, поставщиками информационных сервисов и телекоммуникационными органами, чтобы обеспечить своевременное установление контактов и получение рекомендаций в случае инцидента в системе безопасности.

Обмен информацией по вопросам безопасности должен быть ограничен, чтобы гарантировать, что конфиденциальная информация организации не попадет в руки лиц, не имеющих соответствующие полномочия.

Независимый анализ информационной безопасности

В документе о политике информационной безопасности определяются обязанности по защите информации и формулируется соответствующая политика. Реальные процедуры обеспечения информационной безопасности должны быть подвергнуты независимому анализу, чтобы быть уверенным, что используемые организацией процедуры защиты соответствуют принятой политике безопасности, а также являются реализуемыми и эффективными.

Кандидатами на выполнение такого анализа являются внутренняя аудиторская служба, независимый старший администратор или сторонняя организация, специализирующаяся на сертификации соответствия политике безопасности в тех случаях, когда они имеют надлежащую квалификацию и опыт.

5.4.2. Безопасность доступа сторонних организаций

Цель: Обеспечить безопасность информационных ресурсов организации, к которым имеют доступ сторонние организации.

Особое внимание должно быть уделено доступу сторонних организаций к информационным ресурсам данной организации, для контроля которого разрабатывается комплекс дополнительных мероприятий.

Там, где доступ сторонних организаций необходим по производственным причинам, следует провести анализ рисков нарушения защиты, чтобы определить его последствия для системы безопасности и требования к средствам контроля. Эти средства контроля должны быть согласованы и определены в контракте, заключенном со сторонней организацией.

Такой доступ может быть предоставлен и другим участникам.

Контракты, разрешающие доступ сторонних организаций, должны включать в себя правила для доступа других участников и условия их доступа.

Если в связи с деятельностью организации возникает необходимость в подключении к узлу сторонней организации, следует выполнить оценку рисков, чтобы определить, необходимы ли какие-либо специальные меры по защите информации. При анализе риска следует принять во внимание тип предоставляемого доступа, ценность информации, принятые сторонней организацией меры защиты и последствия от доступа для безопасности информационной инфраструктуры организации.

Доступ сторонних организаций к информационным ресурсам данной организации может быть разрешен только после того, как приняты все необходимые защитные меры и подписан договор, определяющий условия подключения.

При заключении контрактов со сторонними организациями, которым необходим доступ к информационным ресурсам, должны быть оговорены или внесены в содержание контракта следующие вопросы:

а) общая политика информационной безопасности; разрешенные способы доступа, а также контроль и использование уникальных идентификаторов пользователей и паролей;

б) описание каждого предоставляемого информационного сервиса;

в) требование вести список лиц, которым разрешено использовать сервис;

г) время и дата, когда сервис будет доступен;

е) процедуры, касающиеся защиты ресурсов организации, включая информацию;

ж) обязанности, касающиеся правовых вопросов, например, законодательство о защите данных;

з) право отслеживать действия пользователей;

и) право проверять договорные обязательства;

к) ограничения на копирование и раскрытие информации;

л) меры по обеспечению возврата или уничтожения информации и ресурсов по окончании срока действия контракта;

м) необходимые меры по физической защите;

н) механизмы для обеспечения реализации защитных мер;

п) меры по обеспечению защиты от компьютерных вирусов;

р) процедура предоставления разрешения на доступ пользователей.

5.5. Раздел 3. Классификация ресурсов и их контроль

5.5.1. Инвентаризация ресурсов

Цель: Обеспечить надлежащую защиту ресурсов организации.

Все основные информационные ресурсы в рамках организации должны быть учтены и иметь назначенного владельца.

Ответственность за ресурсы позволяет обеспечить их надлежащую защиту. Следует определить владельцев основных ресурсов и назначить ответственных за реализацию соответствующих защитных мер. Ответственность за реализацию защитных мер может быть передана другому лицу, однако назначенный владелец ресурса все равно несет ответственность за него.

Инвентаризация ресурсов помогает убедиться в том, что обеспечивается их эффективная защита, кроме того, перечень ресурсов

может потребоваться для других производственных целей, например, при принятии мер по охране здоровья и по технике безопасности, для страхования или финансовых целей. Инвентаризацию необходимо провести для всех основных ресурсов, связанных с каждой информационной системой. Каждый ресурс должен быть четко идентифицирован, а его владелец и категория секретности согласованы и задокументированы. Примерами ресурсов, связанных с информационными системами, являются:

а) информационные ресурсы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, операционные процедуры и процедуры поддержки, планы обеспечения бесперебойной работы организации, процедуры перехода на аварийный режим;

б) программные ресурсы: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

в) физические ресурсы: компьютеры и коммуникационное оборудование, магнитные носители данных (ленты и диски), другое техническое оборудование (блоки питания, кондиционеры), мебель, помещения;

г) сервисы: вычислительные и коммуникационные сервисы, другие технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха).

5.5.2. Классификация ресурсов

Цель: Обеспечить надлежащий уровень защиты информационных ресурсов.

Различная информация имеет разную степень конфиденциальности и важности. Некоторые виды информации могут потребовать дополнительной защиты или специального обращения. Систему классификации информации по категориям секретности необходимо использовать для определения соответствующего набора уровней защиты и для уведомления пользователей о необходимости специального обращения с этой информацией.

Категории секретности и связанные с ними защитные меры для производственной информации должны учитывать производственную необходимость в коллективном использовании информации или ограничении доступа к ней, а также ущерб для организации, связанный с несанкционированным доступом или повреждением информации. В частности, следует рассмотреть необходимость обеспечения следующих мер:

а) **конфиденциальности**: производственная необходимость коллективного использования или ограничения доступа к информации по отношению к конфиденциальности и средствам контроля, требуемым для ограничения доступа к информации;

б) **целостности**: производственная необходимость осуществления контроля за внесением изменений в информацию и средства контроля, требуемые для обеспечения точности и полноты информации;

в) **доступности**: производственная необходимость обеспечения доступа к информации, когда это требуется, и необходимые для этого средства контроля.

Ответственность за присвоение категории секретности конкретному виду информации, например, документу, файлу данных или дискете, а также за периодическую проверку этой категории, следует возложить на лицо, создавшее эти данные, или на их назначенного владельца.

Секретная информация и выходные данные систем, поддерживающих секретную информацию, должны иметь соответствующие грифы секретности. Однако часто информация перестает быть конфиденциальной через некоторый промежуток времени, например, когда она становиться общедоступной. Это следует принять во внимание, так как чрезмерное засекречивание информации может привести к неоправданным, дополнительным затратам организации.

Выходные данные информационных систем, содержащие секретную информацию, должны иметь соответствующий гриф секретности. Этот гриф должен отражать категорию секретности наиболее уязвимой информации в выводимых данных. Примерами таких выходных данных являются печатные отчеты, информация, выводимая на экраны дисплеев, данные, хранимые на магнитных носителях

(лентах, дисках, кассетах), электронные сообщения и передаваемые файлы.

При рассмотрении этого вопроса всегда необходимо помнить, что чрезмерное засекречивание информации может привести к неоправданным, дополнительным затратам организации.

5.6. Раздел 4. Безопасность персонала

5.6.1. Безопасность при выборе и работе с персоналом

Цель: Уменьшить риск ошибок персонала, краж, мошенничества или незаконного использования ресурсов.

Аспекты, связанные с безопасностью, следует учитывать еще на стадии набора персонала, включать их в должностные инструкции и договоры, а также контролировать в течение всего времени работы данного сотрудника.

Руководители должны убедиться в том, что в должностных инструкциях отражена вся соответствующая данной должности ответственность за безопасность. Следует надлежащим образом проверить принимаемых на работу лиц, особенно если они будут работать с конфиденциальной информацией. Весь персонал организации и пользователи информационных ресурсов из сторонних организаций должны подписать обязательство о конфиденциальности (неразглашении).

Безопасность в должностных инструкциях. Обязанности и ответственность за безопасность, установленные принятой в организации политикой информационной безопасности (см. Политика информационной безопасности), следует включать в должностные инструкции, где это необходимо. В инструкциях необходимо отразить как общую ответственность за проведение в жизнь или поддержку политики безопасности, так и конкретные обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите.

Проверка принимаемых на работу. Заявления о приеме на работу следует тщательно рассмотреть, если работа в данной

должности связана с доступом к конфиденциальным информационным ресурсам. Всех кандидатов на занятие подобных вакансий следует проверить по следующим пунктам:

а) как минимум две положительных характеристики, одна деловых и одна личных качеств;

б) проверка (полноты и точности) сведений, сообщенных претендентом на вакансию в своей автобиографии;

в) подтверждение академических степеней и профессиональной квалификации;

г) проверка идентификации (например, паспорта);

д) проверка кредита для занятых в наиболее критичных заданиях, например, проверка финансового состояния.

Соглашение о конфиденциальности. Пользователи информационных ресурсов организации должны подписать соответствующее обязательство о конфиденциальности (неразглашении). Обычно служащие организации подписывают такое обязательство при приеме на работу.

Пользователи из сторонних организаций, не предусмотренные условиями существующего договора (обязательство о неразглашении является его частью), должны подписать обязательство о неразглашении, прежде чем им будет предоставлен доступ к информационным ресурсам организации.

Обязательства о неразглашении необходимо пересматривать, когда изменяются условия найма или договор, особенно если служащие должны уволиться из организации или если кончаются сроки действия договора.

Условия работы персонала. В соответствии со стандартом, при приеме на работу новых сотрудников необходимо, чтобы они ознакомились и подписали:

- Письменную формулировку их должностных обязанностей.
- Письменную формулировку прав доступа к ресурсам компании (в том числе и информационным).
- Соглашение о конфиденциальности.
- Специальные соглашения о перлюстрации всех видов служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

Пример такого соглашения компании с персоналом может быть представлен в следующем виде:

Вся информация, находящаяся на электронных носителях рабочих станций и в вычислительных сетях компании, является собственностью компании.

Подразделения и лица, уполномоченные на то руководством компании, имеют право в установленном порядке, без уведомления пользователей, производить проверки соблюдения требований настоящей Инструкции, а также осуществлять контроль за данными, находящимися на электронных носителях. В целях осуществления указанных действий они могут получить доступ к любым данным пользователей, находящихся на электронных носителях рабочих станций и в сети, а пользователь обязан предоставить требуемую ими информацию.

Компания имеет право без согласия пользователя передавать информацию, хранящуюся на электронных носителях, третьим лицам, включая правоохранительные органы и иные организации, уполномоченные на это действующим законодательством.

Любые компоненты корпоративной сети могут использоваться пользователями только для выполнения своих служебных обязанностей.

Использование компонентов сети не по назначению, использование, нарушающее требования настоящей Инструкции, приказов и распоряжений руководства компании (Директора, Технического Директора, руководителей подразделений), а также использование, которое наносит вред компании, в зависимости от тяжести наступивших последствий может повлечь за собой дисциплинарную (включая увольнение), административную или уголовную ответственность.

5.6.2. Обучение персонала

Цель: Убедиться в том, что пользователи осведомлены об угрозах нарушения режима информационной безопасности и понимают значение защиты, а также имеют необходимые навыки для выполнения процедур, необходимых для нормального функционирования системы безопасности организации.

Понимая и особо выделяя важность человеческого фактора для обеспечения надежной защиты информационной системы компании, стандарт ISO 17799 подчеркивает необходимость наладить постоянный процесс повышения уровня технической грамотности и информированности пользователей в области информационной

безопасности. Для этого необходимо регулярное проведение тренингов, посвященных общим правилам информационной защиты. Этим будет достигнуто постоянное напоминание пользователям основных правил и требований компании по обеспечению информационной безопасности. Особенно важно проводить подобные тренинги для вновь поступившего на работу персонала и в случае внесения в информационную систему каких-либо изменений (принятие новых технологий, прикладных автоматизированных систем, смены оборудования, ОС, ключевых приложений, принятие новых правил или инструкций и т.д.)

Пользователи должны быть обучены процедурам защиты и правильному обращению с информационными ресурсами.

Необходимо также официально, в письменной форме, утвердить разрешенный пользователям доступ (права и ограничения).

Пользователи должны получить необходимые сведения о политике организации и принятых в ней процедурах, включая требования к безопасности и другим средствам контроля, а также научиться правильно пользоваться информационными ресурсами (например, знать процедуру входа в систему, уметь пользоваться пакетами программ) перед тем, как они получат доступ к информационным сервисам.

Эти меры необходимы для того, чтобы гарантировать, что процедуры защиты выполняются правильно, и для сведения риска нарушения конфиденциальности, целостности и доступности данных из-за ошибки пользователя к минимуму.

Этой политики следует придерживаться как в отношении сотрудников организации, так и в отношении пользователей из сторонних организаций.

Реагирование на события, таящие угрозу безопасности. О событиях, затрагивающих безопасность, необходимо немедленно сообщать по административным каналам.

Все сотрудники и подрядчики должны быть ознакомлены с процедурой уведомления о различных типах инцидентов (нарушение безопасности, угроза, слабость или сбой), которые могут повлиять на безопасность ресурсов организации. Следует обязать пользователей без промедления сообщать обо всех наблюдаемых или подозрительных случаях такого рода в соответствующую службу поддержки системы защиты. В организации должна быть установлена формальная

процедура наложения дисциплинарных взысканий на сотрудников, которые нарушают режим безопасности.

Уведомление об инцидентах в системе безопасности. О событиях, таящих угрозу безопасности, следует без промедления сообщать по административным каналам.

Следует установить формальную процедуру уведомления, а также процедуру реагирования на события, описывающую меры, которые надлежит принять по получении сообщения об инциденте. Все сотрудники и подрядчики должны быть ознакомлены с этой процедурой; они обязаны сообщать о такого рода событиях в соответствующую службу поддержки системы защиты.

Уведомление о слабых местах в системе безопасности. Пользователи информационных сервисов обязаны регистрировать любые наблюдаемые или предполагаемые слабости в системе безопасности, либо угрозы системам или сервисам и сообщать о них. Пользователи должны незамедлительно доводить подобные инциденты до сведения своего непосредственного руководства, либо поставщиков соответствующих услуг. Необходимо информировать пользователей о том, что ни при каких обстоятельствах они не должны пытаться проверять предполагаемые слабости в системы защиты. Это нужно для защиты самих пользователей, поскольку их действия по тестированию слабости могут быть истолкованы как попытки несанкционированного использования системы.

Уведомление об отказах программного обеспечения. Следует обязать пользователей информационных сервисов регистрировать все случаи, когда функционирование программного обеспечения представляется им неправильным, т.е. не соответствующим спецификации; они должны сообщать об этом в местную службу технической поддержки информационных систем или непосредственно поставщику данных услуг.

Следует установить процедуры, которые немедленно должен выполнить пользователь, подозревающий, что сбой вызван вредоносной программой, например, компьютерным вирусом. При разработке таких процедур следует обратить особое внимание на следующие моменты:

1. Записать симптомы и все сообщения, появляющиеся на экране.

2. Прекратить работу на компьютере и, если возможно, отключить его. Немедленно сообщить об инциденте в службу технической поддержки информационных систем. Если оборудование подлежит осмотру, то его необходимо отсоединить от сетей организации, прежде чем снова включить питание. Не использовать на других компьютерах дискеты, записанные на этом компьютере.

3. Немедленно сообщить о происшествии в службу поддержки системы защиты.

Ни при каких обстоятельствах пользователи не должны пытаться удалить подозрительное программное обеспечение. Восстановление программного обеспечения должны выполнять специалисты, имеющие соответствующие знания и опыт работы.

Процедура наложения дисциплинарных взысканий. Следует определить формальную процедуру наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые в организации политику и процедуры безопасности. Эта процедура должна служить сдерживающим фактором для сотрудников, которые склонны пренебрегать процедурами защиты. Кроме того, она должна обеспечивать правильное и справедливое рассмотрение дел сотрудников, подозреваемых в серьезном или постоянном нарушении безопасности. Процедура наложения дисциплинарных взысканий должна быть разработана с учетом кадровой политики организации и утверждена руководством.

5.7. Раздел 5. Физическая безопасность и безопасность окружающей среды

Требования к физической защите могут значительно варьировать от организации к организации, в зависимости от масштаба и структуры предоставляемых информационных сервисов, а также от уязвимости и критичности поддерживаемых производственных процессов**.**

Крупные организации, имеющие специальные центры данных, обычно требуют более высокий уровень защиты своих информационных систем, чем небольшие организации, использующие офисную технологию. Тем не менее понятие защищенных областей, контролируемых периметров, контроля доступа в помещения и общие

меры по защите оборудования применимы к любой организации в соответствующей интерпретации.

5.7.1. Защищенные области

Цель: Предотвратить несанкционированный доступ к информационным сервисам, их повреждение и создание помех в их работе.

Информационные системы, поддерживающие критически важные или уязвимые сервисы организации, должны быть размещены в защищенных областях.

Такие системы должны быть также защищены физически от несанкционированного доступа, повреждения и помех. Их следует разместить в защищенных областях, ограниченных определенным периметром безопасности, с надлежащим контролем доступа в помещения и защитными барьерами.

Физический периметр безопасности. Физическая защита должна быть основана на определенных периметрах безопасности и обеспечиваться путем установки в организации ряда барьеров, расположенных в стратегических местах. Требования к каждому защитному барьеру и его месторасположению должны определяться ценностью ресурсов и сервисов, подлежащих защите, а также рисками нарушения безопасности и существующими защитными мерами. Каждый уровень физической защиты должен иметь определенный периметр безопасности, в пределах которого должен быть обеспечен надлежащий уровень защиты.

Для определения физического периметра безопасности должны учитываться следующие рекомендации:

1. Периметр безопасности должен соответствовать ценности защищаемых ресурсов и сервисов.
2. Периметр безопасности должен быть четко определен.
3. Вспомогательное оборудование (например, фотокопировальные аппараты, факс-машины) должны быть так размещены, чтобы уменьшить риск несанкционированного доступа к защищенным областям или компрометации конфиденциальной информации.

4. Физические барьеры должны по необходимости простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение и загрязнение окружающей среды.

5. Не следует предоставлять посторонним лицам информацию о том, что делается в защищенных областях без надобности.

6. Следует рассмотреть возможность установления запрета на работу в одиночку без надлежащего контроля; это необходимо как для безопасности, так и для предотвращения вредоносных действий.

7. Компьютерное оборудование, принадлежащее организации, следует размещать в специально предназначенных для этого местах, отдельно от оборудования, контролируемого сторонними организациями.

8. В нерабочее время защищенные области должны быть физически недоступны (закрыты на замки) и периодически проверяться охраной.

9. Персоналу, осуществляющему техническое обслуживание сервисов, должен быть предоставлен доступ в защищенные области только в случае необходимости и после получения разрешения. По необходимости доступ такого персонала (особенно к конфиденциальным данным) следует ограничить, а их действия следует отслеживать.

10. В пределах периметра безопасности использование фотографической, звукозаписывающей и видео аппаратуры должно быть запрещено, за исключением санкционированных случаев.

Контроль доступа в помещения. В защищенных областях следует установить надлежащий контроль доступа в помещения, чтобы только персонал, имеющий соответствующие полномочия, имел к ним доступ. Предлагается рассмотреть следующие средства контроля:

1. За посетителями защищенных областей необходимо установить надзор, а дата и время их входа и выхода должны регистрироваться. Посетителям должен быть предоставлен доступ для конкретных, разрешенных целей.

2. Весь персонал, работающий в защищенных областях, должен носить на одежде хорошо различимые идентификационные карточки; кроме того, следует рекомендовать им спрашивать пропуск у незнакомых лиц.

3. Необходимо немедленно изъять права доступа в защищенные области у сотрудников, увольняющихся с данного места работы.

Защита центров данных и компьютерных залов. Центры данных и компьютерные залы, поддерживающие критически важные сервисы организации, должны иметь надежную физическую защиту. При выборе и обустройстве соответствующих помещений необходимо принять во внимание возможность повреждения оборудования в результате пожара, наводнения, взрывов, гражданских беспорядков и других аварий. Следует также рассмотреть угрозы безопасности, которые представляют соседние помещения.

Необходимо рассмотреть следующие меры:

1. Разместить ключевые системы подальше от общедоступных мест и мест прохождения общественного транспорта.
2. Здания не должны привлекать внимание и выдавать свое назначение (по возможности); не должно быть явных признаков как снаружи, так и внутри здания, указывающих на присутствие вычислительных ресурсов.
3. Внутренние телефонные справочники не должны указывать на местонахождение вычислительных ресурсов.
4. Опасные и горючие материалы следует хранить в соответствии с инструкциями на безопасном расстоянии от месторасположения вычислительных ресурсов. Не следует хранить расходные материалы для компьютеров, например, бумагу для принтеров в компьютерных залах.
5. Резервное оборудование и носители информации, на которых храняться резервные копии, следует разместить на безопасном расстоянии, чтобы избежать их повреждение в случае аварии на основном рабочем месте.
6. Следует установить соответствующее сигнальное и защитное оборудование, например, тепловые и дымовые детекторы, пожарную сигнализацию, средства пожаротушения, а также предусмотреть пожарные лестницы. Сигнальное и защитное оборудование необходимо регулярно проверять в соответствии с инструкциями производителей. Сотрудники должны быть надлежащим образом подготовлены к использованию этого оборудования.
7. Процедуры реагирования на чрезвычайные ситуации необходимо полностью задокументировать и регулярно тестировать.

8. Двери и окна должны быть заперты, когда в помещении в данное время никого нет. Следует рассмотреть возможность защиты окон снаружи.

Изолированные места разгрузки и загрузки оборудования и материалов. Рекомендуется выделить помещение для разгрузки и загрузки материалов и оборудования для того, чтобы уменьшить вероятность несанкционированного доступа в компьютерные залы. Требования к безопасности такого помещения следует определить, исходя из оценки рисков. Предлагаются следующие рекомендации:

1. Доступ к складским помещениям снаружи здания должен предоставляться только проверенному персоналу, имеющему соответствующие полномочия.

2. Складское помещение должно быть так спланировано, чтобы материалы можно было разгружать без получения доступа в другие помещения здания.

3. Внешняя дверь в складское помещение должна быть заперта, когда открыта внутренняя дверь.

4. Необходимо установить, какую потенциальную опасность могут представлять собой поступающие материалы, прежде чем их переместить из складского помещения в месту назначения.

Правила использования рабочего стола. Организациям настоятельно рекомендуется ввести правила использования рабочего стола, касающиеся документов и дискет, чтобы уменьшить риск несанкционированного доступа, потери и повреждения информации в нерабочее время.

Носители информации, оставленные на рабочих столах, могут быть повреждены или уничтожены в результате аварии, например, пожара, наводнения или взрыва.

Предлагаются следующие рекомендации:

1. Бумажная документация и дискеты, когда они не используются, должны храниться в специальных шкафах, особенно в нерабочее время.

2. Конфиденциальная или критически важная производственная информация, когда она не используется, должна храниться отдельно (лучше всего в несгораемом шкафу), особенно в нерабочее время.

3. Персональные компьютеры и компьютерные терминалы, когда они не используются, необходимо защитить с помощью блокировки с ключом, паролей или других средств контроля.

4. Следует рассмотреть необходимость защиты входящей и исходящей почты, а также факс-машин, оставленных без присмотра.

Вынос имущества за пределы организации. Сотрудникам запрещается выносить оборудование, данные и программы за пределы организации без письменного разрешения руководства.

5.7.2. Защита оборудования

Цель: Предотвратить потерю, повреждение и компрометацию ресурсов, а также перебои в работе организации.

Необходимо обеспечить физическую защиту оборудования от угроз нарушения безопасности и опасностей, представляемых окружающей средой. Защита оборудования информационных систем (включая оборудование, используемое за пределами организации) необходима как для того, чтобы уменьшить риск несанкционированного доступа к данным, так и для того, чтобы не допустить его потерю или повреждение. Следует также уделить внимание проблемам размещения оборудования и его утилизации. Могут потребоваться специальные меры для защиты от несанкционированного доступа и других опасностей, а также для защиты вспомогательного оборудования, например, системы электропитания и кабельной разводки.

Размещение и защита оборудования. Оборудование информационных систем должно быть так размещено и защищено, чтобы уменьшить риск, связанный с воздействием окружающей среды и несанкционированным доступом. Предлагаются следующие рекомендации:

1. Оборудование следует размещать так, чтобы по возможности свести к минимуму излишний доступ в рабочие помещения. Рабочие станции, поддерживающие конфиденциальные данные, должны быть расположены так, чтобы они были всегда на виду.

2. Следует рассмотреть возможность изоляции областей, требующих специальной защиты, чтобы понизить необходимый уровень общей защиты.

3. Для идентификации возможных опасностей предлагается использовать следующий контрольный список:

- пожар;

- задымление;
- затопление;
- запыление;
- вибрация;
- влияние химических веществ;
- помехи в электропитании;
- электромагнитные излучения и наводки;
- кража.

4. Следует запретить прием пищи и курение в местах размещения компьютерного оборудования.

Следует рассмотреть возможность использования специальной защиты, например, клавиатурных мембран, для оборудования в промышленных средах.

Источники электропитания. Оборудование необходимо защищать от сбоев в системе электропитании и других неполадок в электрической сети. Источник питания должен соответствовать спецификациям производителя оборудования.

Следует рассмотреть необходимость использования резервного источника питания. Для оборудования, поддерживающего критически важные производственные сервисы, рекомендуется установить источник бесперебойного питания. План действий в чрезвычайных ситуациях должен включать меры, которые необходимо принять по окончании срока годности источников бесперебойного питания. Оборудование, работающее с источниками бесперебойного питания, необходимо регулярно тестировать в соответствии с рекомендациями изготовителя.

Защита кабельной разводки. Кабели электропитания и сетевые кабели для передачи данных необходимо защищать от вскрытия для целей перехвата информации и повреждения. Для уменьшения такого риска в помещениях организации предлагается реализовать следующие защитные меры:

Кабели электропитания и линии связи, идущие к информационным системам, должны быть проведены под землей (по возможности) или защищены надлежащим образом с помощью других средств.

Необходимо рассмотреть меры по защите сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, например, воспользовавшись экранами или проложив эти линии так, чтобы они не проходили через общедоступные места.

Техническое обслуживание оборудования. Необходимо осуществлять надлежащее техническое обслуживание оборудования, чтобы обеспечить его постоянную доступность и целостность. Предлагаются следующие рекомендации:

1. Техническое обслуживание оборудования должно осуществляться через промежутки времени, рекомендуемые поставщиком, и в соответствии с инструкциями.
2. Ремонт и обслуживание оборудования должен выполнять только персонал поддержки, имеющий соответствующие полномочия.
3. Необходимо регистрировать все неисправности и неполадки.

Защита оборудования, используемого за пределами организации. Использование оборудования информационных систем (независимо от того, кто им владеет), поддерживающих производственные процессы, за пределами организации должно быть санкционировано руководством; уровень защиты такого оборудования должен быть таким же, как и для оборудования, расположенного на территории организации. Предлагаются следующие рекомендации:

1. Сотрудникам запрещается использовать персональные компьютеры для продолжения работы на дому, если не установлена процедура проверки на наличие вирусов (см. Средства защиты от вирусов).
2. Во время поездок запрещается оставлять оборудование и носители информации в общедоступных местах без присмотра. Портативные компьютеры следует провозить в качестве ручного багажа.
3. Во время поездок портативные компьютеры уязвимы по отношению к кражам, потери и несанкционированного доступа. Для таких компьютеров следует обеспечить надлежащую защиту доступа, чтобы предотвратить несанкционированный доступ к хранящейся в них информации.
4. Следует всегда соблюдать инструкции производителя, касающиеся защиты оборудования, например, защищать оборудование от воздействия сильных электромагнитных полей.

Надежная утилизация оборудования. Данные организации могут быть скомпрометированы вследствие небрежной утилизации оборудования. Перед утилизацией оборудования все его компоненты, включая носители информации, например, жесткие диски, необходимо проверять, чтобы гарантировать, что конфиденциальные данные и

лицензированное программное обеспечение было удалено. Поврежденные запоминающие устройства, содержащие особо ценные данные, могут потребовать оценки рисков для того, чтобы определить, следует ли их уничтожать, ремонтировать или избавиться от них.

5.8. Раздел 6. Администрирование компьютерных систем и вычислительных сетей

5.8.1. Рабочие процедуры и ответственность

Цель: Обеспечить корректную и надежную работу компьютерных систем и вычислительных сетей.

Необходимо определить обязанности и процедуры по администрированию и обеспечению функционирования всех компьютеров и сетей.

Это должно быть подкреплено соответствующими рабочими инструкциями и процедурами реагирования на события. Для уменьшения риска небрежного или несанкционированного использования систем, следует по необходимости применять принцип разделения обязанностей.

Документированные операционные процедуры должны быть подготовлены для всех функционирующих компьютерных систем с целью обеспечения их корректной и надежной работы. Документированные процедуры следует также подготовить для работ, связанных с разработкой, сопровождением и тестированием систем, особенно если это требует поддержки и внимания со стороны других подразделений организации, например, отдела управления компьютерными системами.

Процедуры должны включать в себя подробные корректные инструкции по выполнению каждого задания, в том числе (по необходимости) следующие пункты:

1) корректное оперирование с файлами данных;

2) требования к планированию выполнения заданий, включая взаимосвязи с другими системами, а также самое раннее и самое позднее время начала и окончания выполнения заданий;

3) инструкции по обработке ошибок и других исключительных ситуаций, которые могут возникнуть во время выполнения заданий, в том числе ограничения на использование системных утилит (см. Использование системных утилит);

4) обращение за помощью к персоналу поддержки в случае возникновения технических и других проблем, связанных с эксплуатацией компьютерных систем;

5) специальные инструкции по оперированию с выходными данными, такими, как использование специальной бумаги для печатающих устройств или администрирование конфиденциальных выходных данных, включая процедуры надежного удаления выходной информации от сбойных заданий;

6) процедуры перезапуска и восстановления работоспособности систем, используемые в случае их отказа.

Документированные процедуры должны быть также подготовлены для работ по обслуживанию систем, связанных с администрированием компьютеров и сетей, в том числе процедуры запуска и останова компьютеров, резервное копирование данных, техническое обслуживание оборудования, управление компьютерными залами и обеспечение их защиты. Операционные процедуры должны рассматриваться как формальные документы, изменения в которые следует вносить только после их утверждения руководством, наделенным соответствующими полномочиями.

Процедуры реагирования на события. Для обеспечения своевременного, эффективного и организованного реагирования на события, таящие угрозу безопасности, необходимо определить соответствующие управленческие обязанности и процедуры. Предлагаются следующие рекомендации по определению процедур реагирования на события:

1. Процедуры должны включать в себя все возможные типы инцидентов в системе безопасности, в том числе:

- отказы систем и потеря сервиса;
- ошибки, проистекающие от неполноты или неточности производственных данных;

- случаи нарушения конфиденциальности.

2. Кроме обычного плана действий в экстремальных ситуациях (предназначенного для того, чтобы как можно быстрее восстановить работоспособность систем и сервисов), процедуры должны включать в себя:

- анализ и выявление причины инцидента;
- планирование и реализация мер по предотвращению повторения инцидента;
- ведение контрольного журнала регистрации событий и сбор аналогичной информации;
- взаимодействие с пользователями и другими лицами, пострадавшими от инцидента или участвующими в процессе восстановления систем.

3. Ведение контрольного журнала регистрации событий и сбор аналогичной информации необходимы:

- для анализа внутренних проблем;
- использования в качестве свидетельства возможного нарушения условий контракта или технических нормативов;
- ведения переговоров с поставщиками программных средств и услуг о выплате компенсации;
- использования в качестве свидетельства в случае судебных разбирательств, попадающих под законодательство о несанкционированном использовании компьютерных систем и защите данных.

4. Необходимо осуществлять тщательный и формальный контроль за мерами по восстановлению систем после нарушения режима безопасности и их отказов. Процедуры должны обеспечивать следующее:

- предоставление разрешения на доступ к рабочим системам и данным только персоналу, имеющему соответствующие полномочия;
- подробное документирование всех мер, предпринимаемых в чрезвычайных ситуациях;
- доведение мер, предпринимаемых в чрезвычайных ситуациях, до сведения руководства и их организованный анализ;
- подтверждение целостности производственных систем и средств управления безопасностью с минимальной задержкой.

Разделение обязанностей. Разделение обязанностей позволяет свести риск небрежного или несанкционированного использования систем к минимуму, поэтому следует уделить особое внимание разделению определенных обязанностей или зон ответственности, чтобы уменьшить вероятность несанкционированной модификации или использования данных и сервисов. В частности, рекомендуется, чтобы выполнение следующих функций не было поручено одним и тем же сотрудникам:

- использование производственных систем;
- ввод данных;
- обеспечение функционирования компьютеров;
- сетевое администрирование;
- системное администрирование;
- разработка и сопровождение систем;
- управление процессом внесения изменений;
- администрирование средств защиты;
- контроль (аудит) средств защиты.

Разделение программных средств разработки и рабочих программ. Работы, связанные с разработкой и тестированием систем, могут привести к непреднамеренному внесению изменений в программы и данные, совместно используемые в одной и той же вычислительной среде. Поэтому целесообразно провести разделение программных средств разработки и рабочих программ для уменьшения риска случайного внесения изменений или несанкционированного доступа к рабочему программному обеспечению и производственным данным. Предлагаются следующие средства контроля:

1. Программные средства разработки и рабочие программы должны по возможности запускаться на разных процессорах или в разных директориях/сегментах сети.

2. Работы по разработке и тестированию систем необходимо разнести настолько, насколько это возможно.

3. Компиляторы, редакторы и другие системные утилиты не должны храниться вместе с рабочими системами, если в этом нет необходимости.

4. Для уменьшения риска путаницы, следует использовать разные процедуры входа в рабочие и тестируемые системы. Необходимо приучать пользователей к использованию разных паролей для входа в

эти системы, а система меню должна выводить на экран соответствующие идентификационные сообщения.

Работа со сторонними организациями. Привлечение подрядчика со стороны к администрированию компьютерных систем и вычислительных сетей может привести к дополнительному риску нарушения режима безопасности, например, к возможности компрометации, повреждения или потери данных в организации подрядчика. Необходимо заблаговременно выявить такой риск и включить в контракт надлежащие защитные меры по его уменьшению, согласованные с подрядчиком.

Следует рассмотреть следующие конкретные вопросы:

а) необходимость идентификации особо уязвимых или критически важных приложений, вынос которых за пределы организации нежелателен;

б) необходимость получения санкции на использование производственных приложений от их владельцев;

в) последствия для планов обеспечения бесперебойной работы организации;

г) стандарты безопасности, подлежащие определению, и процесс проверки их соблюдения;

д) обязанности и процедуры по уведомлению об инцидентах в системе безопасности и реагированию на них (Процедуры реагирования на события).

5.8.2. Планирование работы систем и их приемка

Цель: Свести риск отказов систем к минимуму.

Для обеспечения доступности ресурсов и надлежащей нагрузочной способности систем, требуется заблаговременное планирование и подготовка.

Чтобы уменьшить риск перегрузки систем, необходимо оценить будущие потребности в их нагрузочной способности на основе прогноза. Эксплуатационные требования к новым системам следует определить, задокументировать и проверить до их приемки. Требования к переходу на аварийный режим для сервисов, поддерживающих многочисленные приложения, должны быть согласованы и регулярно пересматриваться.

Планирование нагрузки. Для того чтобы избежать отказов систем вследствие их недостаточной нагрузочной способности, необходимо постоянно следить за их нагрузкой. Для обеспечения надлежащей производительности компьютеров и емкости запоминающих устройств, следует оценить будущие потребности в их нагрузочной способности на основе прогноза. Этот прогноз должен учитывать требования к новым системам, а также текущие и прогнозируемые тенденции использования компьютеров и сетей.

Администраторы компьютеров и сетей должны использовать эту информацию для выявления возможных узких мест, которые могут представлять угрозу системе безопасности или пользовательским сервисам, и планирования надлежащих мер по исправлению ситуации.

Приемка систем. Необходимо задать критерии приемки новых систем и провести соответствующие испытания до их приемки. Администраторы компьютеров должны четко определить, согласовать, задокументировать и проверить требования и критерии приемки новых компьютерных систем. Предлагается рассмотреть следующие пункты:

а) требования к производительности и нагрузочной способности компьютеров;

б) подготовка процедур восстановления и перезапуска систем после сбоев, а также планов действий в экстремальных ситуациях;

в) подготовка и тестирование повседневных операционных процедур в соответствии с заданными стандартами;

г) указание на то, что установка новой системы не будет иметь пагубных последствий для функционирующих систем, особенно в моменты пиковой нагрузки на процессоры (например, в конце месяца);

д) подготовка персонала к использованию новых систем.

Для обеспечения эффективной работы предлагаемой системной конфигурации следует консультироваться по вопросам поддержания ее работоспособности на всех стадиях процесса разработки новых систем. Для подтверждения полного соответствия всем критериям приемки систем необходимо провести соответствующие испытания.

Управление процессом внесения изменений в рабочие системы. Внесение изменений в информационные системы необходимо контролировать. Недостаточный контроль за внесением изменений в информационные системы является распространенной причиной их отказов и нарушения режима безопасности. Поэтому следует

определить формальные управленческие процедуры и обязанности для обеспечения удовлетворительного контроля за внесением всех изменений в оборудование, программы и процедуры. В частности, необходимо рассмотреть следующие пункты:

а) выявление и регистрация существенных изменений;

б) оценка возможных последствий от таких изменений;

в) процедура утверждения предлагаемых изменений;

г) доведение деталей предлагаемый изменений до сведения всех лиц, которых они могут затронуть;

д) процедуры и обязанности по ликвидации неудачных изменений и восстановлению систем после их внесения.

5.8.3. Защита от вредоносного программного обеспечения

Цель: Обеспечить целостность данных и программ

Для предотвращения и выявления случаев внедрения вредоносного программного обеспечения требуется принятие надлежащих мер предосторожности.

В настоящее время существует целый ряд вредоносных методов, которые позволяют использовать уязвимость компьютерных программ по отношению к их несанкционированной модификации, с такими именами, как компьютерные вирусы, сетевые черви, троянские кони и логические бомбы. Администраторы информационных систем должны быть всегда готовы к опасности проникновения вредоносного программного обеспечения в системы и по необходимости принимать специальные меры по предотвращению или обнаружению его внедрения. В частности, крайне важно принять меры предосторожности для предотвращения и обнаружения компьютерных вирусов на персональных компьютерах.

Средства защиты от вирусов. Необходимо реализовать меры по обнаружению и предотвращению проникновения вирусов в системы и процедуры информирования пользователей об их вреде. Пользователям следует напомнить, что предотвращение вирусов лучше, чем ликвидация последствий от их проникновения. В основе защиты от вирусов должны лежать хорошие знания и понимание правил

безопасности, надлежащие средства управления доступом к системам и следующие конкретные рекомендации:

1. Организация должна определить формальную политику, требующую соблюдение условий лицензий на использование программного обеспечения и запрещающую использование несанкционированных программ.

2. Противовирусные программные средства, разработанные поставщиком с хорошей репутацией, следует использовать следующим образом:

- программные средства обнаружения конкретных вирусов (которые должны регулярно обновляться и использоваться в соответствии с инструкциями поставщика) следует применять для проверки компьютеров и носителей информации на наличие известных вирусов либо как меру предосторожности, либо как повседневную процедуру;
- программные средства обнаружения изменений, внесенных в данные, должны быть по необходимости инсталлированы на компьютерах для выявления изменений в выполняемых программах;
- программные средства нейтрализации вирусов следует использовать с осторожностью и только в тех случаях, когда характеристики вирусов полностью изучены, а последствия от их нейтрализации предсказуемы.

3. Необходимо проводить регулярную проверку программ и данных в системах, поддерживающих критически важные производственные процессы. Наличие случайных файлов и несанкционированных исправлений должно быть расследовано с помощью формальных процедур.

4. Дискеты неизвестного происхождения следует проверять на наличие вирусов до их использования.

5. Необходимо определить управленческие процедуры и обязанности по уведомлению о случаях поражения систем компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения. Следует составить надлежащие планы обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных, программ и их восстановления.

Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

5.8.4. Обслуживание систем

Цель: Обеспечить целостность и доступность информационных сервисов.

Меры по обслуживанию систем требуются для поддержания целостности и доступности сервисов.

Необходимо определить повседневные процедуры для снятия резервных копий с данных, регистрации событий и сбоев, а также для слежения за средой, в которой функционирует оборудование.

Резервное копирование данных. Резервные копии с критически важных производственных данных и программ должны сниматься регулярно. Для обеспечения возможности восстановления всех критически важных производственных данных и программ после выхода из строя компьютера или отказа носителя информации, необходимо иметь надлежащие средства резервного копирования. Процедуры резервного копирования для отдельных систем должны удовлетворять требованиям планов обеспечения бесперебойной работы организации.

Стандартом предлагаются следующие рекомендации:

1. Минимальную дублирующую информацию вместе с точными и полными записями о резервных копиях следует хранить в удаленном месте на достаточном расстоянии для того, чтобы избежать последствий от аварии на основном рабочем месте. Необходимо создать по крайней мере три поколения резервных копий данных для важных производственных приложений.

2. Резервные копии должны быть надлежащим образом защищены физически от воздействия окружающей среды в соответствии со стандартами, принятыми на основном рабочем месте. Средства защиты носителей информации, принятые на основном рабочем месте, следует распространить на место хранения резервных копий.

3. Резервные данные необходимо регулярно тестировать, чтобы быть уверенным, что на них можно будет положиться в случае аварии.

Владельцы данных должны задать период сохранности критически важных производственных данных, а также требования к постоянному хранению архивных копий.

Журналы регистрации событий. Операторы компьютеров должны вести журнал регистрации всех выполняемых заданий. Этот журнал должен по необходимости включать:

- время запуска и останова систем;
- подтверждение корректного оперирования с файлами данных и выходной информацией от компьютеров.

Журналы регистрации событий должны регулярно сверяться с операционными процедурами.

Регистрация сбоев. Необходимо извещать о сбоях в работе систем и предпринимать соответствующие корректирующие меры. Зафиксированные пользователями сбои, касающиеся проблем с компьютерными и коммуникационными системами, следует заносить в журнал регистрации. Должны существовать четкие правила обработки зарегистрированных сбоев, включая следующие:

а) анализ журнала регистрации сбоев для обеспечения их удовлетворительного разрешения;

б) анализ корректирующих мер, цель которого состоит в проверке того, не скомпрометированы ли средства управления безопасностью и является ли предпринятая мера санкционированной.

Слежение за окружающей средой. Для определения условий, которые могут неблагоприятно сказаться на работе компьютерного оборудования и для принятия корректирующих мер, необходимо постоянно следить за окружающей средой, в том числе за влажностью, температурой и качеством источников электропитания. Такие процедуры следует реализовывать в соответствии с рекомендациями поставщиков

5.8.5. Сетевое администрирование

Цель: Обеспечить защиту информации, циркулирующей в сетях, и поддерживающей инфраструктуры.

Управление безопасностью компьютерных сетей, отдельные сегменты которых могут находиться за пределами организации, требует особого внимания. Возможно также потребуется принятие специальных

мер для защиты конфиденциальных данных, передаваемых по общедоступным сетям.

Средства управления безопасностью сетей. Компьютерные сети требуют целый ряд средств управления безопасностью. Сетевые администраторы должны определить надлежащие средства контроля для обеспечения защиты данных, циркулирующих в сетях, и подключенных к ним систем, от несанкционированного доступа. В частности, необходимо рассмотреть следующие пункты:

1. Обязанности по обеспечению работы сетей и компьютеров должны быть по необходимости разделены (см. Разделение обязанностей).

2. Необходимо определить обязанности и процедуры по управлению удаленным оборудованием, в том числе оборудованием на рабочих местах пользователей;

3. Для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, и для защиты подключенных к ним систем, требуется определение специальных средств контроля, используемых при шифровании и аутентификации сообщений.

4. Необходимо координировать работы по администрированию компьютеров и сетей как для оптимизации сервиса для производственных нужд, так и для обеспечения согласованной реализации защитных мер для всех информационных сервисов.

5.8.6. Оперирование с носителями информации и их защита

Цель: Предотвратить повреждение информационных ресурсов и перебои в работе организации.

Необходимо контролировать компьютерные носители данных и обеспечить их физическую защиту.

Следует определить надлежащие операционные процедуры для защиты компьютерных носителей информации (магнитные ленты, диски, кассеты), входных/выходных данных и системной документации от повреждения, похищения и несанкционированного доступа.

Управление съемными компьютерными носителями информации. Для управления такими съемными носителями информации, как магнитные ленты, диски, кассеты и распечатки,

необходимо иметь соответствующие процедуры. Предлагаются следующие средства контроля в рабочей среде:

1. Применение системы хранения данных, в которой запрещается использовать описательные метки, т.е. по меткам нельзя определить, какие данные хранятся на запоминающем устройстве.

2. Стирание предыдущего содержимого повторно используемых носителей информации, которые подлежат удалению из организации, если они больше не нужны.

3. Получение письменной санкции на удаление всех носителей информации из организации и регистрация всех случаев их удаления в контрольном журнале (см. Защита носителей информации во время транспортировки).

4. Хранение всех носителей информации в надежной, защищенной среде в соответствии с инструкциями производителей.

Все процедуры и уровни полномочий должны быть четко задокументированы.

Процедуры оперирования с данными. Чтобы защитить конфиденциальные данные от несанкционированного раскрытия или использования, необходимо определить процедуры оперирования с такими данными. Должны быть подготовлены процедуры для безопасного оперирования со всеми носителями входных и выходных конфиденциальных данных, например, документов, телексов, магнитных лент, дисков, отчетов, незаполненных чеков, счетов и др. Предлагается рассмотреть следующие пункты:

а) оперирование с носителями входной и выходной информации и их маркировка;

б) формальная регистрация получателей данных, имеющих соответствующие полномочия;

в) обеспечение полноты входных данных;

г) подтверждение получения переданных данных (по необходимости);

д) предоставление доступа к данных минимальному числу лиц;

е) четкая маркировка всех копий данных для получателя, имеющего соответствующие полномочия;

ж) проверка списков получателей с правом доступа к данным через регулярные промежутки времени.

Защита системной документации. Системная документация может содержать конфиденциальную информацию, например, описание прикладных процессов, процедур, структуры данных и процессов подтверждения полномочий. Для защиты системной документации от несанкционированного доступа, необходимо применять следующие средства контроля:

1. Системная документация должна храниться в надежных шкафах под замком.

2. Список лиц с правом доступа к системной документации должен быть максимально ограничен, а разрешение на ее использование должно выдаваться владельцем приложения.

3. Документацию, создаваемую компьютерами, следует хранить отдельно от других файлов приложений, и ей следует присвоить надлежащий уровень защиты доступа.

Удаление носителей данных. Для удаления компьютерных носителей информации, которые больше не нужны, требуются надежные и проверенные процедуры. Конфиденциальная информация может просочиться за пределы организации и попасть в руки лиц, не имеющих соответствующих прав, вследствие небрежного удаления компьютерных носителей данных. Для сведения такого риска к минимуму следует определить четкие процедуры надежного удаления носителей информации. Предлагаются следующие рекомендации:

1. Носители данных, содержащих конфиденциальную информацию, необходимо надежно удалять, например, посредством их сжигания или измельчения (дробления), или освобождены от данных для использования другими приложениями внутри организации.

2. Для идентификации носителей данных, которые могут потребовать надежного удаления, предлагается использовать следующий контрольный список:

- входная документация, например, телексы;
- копировальная бумага;
- выходные отчеты;
- одноразовые ленты для принтеров;
- магнитные ленты;
- съемные диски или кассеты;
- распечатки программ;

- тестовые данные;
- системная документация.

5.8.7. Обмен данными и программами

Цель: Предотвратить потери, модификацию и несанкционированное использование данных.

Обмены данными и программами между организациями необходимо контролировать. Такие обмены следует осуществлять на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо учитывать последствия для производственной деятельности и системы безопасности от использования электронного обмена данными и сообщениями электронной почты, а также требования к средствам управления безопасностью.

Соглашения об обмене данными и программами. Между организациями должны быть заключены формальные соглашения об обмене данными и программами (электронном или посредством курьеров), в том числе соглашения о хранении программного обеспечения (по необходимости). Та часть соглашения, которая касается безопасности, должна отражать степень важности производственной информации, участвующей в процессе обмена. В соглашениях должны быть заданы надлежащие условия безопасности, включая следующее:

а) управленческие обязанности по контролю и уведомлению о передаче и получении данных;

б) процедуры уведомления о передаче и получении данных;

в) минимум технических стандартов по упаковке и передаче информации;

г) стандарты по идентификации курьеров;

д) обязанности и обязательства в случае потери данных;

е) права собственности на данные и программы, а также обязанности по защите данных, соблюдении авторских прав на программное обеспечение и т.п.;

ж) технические стандарты на запись и чтение данных и программ;

з) специальные меры, требуемые для защиты особо важных данных, таких, как криптографические ключи.

Защита носителей информации во время транспортировки. Компьютерные носители данных могут быть уязвимы по отношению к несанкционированному доступу, использованию и повреждению во время транспортировки. Для защиты компьютерных носителей информации, транспортируемых из одной организации в другую, предлагаются следующие средства контроля:

1. Использование надежных курьеров и транспорта. Согласование списка курьеров, наделенных соответствующими полномочиями, с руководством и реализация процедуры идентификации курьеров.

2. Обеспечение надлежащей защиты содержимого упаковки от возможного физического повреждения во время транспортировки в соответствии с инструкциями производителей.

3. Принятие специальных мер (по необходимости) для защиты конфиденциальной информации от несанкционированного раскрытия или модификации.

Примеры:

а) использование контейнеров закрытого типа;

б) доставка посредством курьеров;

в) упаковка, защищенная от постороннего вмешательства (которая позволяет выявить попытки ее вскрытия);

г) в исключительных случаях разделение груза на несколько частей и их посылка разными маршрутами.

Защита электронного обмена данными. Для защиты электронного обмена данными (ЭОД) следует применять (по необходимости) специальные средства управления безопасностью, поскольку ЭОД с торговыми партнерами уязвим по отношению к несанкционированному перехвату и модификации. Кроме того возможно потребуется подтверждение передачи или получения данных. Необходимо также позаботиться о защите подключенных к сети компьютерных систем от угроз, которые исходят от электронного подключения. Средства управления безопасностью операций по ЭОД должны быть согласованы с торговыми партнерами и поставщиками дополнительных сетевых услуг. Для обеспечения совместимости с промышленными стандартами, необходимо проконсультироваться со специалистами соответствующей ассоциацией по ЭОД.

Защита электронной почты. Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля. Электронная почта все чаще используется для передачи информации между организациями, вытесняя традиционные виды связи, такие, как телексы и письма. Электронная почта отличается от традиционных видов связи, например, скоростью, структурой сообщений, степенью формальности и уязвимостью по отношению к перехвату. Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с применением электронной почты, необходимо использовать надлежащие средства контроля. Предлагается рассмотреть следующие пункты:

а) уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;

б) уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная адресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;

в) влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;

г) правовые соображения, такие, как необходимость проверки источника сообщений и др.;

д) последствия для системы безопасности от раскрытия содержания каталогов;

е) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

Организации должны задать четкие правила, касающиеся статуса и использования электронной почты.

Защита систем электронного офиса. Для контроля риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием систем электронного

офиса, требуются четкие правила и рекомендации. Системы электронного офиса предоставляют возможность более быстрого распространения и коллективного использования производственной информации. Следует принять во внимание последствия для производственной деятельности и режима безопасности от использования таких систем. Предлагается рассмотреть следующие пункты:

а) необходимость исключения некоторых категорий конфиденциальной производственной информации, например, секретной информации, в случае, если система безопасности не обеспечивает надлежащий уровень защиты;

б) необходимость определения четких правил и средств контроля для администрирования коллективно используемой информации, например, использование корпоративных электронных досок объявлений;

в) необходимость ограничения доступа к персональной информации, относящейся к избранным лицам, например, к персоналу, работающему над конфиденциальными проектами;

г) пригодность (или непригодность) системы для поддержания производственных приложений;

д) категории персонала и подрядчиков или торговых партнеров, которым разрешено использовать систему и места, из которых можно получить доступ к ней;

е) необходимость ограничения доступа к избранным системам конкретным категориям пользователей;

ж) необходимость указания статуса пользователей, например, сотрудников организации или подрядчиков, в каталогах к сведению других пользователей;

з) правила, касающиеся периода сохранности и резервного копирования информации, хранимой в системе (см. Защита документации организации и Резервное копирование данных);

и) требования и процедуры перехода на аварийный режим.

5.9. Раздел 7. Управление доступом к системам

5.9.1. Производственные требования к управлению доступом к системам

Цель: Обеспечить контроль доступа к производственной информации. Доступ к компьютерным системам и данным необходимо контролировать, исходя из производственных требований.

Такой контроль должен учитывать правила распространения информации и разграничения доступа, принятые в организации.

Документированная политика управления доступом к информации. Производственные требования к управлению доступом к системам необходимо определить и задокументировать. Для обеспечения надлежащего уровня контроля доступа к информационным сервисам и данным и его поддержания, следует четко сформулировать производственные требования к управлению доступом к системам для поставщиков услуг.

Каждый владелец производственного приложения должен четко сформулировать политику контроля доступа к данным, которая определяет права доступа каждого пользователя или группы пользователей. Эта политика должна учитывать следующее:

а) требования к безопасности отдельных производственных приложений;

б) правила распространения информации и разграничения доступа.

Необходимо также принять во внимание соответствующее законодательство и договорные обязательства, касающиеся защиты доступа к данным и сервисам.

Следует рассмотреть возможность создания стандартных профилей полномочий доступа пользователей для общих категорий работ.

5.9.2. Управление доступом пользователей

Цель: Предотвратить несанкционированный доступ к компьютерным системам.

Для управления процессом предоставления прав доступа к информационным системам требуются формальные процедуры.

Эти процедуры должны включать в себя все стадии жизненного цикла управления доступом пользователей — от начальной регистрации новых пользователей до удаления учетных записей пользователей, которые больше не нуждаются в доступе к информационным сервисам. Особое внимание следует уделить необходимости управления процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.

Регистрация пользователей. Для управления доступом ко всем многопользовательским информационным системам должна существовать формальная процедура регистрации и удаления учетных записей пользователей.

Доступ к многопользовательским информационным системам необходимо контролировать посредством формального процесса регистрации пользователей, который должен, например:

а) проверять, предоставлено ли пользователю разрешение на использование сервиса владельцем системы;

б) проверять, достаточен ли уровень доступа к системе, предоставленного пользователю, для выполнения возложенных на него функций и не противоречит ли он политике безопасности, принятой в организации, например, не компрометирует ли он принцип разделения обязанностей;

в) предоставлять пользователям их права доступа в письменном виде;

г) потребовать от пользователей подписания обязательства, чтобы показать, что они понимают условия доступа;

д) потребовать от поставщиков услуг, чтобы они не предоставляли доступ к системам до тех пор, пока не будут закончены процедуры определения полномочий;

е) вести формальный учет всех зарегистрированных лиц, использующих систему;

ж) немедленно изымать права доступа у тех пользователей, которые сменили работу или покинули организацию;

з) периодически проверять и удалять пользовательские идентификаторы и учетные записи, которые больше не требуются;

и) проверять, не выданы ли пользовательские идентификаторы, которые больше не нужны, другим пользователям.

Управление привилегиями. Предоставление и использование излишних системных привилегий зачастую оказывается одним из основных факторов, способствующих нарушению режима безопасности систем (уязвимость).

Для многопользовательских систем, требующих защиты от несанкционированного доступа, предоставление привилегий необходимо контролировать посредством формального процесса определения полномочий следующим образом:

1. Идентифицировать привилегии, связанные с каждым программным продуктом, поддерживаемым системой, например, с операционной системой или СУБД, а также категории сотрудников, которым их необходимо предоставить.

2. Предоставить привилегии отдельным лицам только в случае крайней необходимости и в зависимости от ситуации, т.е. только когда они нужны для выполнения ими своих функций.

3. Реализовать процесс определения полномочий и вести учет всех предоставленных привилегий. Не следует предоставлять привилегии до окончания процесса определения полномочий.

4. Содействовать разработке и использованию системных программ, чтобы избежать необходимость предоставления привилегий пользователям.

5. Пользователи, которым предоставлены большие привилегии для специальных целей, должны использовать другой пользовательский идентификатор для обычной работы.

Управление пользовательскими паролями. В настоящее время пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Назначение паролей необходимо контролировать посредством формального процесса управления, требования к которому должны быть следующими:

1. Потребовать от пользователей подписания обязательства по хранению персональных паролей и паролей рабочих групп в секрете.

2. В тех случаях, когда пользователи должны сами выбирать свои пароли, выдать им надежные временные пароли, которые они обязаны немедленно сменить. Временные пароли также выдаются в случае,

когда пользователи забывают свои пароли. Временные пароли должны выдаваться только после положительной идентификации пользователя.

3. Передавать временные пароли пользователям надежным способом. Следует избегать передачу паролей через посредников или посредством незащищенных (незашифрованных) сообщений электронной почты. Пользователи должны подтвердить получение паролей.

Пересмотр прав доступа пользователей. Для обеспечения эффективного контроля за доступом к данным и информационным системам руководство должно реализовывать формальный процесс пересмотра прав доступа пользователей через регулярные промежутки времени. Такой процесс должен обеспечивать следующее:

а) пересмотр полномочий доступа пользователей через регулярные промежутки времени; рекомендуется период в 6 месяцев;

б) пересмотр разрешения на предоставление специальных привилегированных прав доступа через более короткие промежутки времени; рекомендуется период в 3 месяца;

в) проверка предоставленных привилегий через регулярные промежутки времени, чтобы не допустить получения пользователями несанкционированных привилегий.

5.9.3. Обязанности пользователей

Цель: Предотвратить несанкционированный доступ пользователей.

Крайне важным условием поддержания надлежащего режима безопасности является участие и помощь зарегистрированных пользователей.

Пользователи должны знать свои обязанности по обеспечению эффективного контроля доступа, особенно что касается использования паролей и защиты пользовательского оборудования.

Использование паролей. Пользователи должны следовать установленным процедурам поддержания режима безопасности при выборе и использовании паролей.

Пароли являются основным средством подтверждения полномочий доступа пользователей к компьютерным системам. Предлагаются следующие рекомендации по выбору и использованию паролей:

1. Назначать индивидуальные пароли для обеспечения подотчетности.

2. Хранить пароли в секрете.

3. Не записывать пароли на бумаге, если не представляется возможным ее хранение в защищенном месте.

4. Изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей.

5. Выбирать пароли, содержащие не менее шести символов.

6. При выборе паролей не следует использовать:

- месяцы года, дни недели и т.п.;
- фамилии, инициалы и регистрационные номера автомобилей;
- названия и идентификаторы организаций;
- номера телефонов или группы символов, состоящие из одних цифр;
- пользовательские идентификаторы и имена, а также идентификаторы групп и другие системные идентификаторы;
- более двух одинаковых символов, следующих друг за другом;
- группы символов, состоящие из одних букв.

7. Изменять пароли через регулярные промежутки времени (приблизительно через 30 суток) и избегать повторное или циклическое использование старых паролей.

8. Чаще изменять пароли для привилегированных системных ресурсов, например, пароли доступа к определенным системным утилитам.

9. Изменять временные пароли при первом входе в системы.

10. Не включать пароли в сценарии автоматического входа в системы, например в макросы или функциональные клавиши.

Если пользователям необходим доступ ко многим сервисам и платформам и от них требуется поддержание нескольких паролей, то им следует рекомендовать использовать один единственный надежный пароль для входа во все системы, которые обеспечивают минимальный уровень защиты для хранения паролей.

Пользовательское оборудование, оставленное без присмотра. Пользователи должны обеспечить надлежащую защиту оборудования, оставленного без присмотра. Оборудование, установленное на рабочих

местах пользователей, например, рабочие станции и файловые серверы, может потребовать специальной защиты от несанкционированного доступа в тех случаях, когда оно оставляется без присмотра на продолжительное время. Все пользователи и подрядчики должны знать требования к безопасности и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты. Предлагаются следующие рекомендации:

1. Завершить активные сеансы связи по окончанию работы, если их нельзя защитить посредством соответствующей блокировки.

2. Выйти из мэйнфреймов по окончании сеанса связи. Не ограничиваться только выключением ПК или терминала.

3. Защитить ПК или терминалы, которые не используются, с помощью блокировки с ключом или эквивалентного средства контроля, например, доступом по паролю.

5.9.4. Управление доступом к сети

Цель: Обеспечить защиту систем, объединенных в сеть. Подключения к системам, объединенным в сеть, следует контролировать.

Это необходимо для того, чтобы подключенные пользователи и компьютерные системы не нарушали защиту других сетевых сервисов. Средства контроля должны включать в себя следующее:

а) соответствующие интерфейсы между сетевыми сервисами;

б)надлежащие механизмы аутентификации удаленных пользователей и оборудования;

в) контроль доступа пользователей к информационным системам.

Предоставление ограниченных услуг. Доступ к сети и компьютерным системам, осуществляемый пользователем с конкретного терминала, должен предоставляться в соответствии с политикой управления доступом, принятой в организации. В частности, пользователям следует предоставить только прямой доступ к сервисам, использование которых им разрешено.

Данное средство контроля является особенно важным для сетевых подключений к конфиденциальным или критически важным

производственным приложениям, а также для пользователей в зонах повышенного риска, например, в общедоступных местах или местах, находящихся вне пределов досягаемости администраторов безопасности организации.

Принудительная маршрутизация. В ряде случаев путь от пользовательского терминала к компьютерной системе необходимо контролировать. Современные сети предоставляют максимальные возможности для коллективного использования ресурсов и гибкость маршрутизации. Эти особенности также дают возможность несанкционированного доступа к производственным приложениям или незаконного использования информационных систем. Такой риск можно уменьшить, привлекая средства контроля для ограничения маршрута между пользовательским терминалом и компьютерными системами, доступ к которым пользователю разрешен, т.е. создавая принудительный маршрут.

Цель такой принудительной маршрутизации — предотвратить нежелательное отклонение пользователей от маршрута между пользовательским терминалом и системами, доступ к которым пользователю разрешен. Для этого обычно требуется реализация ряда средств контроля в нескольких точках пути. Принцип состоит в том, чтобы ограничить возможности выбора маршрута в каждой точке сети посредством предопределенных вариантов.

Примерами такого ограничения пути являются:

а) предоставление выделенных линий связи или телефонных номеров;

б) автоматическое подключение портов к определенным прикладным системам или шлюзам безопасности;

в) ограничение возможностей выбора маршрута с помощью системы меню и подменю для отдельных пользователей;

г) предотвращение неограниченного блуждания по сети.

В основе требований к принудительной маршрутизации должна лежать политика управления доступом, принятая в организации.

Аутентификация пользователей. Несанкционированный доступ к производственным приложениям может быть осуществлен посредством внешнего подключения к компьютерам организации через общедоступные сети или сети, не принадлежащие организации. Поэтому необходима аутентификация подключений, осуществляемых

удаленными пользователями через общедоступные (или не принадлежащие организации) сети.

Аутентификация может выполняться на уровне компьютера, поддерживающего приложение, или на сетевом уровне. Для определения необходимого уровня аутентификации, возможно, потребуется оценка рисков и непосредственного ущерба от реализации угроз для организации.

Как на сетевом уровне, так и на уровне компьютера аутентификацию удаленных пользователей можно осуществлять с помощью, например, систем оперативного реагирования на проблемы и шифрования линии связи. Использование выделенных частных линий связи или средства проверки сетевых адресов пользователей также дает уверенность в источнике подключений.

Аутентификация узлов сети. Несанкционированный доступ к производственному приложению может быть осуществлен посредством автоматического подключения удаленного компьютера, поэтому необходимо аутентифицировать подключения удаленных компьютерных систем. Это особенно важно, если подключение осуществляется через открытую сеть, находящуюся вне пределов досягаемости администраторов безопасности организации.

Аутентификацию можно выполнять на уровне компьютера, поддерживающего приложение, или на сетевом уровне. Для определения требований к аутентификации удаленных систем, возможно, потребуется оценка рисков и непосредственного ущерба от реализации угроз для организации. На сетевом уровне аутентификация удаленной системы может быть осуществлена посредством аутентификации узлов сети с помощью, например, систем оперативного реагирования на проблемы или шифрования линии связи. Использование выделенных частных линий связи или средств проверки сетевых адресов пользователей также дает уверенность в источнике подключений.

Защита удаленного диагностического порта. Доступ к диагностическим портам необходимо контролировать.

Многие компьютеры оснащены портами для диагностики удаленного, коммутируемого подключения, используемыми специалистами по техническому обслуживанию. Если такие диагностические порты не защищены, то их можно использовать для

несанкционированного доступа. Поэтому их следует защитить с помощью надлежащих механизмов безопасности, например, посредством блокировки с ключом и процедуры, которая гарантирует, что эти порты становятся доступными только после получения санкции от администратора компьютерной системы на доступ специалистов по техническому обслуживанию программно-аппаратного обеспечения.

Сегментация сетей. В ряде случаев может возникнуть необходимость в разбивке крупных сетей на отдельные сегменты.

По мере формирования деловых партнерских отношений, которые могут потребовать объединение и коллективное использование компьютеров и сетевых сервисов, вычислительные сети все больше и больше выходят за пределы традиционных границ организации. Такое расширение границ может увеличить риск несанкционированного доступа к функционирующим компьютерным системам, подключенным к сети, некоторые из них могут потребовать защиты от других пользователей сети вследствие их уязвимости или важности для организации. В таких случаях необходимо рассмотреть возможность привлечения средств контроля для разделения групп пользователей и компьютеров.

Один из методов управления безопасностью крупных сетей состоит в их разбивке на несколько логических сегментов, каждый из которых защищен межсетевым экраном в пределах заданного периметра безопасности. Тогда доступ к сегментам сети можно контролировать с помощью шлюзов безопасности, привлекая надлежащие средства контроля маршрута и подключения.

В основе критериев разбивки сетей на сегменты должна лежать политика управления доступом, принятая в организации и соответствующие требования. Кроме того, эти критерии должны учитывать относительную стоимость и последствия от внедрения подходящей технологии сетевой маршрутизации и шлюзов для производительности систем.

Следует отметить, что каждый сегмент сети может иметь свою собственную политику безопасности и администраторов безопасности.

Контроль сетевых подключений. Для удовлетворения требований политики управления доступом к определенным производственным приложениям коллективно используемые сети, особенно те из них, которые выходят за пределы границ организации,

могут потребовать реализации средств контроля для ограничения возможности подключения пользователей. Такой контроль может быть осуществлен посредством межсетевых шлюзов, которые фильтруют передаваемые по сети данные с помощью предопределенных таблиц и правил. В основе ограничений на подключение пользователей должна лежать политика управления доступом к производственным приложениям.

Примерами таких ограничений являются:

- пересылка только электронной почты;
- односторонняя передача файлов;
- двухсторонняя передача файлов;
- интерактивный доступ;
- доступ к сети только в определенное время суток или в определенную дату.

Управление сетевой маршрутизацией. Совместно используемые сети, особенно те из них, которые выходят за пределы границ организации, могут потребовать привлечения средств контроля маршрутизации для подключения компьютерных систем, чтобы информационные потоки не нарушали политику управления доступом к производственным приложениям. Это средство контроля особенно важно для сетей, доступ к которым имеют сторонние (не принадлежащие организации) пользователи.

Средства управления маршрутизацией должны быть основаны на механизмах проверки адреса источника данных и назначения. Такие средства можно реализовать на программном или аппаратном уровне. Те, кто реализует средства контроля, должны хорошо знать сильные стороны используемых механизмов.

Защита сетевых сервисов. Существует целый ряд общедоступных и коммерческих сетевых сервисов, некоторые из них предлагают дополнительные услуги. Сетевые сервисы могут иметь уникальные (возможно сложные) защитные характеристики. Организации, пользующиеся сетевыми сервисами, должны потребовать от своих поставщиков сетевых услуг четкого описания атрибутов безопасности всех используемых сервисов и определить последствия от нарушения режима безопасности для конфиденциальности, целостности и доступности производственных приложений.

5.9.5. Управление доступом к компьютерам

Цель: Предотвратить несанкционированный доступ к компьютерам.

Доступ к компьютерным системам необходимо контролировать.

Такой доступ следует предоставлять только зарегистрированным пользователям. Компьютерные системы, обслуживающие многих пользователей, должны быть способны делать следующее:

а) идентифицировать и проверять подлинность личности пользователей, а также по необходимости терминал или местонахождение каждого зарегистрированного пользователя;

б) фиксировать случаи успешного и безуспешного доступа к системам;

в) представить систему управления паролями, которая обеспечивает выбор надежных паролей;

г) по необходимости ограничить время подключения пользователей.

Существуют также более мощные и дорогостоящие системы управления доступом, такие, как системы оперативного реагирования на проблемы. Использование таких систем оправдано в случае высокого риска нарушения режима безопасности организации.

Автоматическая идентификация терминалов. Для аутентификации подключений к конкретным узлам сети следует рассмотреть возможность автоматической идентификации терминалов. Автоматическая идентификация терминалов – это средство, которое можно использовать для тех приложений, для которых важно, чтобы сеанс связи можно было инициировать только с конкретного терминала. Идентификатор, присвоенный терминалу, можно использовать для указания того, разрешено ли конкретному терминалу инициировать сеанс связи или производить определенные действия. Для обеспечения безопасности терминального идентификатора, возможно, потребуется физическая защита терминала.

Процедуры входа в систему с терминала. Доступ к информационным сервисам следует осуществлять с помощью надежной процедуры входа в системы.

Процедура входа в компьютерную систему (logon) должна сводить риск несанкционированного доступа к минимуму, поэтому она должна давать минимум информации о системе, чтобы избежать оказания излишней помощи незарегистрированному пользователю. Хорошая процедура входа в систему должна выполнять следующие функции:

а) не выводить на экран идентификаторы системы или приложения до тех пор, пока не завершится процесс входа в систему;

б) выводить на экран общее предупреждение о том, что только зарегистрированные пользователи имеют право доступа к компьютеру;

в) не предоставлять справочную информацию во время выполнения процедуры входа в систему, которая могла бы оказать помощь незарегистрированному пользователю;

г) проверять достоверность регистрационной информации только по завершении ввода всех данных. При возникновении сбойной ситуации система не должна указывать, какая часть введенных данных правильная или неправильная;

д) ограничивать разрешаемое количество неудавшихся попыток входа в систему (рекомендуется три попытки), прежде чем принять меры:

- по регистрации неудавшейся попытки;
- по принудительному введению временной задержки между дальнейшими попытками входа в систему;
- по разрыву канала связи;

е) разорвать канал связи и не давать справочную информацию после отвергнутой попытки входа в систему;

ж) задать минимальную и максимальную продолжительность процедуры входа в систему. При ее превышении система должна прервать процедуру входа;

з) выводить на экран следующую информацию по завершении успешного входа в систему:

- дату и время предыдущей успешной попытки входа в систему;
- подробности о неудавшихся попытках входа в систему, предпринятых с момента последнего успешного входа в нее.

Идентификаторы пользователей. Для отслеживания действий отдельных лиц всем пользователям необходимо присвоить уникальные персональные идентификаторы. Пользовательские идентификаторы не

должны указывать на уровень привилегий пользователя, например, администратор, наблюдатель и т.п.

В исключительных ситуациях, в случае явных преимуществ для организации, можно использовать общий пользовательский идентификатор для группы пользователей или конкретного задания. Такие случаи должны быть утверждены руководством и задокументированы. Для обеспечения подотчетности могут потребоваться дополнительные средства контроля.

Система управления паролями. Для аутентификации пользователей необходимо использовать эффективную систему управления паролями. Пароли являются основным средством подтверждения полномочий доступа пользователя к компьютерной системе. Системы управления паролями должны предоставлять эффективное, интерактивное средство обеспечения надежных паролей .

Некоторые приложения требуют назначения пользовательских паролей независимым лицом, наделенным соответствующими полномочиями. В большинстве случаев пароли выбираются и поддерживаются самими пользователями.

Хорошая система управления паролями должна:

а) по необходимости принуждать пользователей к применению индивидуальных паролей для обеспечения подотчетности;

б) по необходимости позволять пользователям выбирать и изменять свои собственные пароли, а также включать процедуру их подтверждения, чтобы избежать ошибок при их наборе;

в)задать минимальное количество символов в паролях;

г)принуждать пользователей к изменению паролей через регулярные промежутки времени в тех случаях, когда они сами поддерживают свои пароли. Рекомендуется интервал в несколько дней по умолчанию.

д) по необходимости принуждать привилегированных пользователей, например тех, кто имеет доступ к системным утилитам, к более частому изменению паролей;

е) заставлять пользователей изменять временные пароли при первом входе в систему в тех случаях, когда они сами выбирают свои пароли;

ж) вести учет предыдущих пользовательских паролей, например, за последние 12 месяцев и предотвращать их повторное использование пользователями;

з) не выводить пароли на экран при их наборе на клавиатуре;

и) хранить файлы паролей отдельно от основных данных прикладной системы;

и) хранить пароли в зашифрованном виде, использовать односторонний алгоритм шифрования;

к) изменять пароли, заданные поставщиком программного обеспечения по умолчанию, после его инсталляции;

л) в идеале проверять, выбрал ли пользователь надежный пароль, например, посредством проверки, не основан ли пароль на следующих данных:

- месяцы года, дни недели и т.п.;
- названия и идентификаторы организаций;
- пользовательские идентификаторы, имена пользователей, идентификаторы групп и другие системные идентификаторы;
- более чем два одинаковых символа, следующие друг за другом;
- группы символов, состоящие из одних цифр или одних букв.

Ограничение времени подключения. Дополнительную защиту приложений повышенного риска можно обеспечить посредством ограничения времени подключения. Ограничение разрешаемого периода подключения терминала к компьютерным системам позволяет уменьшить вероятность несанкционированного доступа. Применение такого средства контроля следует рассмотреть для компьютерных систем, поддерживающих конфиденциальные приложения, особенно для систем с терминалами, установленными в зонах повышенного риска, например, в общедоступных местах или местах, находящихся вне пределов досягаемости администраторов безопасности организации. Примерами таких ограничений являются:

а) использование предопределенных интервалов времени разрешенного доступа, например, для пакетной передачи файлов, или регулярных интерактивных сеансов связи небольшой продолжительности;

б) ограничение времени подключения обычными часами работы организации, если не требуется работа в сверхурочное время.

5.9.6. Управление доступом к приложениям

Цель: Предотвратить несанкционированный доступ к информации, хранимой в компьютерных системах.

Для управления доступом к прикладным системам и данным необходимо использовать логические средства контроля доступа.

Логический доступ к компьютерным программам и данным следует предоставлять только зарегистрированным пользователям. Прикладные системы должны:

а) контролировать доступ пользователей к данным и приложениям в соответствии с политикой управления доступом, принятой в организации;

б) обеспечивать защиту программ-утилит, которые способны обойти средства контроля систем и приложений от несанкционированного доступа;

в) не нарушать защиту других систем, с которыми они разделяют информационные ресурсы.

Ограничение доступа к информации. Пользователям прикладных систем, в том числе обслуживающему персоналу, следует предоставлять доступ к данным и приложениям в соответствии с политикой управления доступом к информации (см. Документированная политика управления доступом к информации), принятой в организации, исходя из индивидуальных потребностей в производственных приложениях. Чтобы удовлетворить требования политики управления доступом, необходимо рассмотреть следующие средства контроля:

а) предоставление системы меню для контроля доступа к приложениям;

б) ограничение знания пользователями данных и функций прикладных систем, доступ к которым им не разрешен, посредством соответствующего редактирования пользовательской документации;

в) контроль полномочий доступа пользователей, например прав на чтение, запись, удаление, выполнение;

г) гарантирование того, что выходные данные от прикладных систем, поддерживающих конфиденциальную информацию, содержат только необходимые данные и посылаются только на терминалы и

компьютеры, доступ к которым разрешен, включая периодический анализ таких выходных данных для обеспечения удаления ненужной информации.

Использование системных утилит. Большинство компьютерных систем поддерживают одну или несколько системных программ-утилит, которые способны обойти средства контроля системы и приложений. Необходимо ограничить и тщательно контролировать использование таких системных утилит. Предлагается использовать следующие средства контроля (по возможности):

а) защита системных утилит с помощью паролей;

б) изоляция системных утилит от прикладного программного обеспечения;

в) предоставление доступа к системным утилитам минимальному числу надежных, зарегистрированных пользователей;

г) предоставление разрешения на специальное использование системных утилит;

д) ограничение доступности системных утилит, например временем внесения санкционированного изменения;

е) регистрация всех случаев использования системных утилит;

ж) определение и документирование уровней полномочий доступа к системным утилитам;

з) удаление всех ненужных утилит и системных программ.

Управление доступом к библиотекам исходных текстов программ. Для сведения риска повреждения компьютерных программ к минимуму необходимо осуществлять жесткий контроль за доступом к библиотекам исходных текстов программ:

1. Не следует хранить библиотеки исходных текстов программ в рабочих системах (по возможности).

2. Необходимо назначить библиотекаря программ для каждого приложения.

3. Обслуживающий персонал не должен иметь неограниченный доступ к библиотекам исходных текстов программ.

4. Не следует хранить разрабатываемые или сопровождаемые программы в рабочих библиотеках исходных текстов программ.

5. Обновление библиотек исходных текстов программ и выдача текстов программ программистам должны производиться только

назначенным библиотекарем после получения санкции на доступ к приложению от руководителя обслуживающего персонала.

6. Распечатки программ следует хранить в защищенном месте;

7. Необходимо фиксировать все случаи доступа к библиотекам исходных текстов программ в контрольном журнале.

8. Устаревшие версии исходных текстов программ следует архивировать с четким указанием точной даты и времени их использования вместе со всем вспомогательным программным обеспечением и информацией об управлении выполнением заданий, определением данных и процедур.

9. Сопровождение и копирование библиотек исходных текстов программ необходимо осуществлять в соответствии со строгими процедурами управления процессом внесения изменений.

5.9.7. Слежение за доступом к системам и их использованием

Цель: Выявить несанкционированные действия.

Для обеспечения соответствия политике управления доступом и стандартам необходимо следить за системами.

Это необходимо для того, чтобы определить эффективность принятых мер и обеспечить соответствие модели политики управления доступом.

Регистрация событий. Все чрезвычайные ситуации и события, связанные с нарушением режима безопасности, необходимо регистрировать в контрольном журнале. Записи в таком журнале следует хранить в течение заданного промежутка времени для оказания помощи в будущих расследованиях и осуществлении контроля за доступом. Кроме отвергнутых попыток входа в системы, целесообразно также регистрировать случаи успешного доступа к ним. Контрольный журнал должен включать следующие данные:

- идентификаторы пользователей;
- дата и время входа и выхода из системы;
- идентификатор или местонахождение терминала (по возможности).

Слежение за использованием систем. Необходимо установить процедуры слежения за использованием систем.

Такие процедуры требуются для обеспечения выполнения пользователями только явно разрешенных процессов. Уровень контроля, требуемый для отдельных систем, следует определить с помощью независимой оценки рисков. Необходимо рассмотреть следующие пункты:

- неудачные попытки доступа к системам;
- анализ сеанса входа в систему на предмет выявления несанкционированного использования или восстановленных пользовательских идентификаторов;
- выделение и использование ресурсов с привилегированным доступом;
- отслеживание отдельных действий;
- использование конфиденциальных ресурсов.

Все действия, связанные со слежением за системами, должны быть формально разрешены руководством.

Синхронизация системных часов. Для обеспечения точности контрольных журналов, которые могут потребоваться для расследований или в качестве свидетельства во время судебных разбирательств и при наложении дисциплинарных взысканий, важно правильно установить системные часы компьютеров. Неточные контрольные журналы могут помешать таким расследованиям и подорвать доверие к такому свидетельству.

5.10. Раздел 8. Разработка и сопровождение информационных систем

5.10.1. Требования к безопасности систем

Цель: Обеспечить встроенность средств защиты в информационные системы.

Требования к безопасности должны быть определены и согласованы до разработки информационных систем.

Средства защиты оказываются значительно более дешевыми и эффективными, если их встроить в прикладные системы на стадиях задания требований и проектирования. Все требования к безопасности,

включая необходимость перехода на аварийный режим для продолжения обработки информации, следует определить на стадии задания требований к проекту, а также обосновать, согласовать и задокументировать их в рамках общего плана работ по созданию информационной системы.

Анализ и задание требований к безопасности. Анализ требований к безопасности следует проводить на стадии анализа требований к каждому проекту разработки систем. При формулировании производственных требований к новым системам или модернизации существующих систем, необходимо задать требования к средствам управления безопасностью. Такие требования обычно сосредоточены на автоматических средствах контроля, встраиваемых в системы, однако следует также рассмотреть необходимость использования вспомогательных ручных средств управления безопасностью. Эти соображения следует также принять во внимание при качественной оценке пакетов программ для производственных приложений.

Требования к безопасности и средства управления ею должны отражать ценность информационных ресурсов для организации, а также возможные последствия от нарушения режима безопасности или отсутствия средств защиты для производственных процессов.

Основу анализа требований к безопасности составляют:

- рассмотрение необходимости обеспечения конфиденциальности, целостности и доступности информационных ресурсов;
- определение возможностей использования различных средств контроля для предотвращения и выявления случаев нарушения защиты, а также восстановления работоспособности систем после их выхода из строя и инцидентов в системе безопасности.

В частности, при проведении такого анализа следует рассмотреть необходимость:

а) управления доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;

б) регистрации значительных событий в контрольном журнале для целей повседневного контроля или специальных расследований, в том

числе как свидетельство при проведении переговоров с подрядчиками и другими лицами ;

в) проверки и обеспечения целостности жизненно важных данных на всех или избранных стадиях их обработки;

г) защиты конфиденциальных данных от несанкционированного раскрытия, в том числе возможное использование средств шифрования данных в специальных случаях;

д) выполнения требований инструкций и действующего законодательства, а также договорных требований, в том числе составление специальных отчетов для удовлетворения определенных правовых требований;

е) снятия резервных копий с критически важных производственных данных;

ж) восстановления систем после их отказов, особенно для систем с повышенными требованиями к доступности;

з) защиты систем от внесения несанкционированных дополнений и изменений;

и) предоставления возможности безопасного управления системами и их использования сотрудникам, не являющимся специалистами (но имеющим надлежащую подготовку);

и) обеспечения соответствия систем требованиям аудиторов, например, посредством использования таких средств, как встроенные программы-утилиты для выборочного контроля и независимое программное обеспечение для повторения критически важных вычислений.

Средства управления безопасностью, встроенные в компьютерные системы, могут быть скомпрометированы, если обслуживающий их персонал и пользователи не будут их знать. Поэтому необходимо явно определить эти средства контроля в соответствующей документации.

5.10.2. Безопасность в прикладных системах

Цель: Предотвратить потерю, модификацию и несанкционированное использование пользовательских данных в прикладных системах.

При проектировании прикладных систем необходимо встроить в них надлежащие средства управления безопасностью, в том числе средства регистрации событий в контрольном журнале.

Проектирование и эксплуатация систем должны соответствовать общепринятым промышленным стандартам обеспечения надежной защиты, определенным в настоящих практических правилах.

Системы, которые поддерживают или оказывают влияние на исключительно уязвимые, ценные или критически важные информационные ресурсы организации, могут потребовать принятия дополнительных мер противодействия. Такие меры следует определить исходя из рекомендаций специалиста по безопасности с учетом идентифицированных угроз нарушения защиты и возможных последствий от их реализации для организации.

Проверка достоверности входных данных. Чтобы обеспечить правильный ввод данных в прикладные системы необходимо проверять их на достоверность. Предлагаются следующие средства контроля:

а) проверки с целью выявления следующих ошибок:

- величины, выходящие за заданные пределы;
- неправильные символы в полях данных;
- пропущенные или неполные данные;
- превышенные верхние и нижние пределы на объем вводимых данных;
- несанкционированные или противоречивые управляющие данные;

б) периодический анализ содержания ключевых полей или файлов данных для подтверждения их достоверности и целостности;

в) осмотр печатной входной документации на предмет внесения несанкционированных изменений во входные данные (необходимо получить разрешение на внесение всех изменений во входные документы);

г) процедуры реагирования на ошибки, связанные с проверкой достоверности входных данных;

д) определение обязанностей всех сотрудников, участвующих в процессе ввода данных.

Проверка достоверности внутренней обработки данных. Данные, которые были правильно введены в прикладную систему, могут

быть повреждены в результате ошибок обработки или преднамеренных действий. Чтобы выявить такие случаи повреждения данных, необходимо встроить средства проверки в системы. Требуемые для этого средства контроля определяются характером приложения и последствиями от повреждения данных для организации.

Примерами средств проверки, которые можно встроить в системы, являются:

а) контроль сеанса связи и пакетной обработки для согласования файлов данных о платежном балансе после проведения операций с ними;

б) контроль платежного баланса для сверки начального сальдо с предыдущим конечным сальдо:

- контроль за выполнением операций;
- подведение итогов по обновлению файлов;
- контроль за выполнением программ;

в) проверка достоверности данных, сгенерированных системой (см. Проверка достоверности входных данных);

г) проверка целостности данных и программ, пересылаемых между центральным и удаленными компьютерами (см. Аутентификация сообщений);

д) подведение итогов по обновлению файлов.

Шифрование данных. Для конфиденциальных данных, требующих особой защиты, необходимо рассмотреть возможность их шифрования. Шифрование – это процесс преобразования информации в зашифрованный текст для обеспечения ее конфиденциальности и целостности во время передачи или при хранении. В этом процессе используется алгоритм шифрования и информация о секретном ключе, которая известна только зарегистрированным пользователям. Уровень защищенности, обеспечиваемый процессом шифрования, зависит от качества алгоритма и секретности ключа.

Шифрование может потребоваться для защиты конфиденциальной информации, которая уязвима по отношению к несанкционированному доступу, как во время ее передачи, так и при хранении. Для определения необходимости шифрования данных и требуемого уровня защищенности необходимо провести оценку риска нарушения режима безопасности. Чтобы выбрать подходящие программные продукты с

надлежащим уровнем защищенности и разработать надежную систему управления ключами, следует обратиться за советом к специалистам.

Аутентификация сообщений. Аутентификация сообщений – это метод, используемый для выявления несанкционированных изменений, внесенных в передаваемые электронные сообщения, или их повреждения. Его можно реализовать на аппаратном или программном уровне с помощью физического устройства аутентификации сообщений или программного алгоритма.

Возможность аутентификации сообщений следует рассмотреть для тех приложений, для которых жизненно важным является обеспечение целостности сообщений, например, электронные передачи информации о денежных средствах или другие электронные обмены данными. Для определения необходимости аутентификации сообщений и выбора наиболее подходящего метода ее реализации необходимо провести оценку риска нарушения режима безопасности.

Аутентификация сообщений не предназначена для защиты содержания сообщений от перехвата. Для этих целей подходит шифрование данных, которое можно также использовать для аутентификации сообщений.

В последнее время широко используется электронная подпись — это специальный вид аутентификации сообщений, обычно основанный на методах шифрования с открытым ключом, который обеспечивает аутентификацию отправителя, а также гарантирует целостность содержимого сообщения.

5.10.3. Защита файлов прикладных систем

Цель: Обеспечить надежную реализацию проектов разработки информационных систем и их поддержку.

Доступ к системным файлам необходимо контролировать.

Поддержание целостности прикладных систем должно быть обязанностью пользователя или группы разработки, которой прикладная система или программное обеспечение принадлежит.

Контроль рабочего программного обеспечения. Следует осуществлять жесткий контроль за реализацией программного

обеспечения в рабочих системах. Чтобы свести риск повреждения рабочих систем к минимуму, необходимо реализовать следующие средства контроля:

1. Обновление рабочих библиотек программ должен осуществлять только назначенный библиотекарь после получения санкции на доступ к приложению от руководителя персонала, обслуживающего информационные системы.

2. В рабочих системах следует хранить только выполняемые программы (по возможности).

3. Выполняемые программы не следует запускать на рабочих системах до тех пор, пока они не пройдут тестирование и не будут приняты пользователями, а соответствующие библиотеки исходных текстов программ не будут обновлены.

4. Необходимо фиксировать все случаи обновления рабочих библиотек программ в контрольном журнале.

5. Предыдущие версии программ следует сохранить – мера предосторожности при чрезвычайных ситуациях.

Защита системных тестовых данных. Тестовые данные необходимо защищать и контролировать. Тестирование систем и их приемка обычно требуют значительных объемов тестовых данных, которые близки к реальным данным настолько, насколько это возможно. Необходимо избегать использования реальных баз данных, содержащих персональные данные. Прежде чем использовать такие данные, их необходимо обезличить. Для защиты реальных данных при их использовании для целей тестирования предлагаются следующие средства контроля:

1. Процедуры управления доступом, которые применяются для рабочих прикладных систем, должны также применяться для тестируемых прикладных систем.

2. Необходимо получить отдельное разрешение всякий раз, когда реальные данные копируются в тестируемую прикладную систему.

3. Реальные данные следует удалить из тестируемой прикладной системы сразу после завершения процесса тестирования.

4. Случаи копирования реальных данных необходимо регистрировать в контрольном журнале.

5.10.4. Безопасность в среде разработки и рабочей среде

Цель: Обеспечить защиту прикладного программного обеспечения и данных.

Среду разработки и рабочую среду необходимо жестко контролировать.

Администраторы, отвечающие за прикладные системы, должны также отвечать за защиту среды разработки и рабочей среды. Они должны анализировать все изменения, которые предлагается внести в системы, чтобы гарантировать, что они не нарушат безопасность системы или рабочей среды.

Процедуры управления процессом внесения изменений. Чтобы свести риск повреждения информационных систем к минимуму, следует осуществлять жесткий контроль за внесением изменений в них. Для этого требуются формальные процедуры управления процессом внесения изменений. Эти процедуры должны гарантировать, что безопасность и процедуры управления ею не будут скомпрометированы, что программистам, отвечающих за поддержку систем, предоставлен доступ только к тем компонентам системы, которые необходимы для их работы, и что получено формальное разрешение на внесение изменений. Такой процесс должен включать в себя следующее:

а) регистрацию согласованных уровней полномочий, в том числе:

- служба приема запросов на внесение изменений группой, обслуживающей информационные системы;
- полномочия пользователей на подачу запросов на внесение изменений;
- уровни полномочий пользователей на принятие подробных предложений;
- полномочия пользователей на принятие вносимых изменений;

б) принятие изменений, предлагаемых только зарегистрированными пользователями;

в) проверку средств управления безопасностью и процедур обеспечения целостности на предмет их компрометации внесенными изменениями;

г) выявление всех компьютерных программ, файлов данных, баз данных и аппаратных средств, которые требуют внесения поправок;

д) утверждение подробных предложений до начала работы;

е) обеспечение принятия предлагаемых изменений зарегистрированными пользователями до их внесения;

ж) обновление системной документации по завершении процесса внесения каждого изменения, а также архивирование или уничтожение старой документации;

з) осуществление контроля над версиями всех обновляемых программ;

и) регистрацию всех запросов на внесение изменений в контрольном журнале.

Технический анализ изменений, вносимых в операционную систему. Необходимость во внесении изменений в операционную систему возникает периодически, например, инсталляция новой версии, предоставляемой поставщиком. В таких случаях следует проводить анализ прикладных систем о возможном нарушении режима их безопасности, проистекающий от таких изменений. Этот процесс должен включать в себя следующее:

а) проверку процедур контроля приложений и обеспечения их целостности на предмет компрометации вследствие внесения изменений в операционную систему;

б) включение в ежегодный план поддержки проверки и тестирования систем, связанных с изменениями, вносимыми в операционную систему, а также выделение для этого необходимых финансовых средств;

в) обеспечение своевременного уведомления сотрудников о предлагаемых изменениях в операционной системе для проведения надлежащего анализа до их внесения.

Ограничения на внесение изменений в пакеты программ. Не рекомендуется вносить изменения в пакеты программ. По возможности следует использовать пакеты программ, предоставляемые поставщиками, без их модификации. В тех случаях, когда возникает необходимость во внесении изменений в пакеты программ, следует рассмотреть следующие пункты:

а) риск компрометации встроенных средств контроля и процессов обеспечения целостности;

б) необходимость получения согласия поставщика;

в) возможность получения требуемых изменений от поставщика в рамках стандартного обновления программ;

г) возможность взятия организацией ответственности за дальнейшее сопровождение программного обеспечения в результате внесенных изменений.

Если изменения считаются крайне необходимыми, то следует сохранить исходное программное обеспечение, а изменения внести в четко определенную копию. Эти изменения необходимо полностью задокументировать так, чтобы их можно было вносить в будущие обновленные версии программ в случае необходимости.

5.11. Раздел 9. Планирование бесперебойной работы организации

5.11.1. Вопросы планирования бесперебойной работы организации

Цель: Составить планы для предотвращения перебоев в работе организации.

Для защиты критически важных производственных процессов от последствий крупных аварий и катастроф необходимо иметь планы обеспечения бесперебойной работы организации.

Должен существовать процесс разработки и реализации надлежащих планов для быстрого восстановления критически важных производственных процессов и сервисов в случае серьезных перебоев в работе организации. Такие перебои могут быть вызваны, например, природными катастрофами, авариями, отказами оборудования, преднамеренными действиями и потерей предоставляемых услуг.

Процесс планирования бесперебойной работы организации должен включать в себя меры по идентификации и уменьшению рисков, ликвидации последствий от реализации угроз и быстрому возобновлению основных работ.

Процесс планирования бесперебойной работы организации. Для разработки и реализации планов обеспечения бесперебойной работы организации необходимо иметь соответствующий процесс.

Такой процесс должен предусматривать идентификацию и уменьшение рисков умышленных или случайных угроз, которым подвергаются жизненно важные сервисы. Необходимо разработать планы поддержания непрерывности производственной деятельности после отказа или повреждения жизненно важных сервисов или систем. Процесс планирования бесперебойной работы организации должен включать в себя следующее:

а) идентификацию критически важных производственных процессов и их ранжирование по приоритетам;

б) определение возможного воздействия аварий различных типов на производственную деятельность;

в) определение и согласование всех обязанностей и планов действий в чрезвычайных ситуациях;

г) документирование согласованных процедур и процессов;

д) надлежащую подготовку персонала к выполнению согласованных процедур и процессов в чрезвычайных ситуациях;

е) тестирование планов;

ж) пересмотр и обновление планов.

Процесс планирования должен быть в первую очередь сосредоточен на поддержании работоспособности критически важных производственных процессов и сервисов, включая требования к укомплектованию персоналом и другие требования, не связанные с обработкой информации, а не только на процедурах перехода на аварийный режим для компьютерных систем.

Система планирования бесперебойной работы организации. Чтобы обеспечить согласованность всех уровней планирования и определить приоритеты для тестирования и реализации, необходимо иметь единую систему планов. В каждом плане обеспечения бесперебойной работы организации следует четко задать условия его активации, а также указать сотрудников, отвечающих за реализацию каждого пункта плана. Новые планы не должны противоречить установленным процедурам реагирования на чрезвычайные ситуации,

например, планам эвакуации, и принятым процедурам перехода на аварийный режим для компьютерных и коммуникационных систем.

Вообще говоря, могут потребоваться разные уровни планирования, поскольку каждый уровень сосредоточен на своей задаче, а в его реализации могут участвовать разные группы по восстановлению систем после аварий. Модель системы планирования бесперебойной работы организации включает в себя следующие четыре компонента:

а) процедуры реагирования на чрезвычайные ситуации, описывающие меры, которые надлежит принять сразу после крупного инцидента, подвергающего опасности работу организации и/или жизнь персонала;

б) процедуры перехода на аварийный режим, описывающие меры, которые надлежит принять для временного перевода основных работ и сервисов в другие места;

в) процедуры возобновления работы организации, описывающие меры, которые надлежит принять для возобновления нормальной полноценной производственной деятельности организации, обычно на основном месте;

г) график испытаний, который определяет, как и когда будет проведено тестирование плана.

Каждый уровень планирования и каждый индивидуальный план должны иметь конкретных исполнителей.

Тестирование планов обеспечения бесперебойной работы организации. Многие планы обеспечения бесперебойной работы организации терпят неудачу при их тестировании вследствие неправильных исходных допущений, просчетов или изменений, внесенных в оборудование, и персонала. Поэтому эти планы необходимо регулярно тестировать, чтобы обеспечить их эффективность. Такие тесты должны гарантировать, что все члены группы по восстановлению систем после аварий и другие сотрудники, имеющие к этому отношение, будут постоянно помнить о плане.

Следует составить график проведения испытаний плана обеспечения бесперебойной работы организации. Такой график должен указывать, как и когда будет тестироваться каждый элемент плана.

Рекомендуется поэтапный подход к тестированию, основанный на проведении частых испытаний отдельных компонентов плана. Это должно обеспечить действенность и эффективность плана на протяжении года. Кроме того такой подход позволяет избежать частого проведения исчерпывающих испытаний полного плана.

Обновление планов обеспечения бесперебойной работы организации. Планы обеспечения бесперебойной работы организации быстро устаревают вследствие изменений в производственных процессах и организации, поэтому их необходимо регулярно обновлять. Регулярное обновление планов крайне важно для защиты денежных средств, вложенных в разработку исходного плана, и обеспечения его эффективности. Примерами изменений, которые могут потребовать обновления планов, являются:

- приобретение нового оборудования или модернизация функционирующих систем;
- новая технология выявления и контроля проблем, например, обнаружение пожаров;
- новая технология контроля за окружающей средой;
- кадровые или организационные изменения;
- смена подрядчиков или поставщиков;
- изменение адресов или телефонных номеров;
- изменения, внесенные в производственные процессы;
- изменения, внесенные в пакеты прикладных программ;
- изменения в рабочих процедурах;
- изменения в законодательстве.

Необходимо назначить ответственных лиц для идентификации и внесения изменений в планы. Необходимость в отдельных изменениях следует пересматривать по крайней мере ежемесячно. Это процесс должен быть подкреплен кратким ежегодным анализом полного плана.

Чтобы гарантировать, что последствия от вносимых изменений определены и доведены до сведения сотрудников до обновления плана, требуется формальный метод контроля за внесением изменений.

5.12. Раздел 10. Соответствие системы основным требованиям

5.12.1. Выполнение правовых требований

Цель: Избежать нарушения правовых обязательств и обязательств по соблюдению уголовного и гражданского права, а также обеспечить выполнение требований к информационной безопасности.

На разработку, сопровождение и использование информационных систем могут быть наложены правовые и договорные требования к безопасности.

Все правовые и договорные требования, имеющие отношение к безопасности, необходимо определить в явном виде и задокументировать для каждой информационной системы. Необходимо также определить и задокументировать конкретные средства контроля, меры противодействия и обязанности для выполнения этих требований.

При задании конкретных правовых требований следует обратиться за советом к консультантам организации, занимающимся правовыми вопросами. Следует учесть, что требования законодательства в разных странах разные.

Контроль за копированием ПО, защищенного законом об авторском праве. Следует принять во внимание ограничения, накладываемые действующим законодательством на использование материалов, защищенных законом об авторском праве.

Правовые и договорные требования могут наложить ограничения на копирование программ. В частности, от пользователей могут потребовать, чтобы они применяли только те программы, которые разработаны организацией, или лицензионное программное обеспечение.

Программные продукты обычно поставляются в соответствии с лицензионным соглашением, которое ограничивает их использование определенными машинами и может ограничить процесс копирования созданием только резервных копий. Необходимо учитывать следующее:

1. Политика организации должна запрещать копирование материала, защищенного законом об авторском праве, без согласия его владельца.

2. Пользователям должно быть рекомендовано не нарушать эту политику посредством копирования программ с одной машины на другую без письменной санкции их владельца.

3. Копирование патентованного программного обеспечения или программ организации для использования на компьютерах, которые не принадлежат организации, для целей, не связанных с основной рабочей деятельностью, может также привести к нарушению закона об авторском праве и политики организации.

4. В тех случаях, когда необходимо инсталлировать программный продукт на дополнительных машинах, следует включить соответствующий пункт в лицензионное соглашение или закупить дополнительные копии.

5. Необходимо регулярно проверять использование программного обеспечения и вести надлежащий учет.

Нарушение закона об авторском праве может привести к судебным разбирательствам и даже к возбуждению уголовного дела.

Защита документации организации. Важные для организации документы необходимо защищать от потери, уничтожения и подделки. Некоторые документы могут потребовать хранения в защищенном месте для удовлетворения правовых требований, а также для поддержки основных производственных работ.

Примерами этого являются документы, которые могут потребоваться в качестве свидетельства того, что организация работает в соответствии с правовыми нормами, или для обеспечения надлежащей защиты от возможных гражданских или уголовных исков, или для подтверждения финансового состояния организации по отношению к держателям акций, партнерам и аудиторам.

Целесообразно уничтожить документацию, которая хранится дольше предписываемого законом времени, в случае, когда это не будет иметь пагубные последствия для работы организации.

Для выполнения этих обязательств организация должна предпринять следующее:

1. Подготовить инструкции по хранению и обращению с документацией и информацией, а также их уничтожению.

2. Составить план-график, в котором определяются основные типы документов и сроки их хранения.

3. Проводить инвентаризацию всех источников основной информации.

4. Реализовать надлежащие меры по защите основной документации и информации от потери, уничтожения и подделки.

Защита персональных данных. Во многих странах персональные данные (о лицах, которых можно идентифицировать по ним), хранимые или обрабатываемые на компьютере, попадают под законодательство о защите информации.

Соблюдение законодательства о защите информации требует определенного структурирования руководства и контроля. Это, зачастую, достигается посредством назначения сотрудника, отвечающего за защиту данных, который дает рекомендации администраторам, пользователям и поставщикам услуг по распределению обязанностей и использованию конкретных процедур. В круг обязанностей владельца данных должны входить доведение предложений о хранении персональной информации на компьютере до сведения сотрудника, отвечающего за защиту данных, и обеспечение знания и понимание принципов защиты информации, определенных в действующем законодательстве.

Для примера ниже приведены сведения о законе Великобритании о защите данных от 1984 года, излагаются восемь принципов, которые применимы ко всем системам, обрабатывающим персональную информацию. Они перечислены ниже:

Первый принцип. **Необходимо предоставлять доступ к информации, содержащейся в персональных данных, и обрабатывать персональные данные на законном основании и в соответствии с принципами справедливости.**

Второй принцип. **Персональные данные следует хранить только для определенных, законных целей.**

Третий принцип. **Персональные данные, хранимые для тех или иных целей, не следует использовать или раскрывать способом, который несовместим с этими целями.**

Четвертый принцип. **Персональные данные, хранимые для тех или иных целей, должны быть адекватны этим целям и не должны быть избыточными по отношению к ним.**

Пятый принцип. **Персональные данные должны быть точными и по необходимости свежими.**

Шестой принцип. **Персональные данные, хранимые для тех или иных целей, не следует хранить дольше, чем это необходимо для этих целей.**

Седьмой принцип. **Сотрудник должно иметь право:**

а) через разумные промежутки времени и без задержек:

- **получать информацию от пользователя данных о том, хранит ли он персональные данные, субъектом которых является данный сотрудник;**
- **доступа к таким данным, хранимых пользователем;**

б) по необходимости исправлять или стирать такие данные.

Восьмой принцип**. Следует принять надлежащие меры по защите персональных данных от несанкционированного доступа, их изменения, раскрытия и уничтожения, а также от их случайной потери или уничтожения.**

Предотвращение незаконного использования информационных ресурсов. Информационные ресурсы организации предоставляются для производственных целей. Их использование должно быть санкционировано руководством. Использование этих ресурсов для целей, не связанных с основной работой организации, или для несанкционированных целей без утверждения руководства и процедур учета следует рассматривать как незаконное использование информационных ресурсов. При выявлении таких случаев с помощью средств отслеживания действий или других средств, их следует довести до сведения соответствующего руководства для наложения дисциплинарных взысканий.

Многие страны приняли или находятся в процессе принятия законодательства о защите от незаконного использования компьютеров. Использование компьютера для незаконных целей можно считать уголовным преступлением. Поэтому крайне важно, чтобы все пользователи получили письменную санкцию на доступ, который им разрешается. Сотрудников организации и пользователей со стороны следует предупредить, что они не имеют право доступа, кроме случаев, которые формально санкционированы и задокументированы.

5.12.2. Проверка безопасности информационных систем

Цель: Обеспечить соответствие систем политике и стандартам безопасности организации.

Безопасность информационных систем необходимо регулярно проверять.

Такие проверки следует проводить исходя из соответствующей политики безопасности, а технические платформы и информационные системы необходимо проверять на соответствие принятым стандартам обеспечения безопасности.

Соответствие политике безопасности. Все подразделения организации следует регулярно проверять, чтобы обеспечить соответствие принятой политике и стандартам безопасности. Проверке подлежат:

а) информационные системы и их поставщики;

б) информация и владельцы данных;

в) пользователи;

г) руководство.

Владельцы информационных систем (см. Ответственность за ресурсы) должны организовывать регулярные проверки своих систем на соответствие принятой политике безопасности, стандартам и другим требованиям к их защите.

Техническая проверка на соответствие стандартам безопасности. Информационные ресурсы необходимо регулярно проверять на соответствие стандартам обеспечения безопасности. Техническая проверка на такое соответствие включает в себя осмотр рабочих систем, чтобы гарантировать правильную реализацию средств управления безопасностью программного и аппаратного обеспечения. Этот вид проверки требует обращения за технической помощью к специалистам. Такая проверка должна проводиться опытным системным инженером вручную или автоматически с помощью пакета программ, который создает технический отчет для последующей обработки техническим специалистом.

Такие проверки должны проводиться только компетентными законными лицами или под их наблюдением.

5.12.3. Аудит систем

Цель: Свести вмешательство в процесс аудита систем к минимуму.

Необходимо иметь средства контроля для защиты рабочих систем и средств аудита во время их проверки.

Защита также требуется для обеспечения целостности средств аудита и предотвращения их несанкционированного использования.

Средства аудита систем. Для сведения риска возникновения сбоев в производственных процессах к минимуму требования к аудиту и работы, связанные с проверкой рабочих систем, следует аккуратно запланировать и согласовать. Предлагается рассмотреть следующее:

1. Требования к аудиту систем должны быть согласованы с соответствующим руководством.
2. Масштаб проверок необходимо согласовать и контролировать.
3. Проверки должны быть ограничены доступом к данным и программам только на чтение.
4. Другие типы доступа (отличные от доступа только на чтение) должны быть разрешены для отдельных копий системных данных, которые необходимо стереть по завершении процесса аудита.
5. Необходимо явно идентифицировать информационные ресурсы для проведения проверок и сделать их доступными.
6. Необходимо определить требования к специальной или дополнительной обработке и согласовать их с поставщиками услуг.
7. Все случаи доступа следует отслеживать и фиксировать в контрольном журнале для справок.
8. Все процедуры, требования и обязанности необходимо задокументировать.

Защита средств аудита систем. Доступ к средствам аудита систем, т.е. к программам и файлам данных необходимо защищать, чтобы предотвратить их возможное несанкционированное использование или компрометацию. Такие средства следует изолировать от разрабатываемых и рабочих систем, и их не следует хранить в библиотеках магнитных лент и на рабочих местах пользователей, если они не обеспечены надлежащей дополнительной защитой**.**

Контрольные вопросы

1. Назовите 10 разделов для управления ИБ по стандарту ISO 17799.

2. Расскажите о ключевых средствах контроля ИБ предприятия.

3. Дайте определения понятия «Политика безопасности» и опишите особенности его разработки.

4. Опишите основные положения политики обеспечения информационной безопасности.

5. Какие организационные меры используются при управлении ИБ?

6. Назовите вопросы, которые рассматриваются при заключении контрактов со сторонними организациями.

7. Приведите классификацию ресурсов и опишите уровни их защиты.

8. Перечислите правила безопасности при выборе и работе с персоналом.

9. Какие вопросы должны рассматриваться при обучении персонала?

10. Что включает в себя понятие «Защищенные области»?

11. Назовите основные правила защиты центров данных и компьютерных залов.

12. Какие требования предъявляются при защите оборудования?

13. Что включает понятие «администрирование компьютерных систем и вычислительных сетей»?

14. Как регламентируется защита вредоносного программного обеспечения?

15. Определите основные правила работы с носителями информации и их защитой.

16. Дайте характеристику понятия «управление доступа к системам».

17. В каком разделе стандарта ISO 17799 рассматриваются вопросы шифрования данных?

18. Какие вопросы рассматриваются в разделе «Планирование бесперебойной работы организации»?

19. Что контролируется при выполнении правовых требований?

20. Какие условия должны выполнятся при аудите ИБ?

Глава 6. Программные средства для проведения аудита информационной безопасности*

6.1. Анализ видов используемых программных продуктов

Выполнение комплекса работ при аудите информационной безопасности связано с большим объемом анализируемой информации, проведением оценок рисков и представления их в виде определенных документов. Кроме этого встает задача поиска уязвимости ресурсов и в целом анализа защищенности информационных систем.

Все эти задачи решить на основе использования «бумажных» методик не всегда предоставляется возможным.

Поэтому фирмы, занимающиеся проведением внешнего аудита используют различные программные продукты, которые можно разделить по назначению и методике использования на два вида:

1) инструментарий для анализа и управления рисками;
2) средства анализа защищенности информационных систем.

Первый вид программных систем построен на использовании методик одного из видов международных стандартов BS 7799 (метод CRAMM), стандарте ISO 17799 (система COBRA и система Кондор), американских стандартов в области анализа и управления рисками (RiskWatch).

* **Глава 6 написана к.т.н. Аверченковым А.В.**

Второй вид программных средств ориентирован на анализ защищенности автоматизированных систем (АС). Здесь можно выделить две группы систем, основанных:

- на использовании технологии интеллектуальных программных агентов (например, система ESM компании Symantec)
- использовании метода анализа на основе активного тестирования механизмов защиты путем эмуляции действий злоумышленника по осуществлению попыток сетевого вторжения в АС.

В качестве примера систем, использующих этот метод, могут быть приведены сетевые сканеры и наиболее известные из них Nessus.

Ниже рассмотрены общие характеристики названных систем.

6.2. Система CRAMM

Этот метод и программный комплекс на его основе был разработан в Великобритании (в 1985г.) и в дальнейшем доработан с учетом требований Британского стандарта BS 7799, принятого в 1995г.

В настоящее время CRAMM является, судя по числу ссылок в Интернет, самым распространенным методом анализа и контроля рисков.

Целью разработки метода являлось создание формализованной процедуры, позволяющей:

1) убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;

2) избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;

3) оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;

4) обеспечить проведение работ в сжатые сроки;

5) автоматизировать процесс анализа требований безопасности;

6) представить обоснование для мер противодействия;

7) оценивать эффективность контрмер, сравнивать различные варианты контрмер;

8) генерировать отчеты.

Анализ рисков включает в себя идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Контроль рисков состоит в идентификации и выборе контрмер, позволяющих снизить риски до приемлемого уровня.

Формальный метод, основанный на этой концепции, должен позволить убедиться, что защита охватывает всю систему и существует уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- угрозы идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с ИБ, оправданы.

Выполнение автоматизированных процедур в рамках метода CRAMM предполагает выделение трех последовательных этапов.

На **первом этапе** проводится анализ применяемых средств базового уровня системы защиты и делается заключение о соответствии уровню рисков.

Если по результатам проведения первого этапа установлено, что уровень критичности ресурсов является очень низким и существующие риски заведомо не превысят некоторого базового уровня, то к системе предъявляется минимальный набор требований безопасности. В этом случае большая часть мероприятий второго этапа не выполняется, а осуществляется переход к третьему этапу, на котором генерируется стандартный список контрмер для обеспечения соответствия базовому набору требований безопасности.

На **втором этапе** производится анализ угроз безопасности и уязвимостей. Исходные данные для оценки угроз и уязвимостей аудитор получает от уполномоченных представителей организации в ходе соответствующих интервью. Для проведения интервью используются специализированные опросники.

На **третьем этапе** решается задача управления рисками, состоящая в выборе адекватных контрмер.

Решение о внедрении в систему новых механизмов безопасности и модификация старых принимает руководство организации, учитывая связанные с этим расходы, их приемлемость и конечную выгоду для

бизнеса. Задачей аудитора является обоснование рекомендуемых контрмер для руководства организации.

В случае принятия решения о внедрении новых контрмер и модификации старых, на аудитора может быть возложена задача подготовки плана внедрения новых контрмер и оценки эффективности их использования. Решение этих задач выходит за рамки метода CRAMM.

Общая схема анализа угроз, уязвимостей и выбора контрмер показана на рис. 6.1.

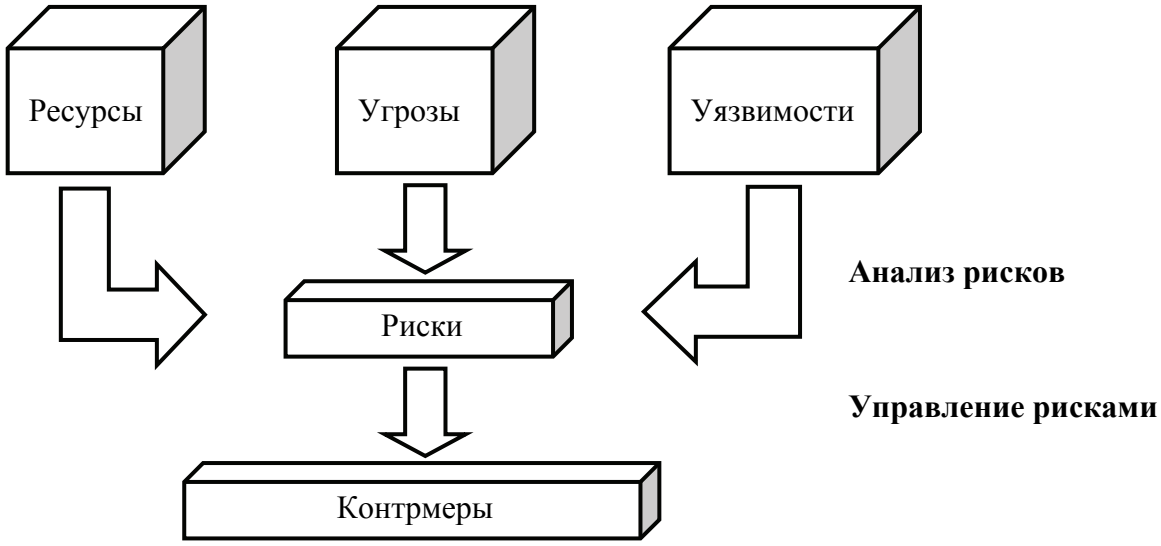

Рис. 6.1. **Концептуальная схема проведения обследования по методу CRAMM**

Процедура аудита в методе CRAMM является формализованной. На каждом этапе генерируется довольно большое количество промежуточных и результирующих отчетов.

Так, на **первом этапе** создаются следующие виды отчетов:

- Модель ресурсов, содержащая описание ресурсов, попадающих в границы исследования, и взаимосвязей между ними.
- Оценка критичности ресурсов.
- Результирующий отчет по первому этапу анализа рисков, в котором суммируются результаты, полученные в ходе обследования.

На **втором этапе** проведения обследования создаются следующие виды отчетов:

- Результаты оценки уровня угроз и уязвимостей.

- Результаты оценки величины рисков.
- Результирующий отчет по второму этапу анализа рисков.

По результатам **третьего этапа** обследования создаются следующие виды отчетов:

- Рекомендуемые контрмеры.
- Детальная спецификация безопасности.
- Оценка стоимости рекомендуемых контрмер.
- Список контрмер, отсортированный в соответствии с их приоритетами.
- Результирующий отчет по третьему этапу обследования.
- Политика безопасности, включающая в себя описание требований безопасности, стратегий и принципов защиты ИС.
- Список мероприятий по обеспечению безопасности.

Особого внимания заслуживают возможности CRAMM по автоматической генерации нескольких вариантов мер противодействия, адекватных выявленным рискам и их уровням, число которых в базе данных системы составляет более 1000. Все контрмеры разбиты на 61 группу:

- идентификация и аутентификация;
- логическое управление доступом;
- протоколирование;
- аудит;
- безопасность многократного использования объектов;
- тестирование систем;
- контроль целостности ПО;
- управление вводом/выводом;
- управление безопасностью в сети;
- обеспечение неотказуемости;
- обеспечение конфиденциальности вне соединения;
- управление доступом в сети;
- физическая безопасность сети;
- защита сообщений;
- обеспечение целостности данных вне соединения;
- сохранение правильной последовательности сообщений;
- пополнение трафика;
- контроль операций в системе;
- контроль действий системного администратора;

- контроль действий прикладных программистов;
- контроль операций по поддержке прикладного ПО;
- контроль операций по обслуживанию СВТ;
- контроль пользователей;
- контроль ввода/вывода приложений;
- финансовая отчетность;
- контроль выходных документов;
- контроль носителей данных;
- контроль транспортировки физических носителей данных;
- резервное копирование и восстановление для серверов;
- резервирование и восстановление сетевых интерфейсов;
- резервирование и восстановление сетевых сервисов;
- восстановление помещений;
- резервирование и восстановление носителей данных;
- планирование восстановления;
- резервное копирование данных;
- планирование потребностей в ресурсах;
- защита от сбоев СВТ;
- обеспечение физической безопасности помещений;
- оптимизация расположения СВТ в помещениях;
- организация зон безопасности;
- защита от краж;
- физическая защита СВТ;
- контрмеры против террористов и экстремистов;
- защита средств контроля доставки;
- обнаружение бомб и взрывчатых веществ;
- защита от минирования со стороны сотрудников и посторонних лиц;
- защита от пожара;
- защита от затоплений;
- защита от природных катаклизмов;
- защита источников электропитания;
- защита поддерживающей инфраструктуры;
- защита персонала;
- обучение персонала;
- политика безопасности;
- инфраструктура безопасности;

- оповещение об инцидентах;
- проверка жалоб.

Грамотно применять метод CRAMM в состоянии только высококвалифицированный аудитор, прошедший обучение. Если организация не может себе позволить содержать в штате такого специалиста, тогда самым правильным решением будет приглашение аудиторской фирмы, располагающей штатом специалистов, имеющих практический опыт применения метода CRAMM.

Обобщая практический опыт использования метода CRAMM при проведении аудита безопасности, можно сделать следующие выводы, относительно сильных и слабых сторон этого метода.

К **сильным сторонам метода CRAMM** относится следующее:

- CRAMM является хорошо структурированным и широко опробованным методом анализа рисков, позволяющим получать реальные практические результаты.
- Программный инструментарий CRAMM может использоваться на всех стадиях проведения аудита безопасности ИС.
- В основе программного продукта лежит достаточно объемная база знаний по контрмерам в области информационной безопасности, базирующаяся на рекомендациях стандарта BS 7799.
- Гибкость и универсальность метода CRAMM позволяет использовать его для аудита ИС любого уровня сложности и назначения.
- CRAMM можно использовать в качестве инструмента для разработки плана непрерывности бизнеса и политик информационной безопасности организации.
- CRAMM может использоваться в качестве средства документирования механизмов безопасности ИС.

К **недостаткам метода CRAMM** можно отнести следующее:

- Использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора.
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки.

- Аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора.
- Программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике.
- CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся.
- Возможность внесения дополнений в базу знаний CRAMM не доступна пользователям, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации.

6.3. Система КОНДОР

Существует целый ряд зарубежных и отечественных систем, позволяющих провести проверку соответствия информационной системы требованием стандарта ISO 17799. В основе этих программных комплексов лежит использование принципов экспертных систем, включающих обширные базы знаний по угрозам и уязвимостям и большое количество вопросников. Наиболее известной из зарубежных систем этого класса является система COBRA. Аналогом подобной системы является система КОНДОР, разработанная российской консалтинговой компанией Digtal Secrity [9].

Рассмотрим более подробно эту систему.

КОНДОР – предназначен для проверки соответствия политики информационной безопасности предприятия требованиям ISO 17799.

КОНДОР включает в себя более 200 вопросов, соответствующих 10 направлениям, определяемых стандартом ISO 17799.

Принцип работы системы заключается в постановке вопросов пользователю и составлении рекомендаций и отчетов на их основе. На рис. 6.2 представлено рабочее окно системы КОНДОР при анализе направления "Контроль доступа" в компании.

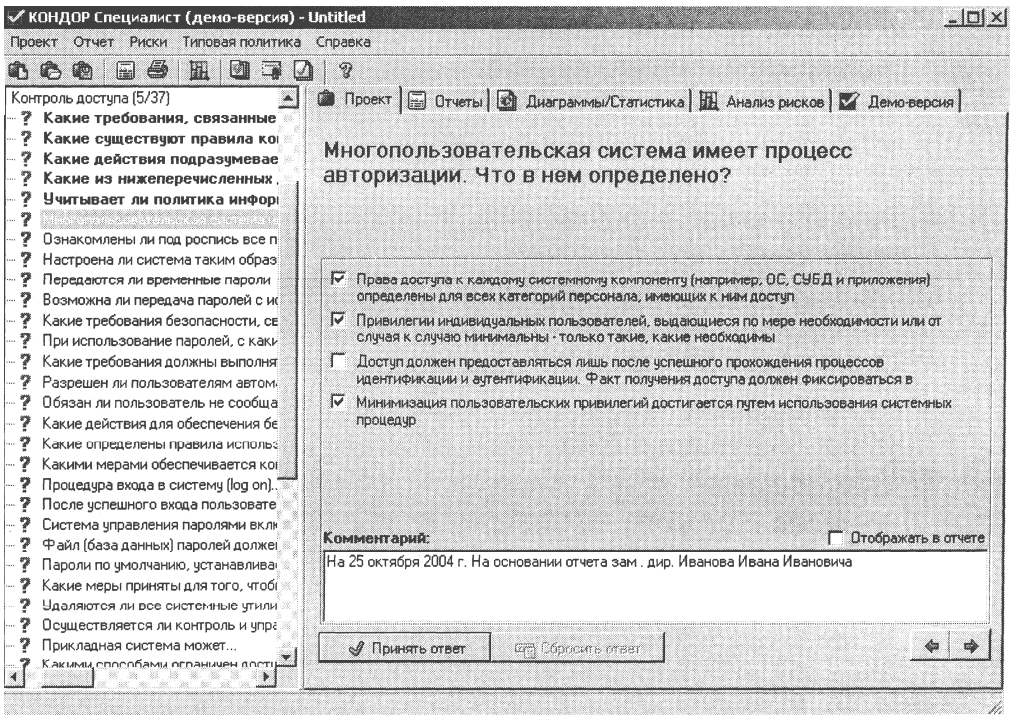

Рис. 6.2. **Вопросы анализа по направлению «Контроль доступа» в системе КОНДОР**

После определения ответов на поставленные вопросы система Кондор создает отчеты, которые включают:

1. Ответы на вопросы
2. Диаграммы и статистику (представлена на рис. 6.3)
3. Анализ рисков

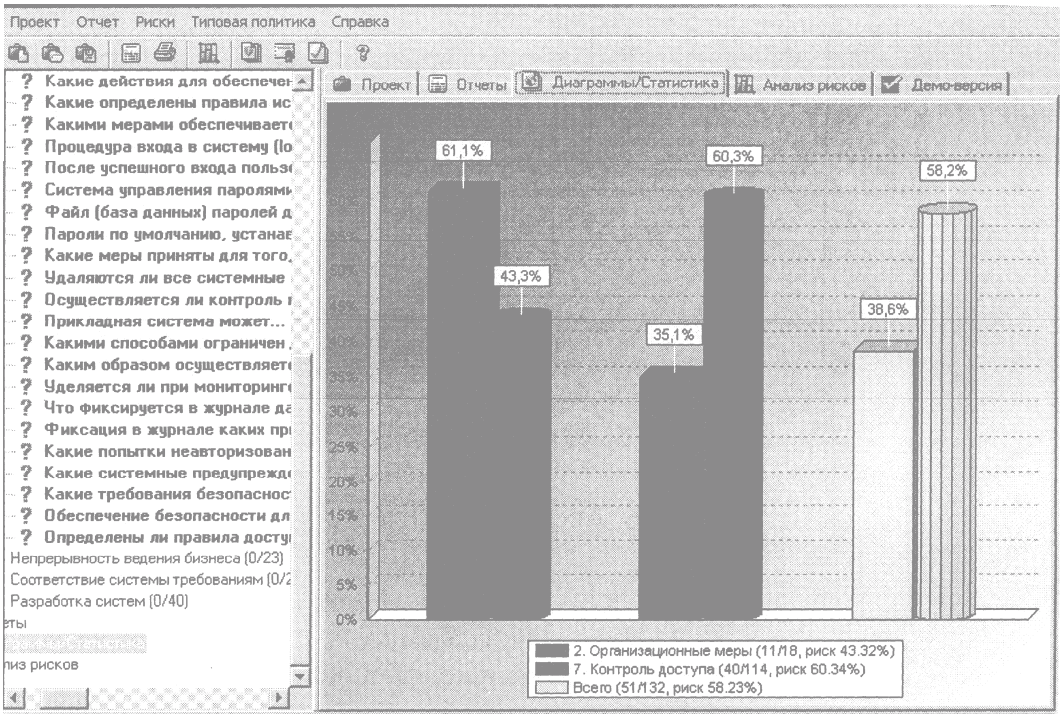

Рис. 6.3. **Диаграммы и статистика в системе КОНДОР**

Данные, представленные в разделе «Диаграммы и статистика» и «Анализ рисков», являются результатом работы системы и могут быть использованы при оценке информационной безопасности компании.

Кроме анализа система КОНДОР предоставляет ряд документов, требований и инструкций, которые могут помочь специалисту в разработке общей политики безопасности компании.

К недостаткам системы "КОНДОР" можно отнести:

- отсутствие возможности установки пользователем значимости каждого требования;
- отсутствие возможности внесения пользователем комментариев.

Демо-версия системы доступна для скачивания и изучения с официального сайта разработчиков http://www.dsec.ru/.

К наиболее важным элементам политики безопасности даются комментарии и рекомендации эксперта. По желанию специалиста, работающего с системой, может быть сформирован общий отчет, а также отдельные отчеты по одному или нескольким разделам стандарта ISO 17799.

Все варианты отчетов сопровождаются аналитическими диаграммами. Важной является процедура последовательного внесения изменений в политику безопасности с учетом выданных рекомендаций, что позволяет постепенно привести рассматриваемую на предприятии ситуацию в полное соответствие с требованиями стандарта ISO 17799.

6.4. Сетевые сканеры

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, в число которых входят ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС, в

конечном счете, приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Сканер является необходимым инструментом в арсенале любого администратора, либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и не потерявшие актуальности по сей день.

Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- идентификация доступных сетевых ресурсов;
- идентификация доступных сетевых сервисов;
- идентификация имеющихся уязвимостей сетевых сервисов;
- выдача рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и

т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество как коммерческих, так и свободно распространяемых сканеров, как универсальных, так и специализированных - предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в сети Интернет. Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 1000. Одним из наиболее продвинутых коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей UNIX, Windows и NetWare систем и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление обо всех продуктах этого класса.

Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

По своим функциональным возможностям сканер защищенности Nessus находится в одном ряду, а по некоторым параметрам и превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS и CyberCop Scanner компании NAI.

Версии 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (Сертификат N 361 от 18 сентября 2000 г.).

Сценарии атак реализованы в NESSUS в качестве подключаемых модулей (plugins). Количество подключаемых модулей постоянно увеличивается, в настоящее время насчитывается более 700. Новые внешние модули, эмулирующие атаки, можно инсталлировать,

скопировав файлы, содержащие их исходные тексты, с web-сервера разработчиков www.nessus.org.

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования TCP и UDP портов, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP. Кроме того, поддерживаются различные стелс-режимы сканирования, реализуемые популярным некоммерческим стелс-сканером nmap, который можно рассматривать в качестве одного из компонентов сканера Nessus. Другой популярный некоммерческий сканер queso используется в составе Nessus для определения типа и номера версии сканируемой ОС.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопотоковой архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов. Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения.

Подробное описание используемых методов сканирования TCP/UDP портов можно найти в онлайновой документации на сканер nmap.

При реализации Nessus использована нетипичная для сетевых сканеров клиент/серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных. Сервер nessusd работает только в среде UNIX и предназначен для выполнения сценариев сканирования. Механизмы собственной безопасности, реализованные в сервере nessusd, позволяют осуществлять аутентификацию пользователей сканера, ограничивать полномочия пользователей по выполнению сканирования и регистрировать все действия пользователей в журнале регистрации событий на сервере.

Клиентская часть Nessus работает и в среде UNIX, и в среде Windows и реализует графический интерфейс пользователя для

управления сервером nessusd. Пользователь сканера перед запуском сеанса сканирования определяет параметры сканирования, указывая диапазон сканируемых IP-адресов и TCP/UDP портов, максимальное количество потоков сканирования (число одновременно сканируемых хостов), методы и сценарии сканирования (plugins), которые будут использоваться.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак, обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеются специальные группы сценариев:

- Backdoors для обнаружения "троянских" программ;
- Gain Shell Remotely - для реализации атак на получение пользовательских полномочий на удаленной UNIX системе;
- Firewalls - для тестирования МЭ;
- FTP - для тестирования FTP-серверов;
- Windows - для поиска уязвимостей Windows-систем и т.п.

Особую группу сценариев сканирования Denail of Service составляют атаки на отказ в обслуживании (DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS - это выполнить эту атаку и посмотреть на реакцию системы. Эта группа сценариев, однако, является потенциально опасной, т.к. их запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных и "полный паралич" корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено.

Для написания сценариев атак служит специализированный C-подобный язык программирования высокого уровня NASL (Nessus Attack Scripting Language). Существует также интерфейс прикладного программирования (API) для разработки подключаемых модулей со сценариями атак на языке C, однако, предпочтительным является все же использование NASL.

NASL является интерпретируемым языком программирования, что обеспечивает его независимость от платформы. Он предоставляет мощные средства для реализации любых сценариев сетевого

взаимодействия, требующих формирования IP-пакетов произвольного вида.

Результаты работы сканера Nessus представляются в виде специальных протоколов. Данные об обнаруженных уязвимостях сортируются по IP-адресам просканированных хостов. Найденные уязвимости могут быть проранжированы. Наиболее критичные (security holes) уязвимости выделяются красным цветом, менее критичные (security warning) – желтым. По каждой уязвимости приводится ее описание, оценка ассоциированного с ней риска (Risk Factor) и рекомендации по ее ликвидации (Solution).

Контрольные вопросы

1. *Назовите виды используемых программных продуктов и их назначение.*
2. *Опишите назначение системы CRAMM.*
3. *Расскажите о концептуальной схеме проведения обследования предприятия по методу CRAMM.*
4. *Перечислите достоинства и недостатки CRAMM.*
5. *Охарактеризуйте назначение и принципы работы системы КОНДОР.*
6. *Для каких целей предназначены сетевые сканеры?*
7. *Приведите примеры сетевых сканеров и опишите сценарии их использования.*

Глава 7. Методика проведения аудита информационной безопасности на предприятии

7.1. Три подхода к проведению аудита ИБ

В настоящее время существует три главных практических подхода к анализу и оценке текущего состояния информационной безопасности предприятия [11]:

- анализ требований к корпоративной системе информационной безопасности;
- инструментальные проверки состояния информационной безопасности предприятия;
- анализ информационных рисков предприятия.

Первый подход обычно используется при определении так называемого базового уровня информационной безопасности предприятия, когда достаточно выработать и проверить их соблюдение на практике некоторых общих требований обеспечения информационной безопасности предприятия. Сегодня существует два основных способа определения названных требований: основанные на жестких априорных

(действующих РД Гостехкомиссии РФ) и на гибких адаптивных требованиях (ISO 15408). Более перспективным считается второй способ, что и подтверждается международной практикой выполнения подобных работ.

Второй подход, так называемый «активный аудит» (например, OSS TM-2.0 www.ideahamster.org), используется в основном для выявления возможных уязвимостей технического уровня обеспечения информационной безопасности предприятия. Данный подход является, безусловно, необходимым, но явно недостаточным для адекватного поставленным целям обеспечения информационной безопасности предприятия. Дело в том, что в этом подходе уделяется мало внимания *организационно-режимным средствам и мероприятиям, которые являются преимущественными по отношению к другим мерам и средствам защиты.* В результате при неправильном определении степени конфиденциальности защищаемой информации может оказаться неэффективным следование рекомендациям, полученным в ходе выполнения работ по активному аудиту сети предприятия. Другими словами, практика работ отчетливо показывает, что любая проверка эффективности системы защиты предприятия должна начинаться с *контроля и проверки организационно-режимных мер и средств защиты.* Цель этих мероприятий – выявление нарушений действующих на данном предприятии инструкций по обеспечению режима, а также определение степени соответствия данных инструкций возложенным на них задачам.

Третий подход (ISO 17799), основанный на использовании стандарта ISO 17799 предназначен для проведения полного анализа защищенности корпоративной сети и управления информационной безопасностью предприятия на основе специальных методов и инструментальных средств, построенных с использованием структурных методик системного анализа и проектирования, например COBRA, CRAMM, КОНДОР.

Данные методики позволяют [11]:

- убедиться, что требования, предъявляемые к организации системы безопасности, полностью проанализированы и документированы;
- избежать расходов на принятие излишних мер безопасности, что возможно при субъективней оценке рисков;
- оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;

- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- предоставить обоснование для мер противодействия;
- оценить эффективность различных вариантов контрмер;
- генерировать отчеты.

Очевидно, что в зависимости от поставленной задачи аудита безопасности на предприятии может быть использован любой из указанных подходов, а при необходимости – и их комбинация.

7.2. Задачи и содержание работ при проведении аудита ИБ

Здесь под термином «аудит информационной безопасности корпоративной системы» понимается *системный процесс* получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности на предприятии в соответствии с определенными критериями и показателями безопасности на всех основных уровнях обеспечения безопасности: *методологическом, организационно-управленческом, технологическом и техническом* [10].

В целом независимо от своей разновидности, состава и объема аудит безопасности корпоративной системы должен позволить решить следующие актуальные задачи каждого проверяемого предприятия:

- обеспечить (при необходимости повысить) информационную безопасность предприятия;
- снизить потенциальные потери предприятия путем повышения устойчивости функционирования корпоративной сети;
- защитить конфиденциальную информацию, передаваемую по открытым каналам связи;
- защитить информацию от умышленного искажения (разрушения), несанкционированного копирования, доступа или использования;
- обеспечить контроль действий пользователей в корпоративной сети предприятия;
- своевременно оценить и переоценить информационные риски

бизнес-деятельности компании;

- выработать оптимальные планы развития и управления предприятием.

Теперь посмотрим, что может лежать в основе проведения аудита информационной безопасности российских компаний.

Реализация описанного подхода может быть осуществлена в ходе следующих практических шагов аудита безопасности [10].

1. Комплексный анализ ИС предприятия и подсистемы информационной безопасности на методологическом, организационно-управленческом, технологическом и техническом уровнях. Анализ рисков.

1.1. Исследование и оценка состояния информационной безопасности ИС и подсистемы информационной безопасности предприятия.

1.1.1. Комплексная оценка соответствия типовых требований РД Гостехкомйссии РФ системе информационной безопасности предприятия.

1.1.2. Комплексная оценка соответствия типовых требований международных стандартов ISO системе информационной безопасности предприятия.

1.1.3. Комплексная оценка соответствия специальных требований Заказчика системе информационной безопасности предприятия.

1.2. Работы на основе анализа рисков.

1.2.1. Анализ рисков. Уровень управления рисками на основе качественных оценок рисков.

1.2.2. Анализ рисков. Уровень управления рисками на основе количественных оценок рисков.

1.3. Инструментальные исследования.

1.3.1. Инструментальное исследование элементов инфраструктуры компьютерной сети и корпоративной информационной системы на наличие уязвимостей.

1.3.2. Инструментальное исследование защищенности точек доступа предприятия в Internet.

1.4. Анализ документооборота предприятия.

2. Разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, общетехническому и программно-аппаратному обеспечению режима информационной безопасности предприятия.

2.1. Разработка концепции обеспечения информационной безопасности предприятия.

2.2. Разработка корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом, технологическом и техническом уровнях.

2.3. Разработка плана защиты предприятия Заказчика.

2.4. Дополнительные "работы по анализу и созданию методологического, организационно-управленческого, технологического, инфраструктурного и

технического обеспечения режима информационной безопасности предприятия Заказчика.

3. Организационно-технологический анализ ИС предприятия.

3.1. Оценка организационно-управленческого уровня безопасности.

3.1.1. Оценка соответствия типовым требованиям руководящих документов РФ к системе информационной безопасности предприятия в области организационно-технологических норм.

3.1.2. Анализ документооборота предприятия категории «конфиденциально» на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

3.3.3. Дополнительные работы по исследованию и оценке информационной безопасности объекта.

3.2. Разработка рекомендаций по организационно-управленческому, технологическому, общетехническому обеспечению режима информационной безопасности предприятия.

3.2.1. Разработка элементов концепции обеспечения информационной безопасности предприятия.

3.2.2. Разработка элементов корпоративной политики обеспечения информационной безопасности предприятия на организационно-управленческом, правовом и технологическом уровнях.

4. Экспертиза решений и проектов.

4.1. Экспертиза решений и проектов автоматизации на соответствие требованиям по обеспечению информационной безопасности экспертно-документальным методом.

4.2. Экспертиза проектов подсистем информационной безопасности на соответствие требованиям по безопасности экспертно-документальным методом.

5. Работы по анализу документооборота и поставке типовых комплектов организационно-распорядительной документации.

5.1. Анализ документооборота предприятия категории «конфиденциально» на соответствие требованиям концепции информационной безопасности, положению о коммерческой тайне, прочим внутренним требованиям предприятия по обеспечению конфиденциальности информации.

5.2. Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровне.

6. Работы, поддерживающие практическую реализацию плана защиты.

6.1. Разработка технического проекта модернизации средств защиты КИС, установленных у Заказчика по результатам проведенного комплексного аналитического исследования корпоративной сети.

6.2. Разработка системы поддержки принятия решений на предприятии Заказчика по обеспечению информационной безопасности предприятия на основе CASE-систем и программных СППР.

6.3. Подготовка предприятия к аттестации.

6.3.1. Подготовка «под ключ» предприятия к аттестации объектов информатизации заказчика на соответствие требованиям РД РФ.

6.3.2. Подготовка предприятия к аттестации КИС на соответствие требованиям по безопасности международных стандартов ISO 15408, ISO 17799, стандарта ISO 9001 при обеспечении требований информационной безопасности предприятия.

6.4. Разработка организационно-распорядительной и технологической документации.

6.4.1. Разработка расширенного перечня сведений ограниченного распространения как части политики безопасности.

6.4.2. Разработка пакета организационно-распорядительной документации (ОРД) в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровне.

6.4.3. Поставка комплекта типовой организационно-распорядительной документации в соответствии с рекомендациями корпоративной политики ИБ предприятия на организационно-управленческом и правовом уровнях.

7. Повышение квалификации и переподготовка специалистов.

7.1. Тренинги в области организационно-правовой составляющей защиты информации.

7.2. Обучение основам экономической безопасности.

7.3. Тренинги в области технологии защиты информации.

7.4. Тренинги по применению продуктов (технических средств) защиты информации.

7.5. Обучение действиям при попытке взлома информационных систем.

7.6. Обучение и тренинги по восстановлению работоспособности системы после нарушения штатного режима ее функционирования, а также по восстановлению данных и программ из резервных копий.

8. Сопровождение системы информационной безопасности после проведенного комплексного анализа или анализа элементов системы ИБ предприятия.

9. Ежегодная переоценка состояния ИБ.

7.3. Подготовка предприятий к проведению аудита ИБ

Каждая компания, решившая провести аудит информационной безопасности, в соответствии с требованиями международных стандартов должна осуществить подготовительные мероприятия, подготовить документацию и систему управления информационной

безопасностью. Только после выполнения этих требований компания приглашает аудитора.

Подготовительные мероприятия включают в себя подготовку нормативно-методической документации компании по организации информационной безопасности и проведение внутренней проверки соответствия системы обеспечения информационной безопасности компании требованиям стандарта ISO 17799.

Процесс аудита информационной безопасности компании начинается с подготовки детальных и подробных планов проведения аудита. Планы должны быть предоставлены соответствующим лицам компании до начала процедуры аудита безопасности. При этом важно, чтобы аудиторы были ознакомлены с тем, каким законодательно-правовым нормам и требованиям отраслевых и ведомственных стандартов следует проверяемая организация или компания.

Далее начинается проверка нормативно-методической документации компании, которая может проводиться как внутри компании, так и за ее пределами. Состав проверяемой документации может включать: *Концепцию и Политику безопасности,* описание рамок защищаемой системы*,* в том числе описание состава и структуры используемого на предприятии прикладного и системного программного обеспечения), *должностные инструкции* корпоративных пользователей, *положения* о Службе ИБ, а также описания *методик оценки и управления* информационными рисками, оценки состояния ИБ на предприятии, *правил и норм эксплуатации* программно-технических средств обеспечения информационной безопасности и пр.

Если предприятие уже проходило процедуру аудита, то также представляется отчет о предыдущей проверке и данные о всех выявленных ранее несоответствиях.

Кроме того, должна быть подготовлена так называемая *Ведомость соответствия* – документ, в котором оценивается соответствие поставленных целей и средств управления ИБ требованиям стандарта.

Сущность аудита безопасности на соответствие системы управления информационной безопасностью компании требованиям стандарта заключается в проверке выполнения каждого положения стандарта ISO 17799. По каждому такому положению проверяющие должны ответить на два вопроса: выполняется ли данное требование, и

если нет, то каковы причины невыполнения? На основе ответов составляется *Ведомость соответствия,* основная цель которой – аргументированное обоснование имеющихся отклонений ИБ от требований стандарта ISO 17799.

По завершении аудита безопасности выявленные несоответствия при необходимости могут быть устранены. Другими словами, в ходе выполнения аудита всего предприятия в целом, аудитор, выполняющий данную работу, должен собрать доказательства того, что оно отвечает всем требованиям стандарта ISO 17799. Это делается на основе анализа документов, бесед с экспертами, а при необходимости и проведения соответствующих организационных проверок режима безопасности и инструментальных проверок компонентов корпоративной системы.

В результате должны быть проверены: *организация* информационной безопасности компании, *обязанности* по обеспечению информационной безопасности сотрудников всех должностей, *наличие* документированной политики и стратегии информационной безопасности для компании и, в частности, документированной стратегии и общих положений подхода к оцениванию и управлению рисками.

При этом обращается внимание на наличие документированных, применимых на практике методик по оцениванию и управлению рисками, обоснования правильности выбора средств защиты для информационной системы компании. Попутно выявляется наличие документированных процедур оценки остаточного риска, проверки режима информационной безопасности, а также журналов, в которых фиксируются результаты проверки. У проверяющего аудитора должна быть полная ясность относительно наличия документированных правил обслуживания и администрирования информационной системы, наличия документированных распоряжений должностных лиц по проведению периодических проверок оценивания и управления рисками, документации по системе управления ИБ и реестра необходимых средств.

Аудитор, проводящий аудит информационной безопасности предприятия, должен сделать выборочные проверки выводов, сделанных при оценивании рисков. Для каждого случая нужно подтвердить, что все, что подверглось выборочной проверке, имеет

необходимую документацию в должном объеме, оценивание рисков было выполнено в соответствии с корректными методиками, а их результаты оформлены документально, достоверны и могут быть использованы. Кроме того, должен быть подтвержден факт соответствия рассматриваемым рискам средств обеспечения ИБ, выбранных на основе рекомендаций, их документирования, правильного использования и прохождения ими тестирования, а также знания сотрудниками политики информационной безопасности предприятия. Используемая система управления ИБ должна быть надлежащим образом документирована и подготовлен документ «Ведомость соответствия», в котором описаны риски, используемые законодательные и нормативные требования, указаны выбранные средства обеспечения ИБ и обоснован их выбор. В заключение проводящий аудит сотрудник должен стандартным образом оформить соответствующий документ.

В общем плане возможны два варианта аудита информационной безопасности: 1) *аудит предприятия в целом* и 2) *аудит только информационной системы* (в этом случае могут быть использованы также рекомендации международного стандарта ISO 15408.

В случае **аудита предприятии в целом** должны быть подготовлены для проверки [11]:

- документы, подтверждающие внедрение в организации выработанной политики информационной безопасности и, в частности, наличие документированного подхода к оцениванию и управлению рисками в рамках всей компании;
- описание организационной инфраструктуры ИБ на местах – распределение обязанностей сотрудников по обеспечению безопасности;
- обоснование выбора средств защиты для рассматриваемой системы;
- документация на процессы обслуживания и администрирования информационной системы;
- документация с описанием подходов к оцениванию и управлению рисками;
- документация по подготовке периодических проверок по оцениванию и управлению рисками;

- описание процедуры принятия уровня остаточного риска, с документированным выводом о реализации необходимых средств обеспечения ИБ, степени их тестирования и корректности использования;
- документация по системе управления ИБ и реестр средств управления безопасностью в документе «Ведомость соответствия»;
- результаты оценивания рисков по информационной системе;
- описание контрмер для противодействия выявленным рискам.

Все перечисленные проверки выполняются с использованием принятых в компании подходов к оценке и управлению рисками.

В случае **аудита только информационной системы** предприятие должно подготовить для проверки:

- описание политики информационной безопасности, документацию по системе управления информационной безопасностью и документ «Ведомость соответствия», отражающий реальное состояние оцениваемой системы;
- документацию по проведенному оцениванию рисков;
- документацию по средствам управления ИБ;
- доказательства эффективности принятых контрмер и результаты их тестирования.

Кроме того, при аудите только информационной системы аудитор должен подтвердить документированность вопросов, рассматриваемых в ходе проведения периодических проверок системы управления информационной безопасностью, а также корректность оценки рисков, выполненных посторонними или рекомендуемыми стандартом методами. Он должен заверить достоверность результатов оценки, подтвердить, что результаты оценивания рисков достоверны, приемлемы и документированы должным образом. Познакомившись со средствами обеспечения информационной безопасности, аудитор должен подтвердить, что необходимые средства обеспечения ИБ были установлены корректно, прошли тестирование и правильно используются, сотрудники знакомы с Политикой информационной безопасности, а система управления информационной безопасностью должным образом документирована и подготовлен документ «Ведомость соответствия». В заключение проводящий аудит сотрудник должен стандартным образом оформить соответствующий документ.

7.4. Планирование процедуры аудита ИБ

В соответствии с рекомендациями международных стандартов информационной безопасности процедура проведения аудита безопасности компании должна планироваться заранее. Для этого необходимо составить *план проведения аудита,* который должен отражать все мероприятиями процедуры, связанные с первоначальными и контрольными проверками продолжительностью более одного дня. Кроме того, необходимо ознакомиться с соответствующей законодательной и нормативной базой для выявления требований по информационной безопасности, которые могут быть использованы для обеспечения информационной безопасности компании.

Для проведения аудита информационной безопасности компании необходимо подготовить все необходимые сведения о собственной структуре, бизнес-деятельности, текущих проектах, состоянии информационной инфраструктуры и т.п. Кроме того, потребуется документально оформленные Концепция и Политика безопасности компании, список используемого в компании системного и прикладного программного обеспечения, описание технологии обработки данных, состав и структура подсистемы защиты информации, а также общая карта компьютерной сети компании.

План проведения аудита должен определять проверяемые области деятельности компании и время их проверки с указанием, какие именно требования международных стандартов, например ISO 15408, ISO 17799, и руководящих документов Гостехкомиссии РФ будут проверяться (согласно «Ведомости соответствия»). Другими словами, план подготовки и проведения аудита должен определять потребности компании в оценке и объективном анализе состояния информационной безопасности, потребности в соответствующих аппаратно-программных средствах защиты информации, потребности в обучении и переподготовке службы информационной безопасности, а также освещать другие вопросы, ответы на которые невозможно дать без проведения аудита. В дальнейшем план проведения аудита с внесенными в него изменениями по ходу проверок прилагается к отчету о проведении аудита. Кроме того, необходимо помнить о согласовании

плана проведения аудита с концепцией и политикой информационной безопасности компании.

Рекомендуется выделять четыре возможных этапа планирования аудита: п*одготовка аудита безопасности*, *анализ требований и исходных данных*, *расчет трудоемкости и стоимости выполняемых работ и документирование процедуры проведения аудита* [11].

1. На **подготовительном этапе** исполнитель определяет общий порядок работ, устанавливающий последовательность выполнения и возможные затраты ресурсов, и согласовывает его с заказчиком. На этом этапе рассматриваются:

- Назначение и цели предстоящего аудита, порядок их достижения. Принципы установки рамок проведения аудита. Функции, структура и состав корпоративной системы, узкие места и потенциальные уязвимости в системе управления информационной безопасностью. Методики оценки квалификации специалистов и сотрудников службы ИБ. Способы категорирования обрабатываемой в корпоративной информационной системе информации, например на общедоступную, конфиденциальную и строго конфиденциальную.
- Методы и инструментарии оценки временных затрат и затрат ресурсов компании на аудит информационной безопасности. Возможность использования результатов ранее проведенного аудита, в том числе анализа информационных рисков и анализа соответствия требованиям международных стандартов и руководящих документов Гостехкомиссии РФ.
- Состав группы экспертов в области безопасности корпоративных систем и распределение обязанностей между ними.
- Параметры корпоративной информационной сети предприятия и среды ее функционирования, оказывающие существенное влияние на качество аудита безопасности
- Совокупность учитываемых при проведении аудита безопасности требований международных, государственных, межведомственных и внутренних стандартов.
- Внутренняя отчетная документация, оформление и при необходимости корректировка концепции и политики информационной безопасности предприятия.
- Перспективы и тенденции развития корпоративной системы

защиты информации предприятия, вопросы выработки стратегии и тактики его развития.

Согласованный с заказчиком общий порядок проведения аудита безопасности компании может быть отражен в соответствующем техническом задании.

2. **Этап анализа требований и исходных данных** составляет главную часть планирования аудита. В процессе анализа рассматриваются:

- *Требования информационной безопасности.* Цель аудита – объективно и оперативно оценить и проверить соответствие исследуемой корпоративной системы защиты компании предъявляемым к ней требованиям ИБ. Поэтому для такой оценки необходимо сначала рассмотреть требования информационной безопасности. Основными требованиями информационной безопасности для отечественных предприятий и компаний являются требования руководящих документов Гостехкомиссии РФ, законов Российской Федерации, внутриведомственных, межведомственных, национальных и международных стандартов. Кроме этого, для каждой корпоративной информационной системы необходимо учитывать специальные требования внутреннего использования, согласованные с концепцией и политикой безопасности компании.

- *Исходные данные для проведения аудита.* В руководящем документе Гостехкомиссии «Положение по аттестации объектов информатизации по требованиям безопасности информации» приводится стандартный перечень исходных данных, необходимых для разработки программы и методики аттестационных испытаний. Помимо стандартных исходных данных могут использоваться и дополнительные исходные данные, специфичные для каждого конкретного предприятия, например, статистика нарушений политики безопасности компании, статистика внешних и внутренних атак, уязвимости наиболее критичных корпоративных информационных ресурсов и т. д. Также нужно учитывать, что, как правило, руководство компании имеет собственные взгляды на информацию, предоставляемую в качестве исходных данных для аудита безопасности. Поэтому между заказчиком и исполнителем работ по аудиту ИБ рекомендуется заключить специальное соглашение о конфиденциальности или соответствующий протокол о намерениях.

- *Рамки проведения аудита.* При определении рамок проведения аудита необходимо в равной степени учитывать организационный, технологический, и программно-технический уровни обеспечения информационной безопасности. В противном случае результаты аудита не будут объективно отражать реальный уровень информационной безопасности компании. Например, дорогостоящие аппаратно-программные средства защиты информации могут оказаться бесполезными, если неправильно определены и реализованы меры и мероприятия на организационном и технологическом уровнях. При определении рамок аудита необходимо зафиксировать штатные условия функционирования корпоративной информационной системы безопасности предприятия.
- *Области детального изучения.* При проведении аудита основное внимание должно уделяться компонентам и подсистемам, осуществляющим обработку конфиденциальной информации предприятия. При этом необходимо уметь рассчитать возможный ущерб, который может быть нанесен компании в случае разглашения конфиденциальной информации и нарушения политики безопасности. Это должно быть отражено в соответствующих документах компании, регламентирующих ее политику информационной безопасности. Для определения возможного ущерба могут использоваться разнообразные формальные методы, например методы экспертных оценок.
- *Требуемый уровень детализации и полноты.* В большинстве случаев для получения адекватных результатов достаточно провести базовый анализ корпоративной системы защиты информации, позволяющий определить общий уровень ИБ предприятия и проверить его на соответствие некоторым требованиям безопасности. В некоторых случаях дополнительно требуется провести детальный анализ, цель которого – количественно оценить уровень информационной безопасности компании на основе специальных количественных метрик и мер информационной безопасности. Для этого сначала определяются все необходимые количественные показатели, а затем производится оценка уровня информационной безопасности компании. Существенно, что при этом становится возможным сравнивать уровень безопасности компании с некоторым эталоном, определять тенденции и перспективы развития системы корпоративной безопасности, необходимые инвестиции и т. д.

3. На ***этапе расчета трудоемкости и стоимости*** проводимых работ по данным проведенного анализа оцениваются временные, финансовые, технические, информационные и прочие ресурсы, необходимые для аудита информационной безопасности. Выделение ресурсов рекомендуется производить с учетом возможных нештатных ситуаций, способных увеличить трудоемкость аудита безопасности.

4. Завершается планирование аудита ***этапом формализации и документирования выполнения аудита,*** что прежде всего подразумевает подготовку и согласование плана проведения аудита. План проведения аудита в общем случае включает в себя следующие разделы:

- ***Краткая характеристика работ***. Здесь представляются все необходимые сведения о порядке проведения работ;
- ***Введение***. Указывается актуальность проведения аудита безопасности, особенности и требования к порядку проведения аудита, характеристика исследуемого объекта, рамки проведения аудита, общий порядок работ, требования по фиксации результатов аудита. Дополнительно приводятся сведения о категорировании корпоративной информации, например конфиденциальной и строго конфиденциальной. Также перечисляются основные решаемые задачи, ограничения, выполняемые функции и критерии оценивания уровня ИБ предприятия, требования нормативных документов РФ, международных стандартов и внутренних требований предприятия;
- ***Распределение обязанностей***. Определяется штат и функциональные обязанности группы специалистов, которые будут проводить аудит безопасности;
- ***Требования информационной безопасности***. Фиксируется обоснованный выбор требований ИБ, определяются критерии и показатели оценки ИБ предприятия, выбираются количественные метрики и меры безопасности. Помимо нормативной и законодательной базы РФ дополнительно рекомендуется использовать требования международных и внутренних стандартов компании, актуальные для каждой отдельно взятой.
- ***Формализация оценок уровня безопасности предприятия.*** Определяются качественные и количественные

параметры для получения объективных оценок уровня ИБ предприятия. Перечисляются задачи, выполняемые при проведении базового и детального анализа информационных рисков. В этом разделе отражаются критичные информационные ресурсы компании, оценка экономической эффективности ее деятельности, используемые модели, методы средства проведения аудита безопасности, исходные данные.

- ***План-график работ***. Определяются сроки, календарный план выполняемых работ, время их окончания, формы отчетных документов, требования по приему-сдаче работы и прочее;
- ***Поддержка и сопровождение***. Перечисляются требования к административной, технологической и технической поддержке аудита ИБ;
- ***Отчетные документы***. Основными отчетными документами являются отчет по результатам аудита безопасности, концепция и Политика информационной безопасности, План защиты компании;
- ***Приложения***. В приложениях приводятся протоколы проверок, а также информация по методикам и инструментарии проведения аудита, выявленные замечания, рекомендации и прочее.

7.5. Организация работ по аудиту ИБ

Организация проведения работ по аудиту безопасности должна начинаться с официального вступительного собрания. На собрании до сотрудников, занимающихся вопросами безопасности, руководства среднего и верхнего звена (TOP-менеджеров предприятия) доводятся следующие вопросы:

- план проведения аудита, в котором описано, что и когда планируется проверять;
- поясняются методы оценки рисков, которые предполагается использовать в процессе проверки;
- объясняется процедура определения несоответствий, их квалификация и действия по их устранению;
- разъясняются причины, по которым по результатам проверки могут быть сделаны замечания, и возможная реакция на них;
- перечисляются руководящие документы аудитора и компании и правила доступа к ним;

- выясняются возможные трудности, которые могут возникнуть в процессе работы – отсутствие ведущих специалистов и т.д.;
- обговаривается организация работы с конфиденциальными сведениями компании, необходимыми для проведения аудита, включая отчет о проведении аудита и замечания о несоответствиях.

Администрация компании должна понимать, что аудитору, возможно, потребуется обратиться к потенциально уязвимым участкам компьютерной информационной системы и конфиденциальной информации компании, например к спискам паролей и учетных записей корпоративных пользователей, личным делам сотрудников, результатам проверки лояльности сотрудников компании и пр.

В процессе аудита подсистемы информационной безопасности компании на соответствие стандарту ISO 17799 аудиторы должны проанализировать наиболее важные аспекты с учетом объема подлежащей защите проверяемой информации, ее специфики и ценности для проверяемого предприятия.

В результате проведения аудита создается список замечаний, выявленных несоответствий требованиям стандарта и рекомендаций по их исправлению. При этом аудиторы должны гарантировать выполнение всех требований процедуры аудита. Поскольку и аудиторам, и проверяемой компании необходимо знать, насколько серьезны обнаруженные недостатки и каковы способы их исправления, то в *стандарте используются следующие категории несоответствия* [11].

Существенное несоответствие: не выполняется одно или несколько базовых требований стандарта ISO 17799 или установлено использование неадекватных мер по обеспечению конфиденциальности, целостности или доступности критически важной информации компании, приводящих к недопустимому информационному риску.

Несущественное несоответствие: не выполняются некоторые второстепенные требования, что несколько повышает информационные риски компании или снижает эффективность мер обеспечения информационной безопасности компании.

Каждое выявленное несоответствие обязательно должно иметь ссылку на соответствующее требование стандарта ISO 17799. При выявлении в процессе проверки значительного числа несущественных несоответствий аудитор обязан исследовать возможность

возникновения существенного несоответствия. После выявления несоответствий аудитор и представители компании обязаны наметить пути их устранения. По результатам проверки аудитор может сформулировать в отчетных документах замечание, если он допускает возможность усовершенствования подсистемы ИБ компьютерной информационной системы. Реакция предприятия на замечания аудитора может быть различной, поскольку компании сами в добровольном порядке определяют свои действия по их устранению. Замечания фиксируются и при последующих проверках. Аудиторы обязаны выяснить действия предприятия по их устранению.

Аудитор анализирует предоставленные компанией ранее описанные документы, а в случае повторного аудита компании или ее подсистемы информационной безопасности предоставляет «Ведомость соответствия» – документ, составленный аудитором при предыдущей проверке.

После проведения аудита проводится заключительное собрание с руководителями верхнего звена, на которое выносится:

- подтверждение заявленных перед проверкой объема проверок и рамок аудита;
- краткое изложение найденных несоответствий и согласованных изменений;
- ознакомление присутствующих с замечаниями и предложениями по их устранению;
- общие замечания по ходу аудита и комментарии к отчету;
- оглашение выводов: положительное заключение, отказ в сертификации или продолжение аудита;
- подтверждение взятых обязательств по сохранению конфиденциальности сведений, полученных в ходе аудита.

Участники вступительного и заключительного собраний должны быть официально зарегистрированы. Главным результатом проведения аудита является официальный отчет, в котором должны быть отражены:

- степень соответствия проверяемой компьютерной информационной системы стандарту ISO 17799 и собственным требованиям компании в области информационной безопасности согласно плану проведения аудита и «Ведомости соответствия»;
- подробная ссылка на основные документы заказчика, включая

политику безопасности, «Ведомость соответствия», описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании;

- общие замечания по выводам проведения аудита;
- количество и категории полученных несоответствий и замечаний;
- необходимость дополнительных действий по аудиту и их общий план;
- список сотрудников, принимавших участие в тестировании.

В практических рекомендациях Британского института стандартов BSI отмечается, что в среднем трудоемкость аудита информационной безопасности средней и крупной компаний может составлять 30-45 человеко-дней работы аудитора. По результатам успешно выполненного аудита компании или ее информационной системы и подсистемы информационной безопасности осуществляется выдача сертификатов на соответствие стандарту BS ISO/IEC 7799:2000 (BS 7799-1:2000), которые считаются действительными в течение 3 лет.

7.6. Алгоритм проведения аудита безопасности предприятия

Исходя из опыта многих компаний, занимающихся проведением аудита информационной безопасности, может быть рекомендован следующий алгоритм его проведения.

I. ***Определение и систематизация перечня угроз информационной безопасности****.*

1. Оформление официальных запросов предоставления информации об организационно-штатной структуре, организации сети, организации защиты информации, отправка Заказчику.

2. Получение информации, проведение первичного анализа системы информационной безопасности объекта, выбор инструментальных средств для проведения исследования уязвимостей сети.

3. Выезд на предприятие для предварительного обследования

корпоративной сети:

- проведение экспресс-анализа по выделению наиболее критичных автоматизированных систем, исходя из потенциальной ценности обрабатываемой и хранимой в них информации;
- проведение работы по построению структурной и функциональной схемы информационной системы с обозначением основных информационных потоков обмена информацией;
- проведение работы по построению типовой модели нарушителя для информационной системы, перечня угроз информационной безопасности в информационной системе (совместно с представителями структурных подразделений безопасности);
- проведение работы по наложению перечня сведений ограниченного распространения на функциональную схему информационной системы, выделение критичных информационных ресурсов, методов и средств их защиты;
- проведение работы по изучению организационного обеспечения информационной безопасности в части организационно-штатной структуры, правового и технологического обеспечения;
- проведение работы по анализу уязвимостей компьютерной сети, в том числе с помощью инструментальных средств;
- проведение работы по анализу рисков в информационной системе, выработка уровней риска по различным видам угроз для конкретных информационных ресурсов корпоративной сети объекта;
- формирование выводов;
- проведение согласования отчетной документации по первому этапу работ.

II. Разработка концепции обеспечения информационной безопасности и эскизного проекта

1. Определение комплексных критериев для построения системы информационной безопасности – установление приемлемых уровней риска (совместно со службой безопасности).

2. Разработка концепции обеспечения информационной безопасности заказчика, включающей:

- описание целей защиты информации;
- описание задач, решаемых для достижения целей защиты информации;

- описание основных объектов защиты, угроз их безопасности, учитывая специфику деятельности;
- взгляды на основные направления, условия и порядок практического решения задач информационной безопасности по направлениям: правовому, организационному и техническому;
- основные принципы взаимодействия подразделений для наиболее эффективного достижения целей системы информационной безопасности;
- перспективную программу создания системы информационной безопасности.

3. Разработка требований к системе ИБ, включающих:

- общие принципы защиты информационного ресурса, классифицированные в соответствии с угрозами информационной безопасности;
- требования к организационному и правовому обеспечению информационной безопасности с учетом выбранного критерия;
- описание конкретных мер защиты, рекомендованных для построения системы информационной безопасности с учетом выбранного критерия;
- требования к настройкам используемого в информационной системе активного сетевого оборудования, операционных систем, систем управления базами данных, почтовых систем и Web-браузеров, реализации заложенных в них механизмов безопасности, обновлению программного обеспечения, установке необходимых обновлений программного обеспечения;
- описание требований к средствам защиты информации в корпоративной сети, включая централизованные системы управления защитой сети, интегрированные системы безопасности с системами управления сетью, распределенные межсетевые экраны, системы виртуальных частных сетей, системы аудита и мониторинга безопасности сети, системы централизованной антивирусной защиты, средства обеспечения защиты рабочих станций от несанкционированного доступа, системы электронной цифровой подписи, системы поддержания отказоустойчивости;
- требования по настройке элементов системы защиты.

4. Проведение технико-экономической оценки мероприятий по

обеспечению информационной безопасности.

5. Разработка Эскизного проекта обеспечения безопасности на объекте Заказчика.

6. Разработка организационно-распорядительной документации согласно заданию Заказчика, а также на основании результатов проведенного исследования.

7. Разработка Плана защиты, включающего календарный план построения системы информационной безопасности.

8. Предложения по управлению (оценка и переоценка рисков предприятия) информационной безопасностью предприятия.

9. Предложения по сопровождению корпоративной системы обеспечения безопасности.

Приведем примерный план по проведению аудита информационной безопасности с указанием времени выполнения его основных этапов (табл. 7.1.).

Таблица 7.1

Примерный план действий по разработке концепции обеспечения информационной безопасности и эскизного проекта [11]

Этап	**Место проведения**	**Сроки проведения (раб. дни)**	**Представляе-мые отчетные документы**
1. Сбор Заказчиком и предоставление Исполнителю комплекта технической, проектной, управленческой документации по первому этапу работ, необходимой для проведения научно-исследовательских работ по определению и систематизации перечня угроз информационной безопасности	Предприятие	10	Акт приема-передачи документации
2. Составление на основании данных, полученных от Заказчика, плана мероприятий по проведению научно-исследовательских работ	Исполнитель	5	План мероприятий

Окончание табл. 7.1

Этап	Место проведения	Сроки проведения (раб. дни)	Представляе-мые отчетные документы
3. Выезд на объект для дополнительного сбора информации, проведения инструментальных проверок и анализа объекта на месте	Предприятие	15	–
4. Проведение научно-исследовательских работ по определению и систематизации перечня угроз, вероятности утечки информации по выявленным каналам, оценка потенциального возможного ущерба и формирование выводов. Оформление отчета	Исполнитель	25	Отчет по исследованию объекта
5. Согласование отчета с Заказчиком. Определение критерия для построения системы информационной безопасности. Согласование перечня документов организационно-нормативной базы для последующей разработки	Предприятие	10	–
6. Разработка концепции, требований к системе информационной безопасности, упрощенного технико-экономического расчета, эскизного проекта, организационно-распорядительной документации, плана защиты, планы работ по сопровождению, оценки и переоценки информационных рисков предприятия	Исполнитель	25	Пакет документов на этапе разработки требований и рекомендаций безопасности
7. Согласование, отработка замечаний и защита отчетных документов по п.4 и 6	Предприятие	30	Акт выполненных по договору работ
ИТОГО:		120	

7.7. Перечень данных, необходимых для проведения аудита ИБ

Проведение аудита ИБ требует анализа большого объема данных, характеризующих все стороны деятельности предприятия, связанных с ИБ. Можно рекомендовать следующую структуру данных, разделенных по определенным направлениям изучения фактического состояния объекта [11].

***Общая информация об организации**:*

- иерархическая организационная структура организации;
- сведения о степени конфиденциальности данных, хранящихся, обрабатываемых и передаваемых по каналам связи, в том числе с использованием средств вычислительной техники;
- руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, обработки и передачи информации, доступа в помещения;
- положение о защите информации в организации;
- перечень сведений, составляющих в организации коммерческую или служебную тайну.

Информация технологического характера о функционировании предприятия Заказчика:

- технологические связи между отделами на уровне потоков данных, передачи файлов;
- направления движения потоков данных;
- служебные инструкции персонала;
- технология доступа к критичным ресурсам: к информации, в помещения руководства, для администраторов безопасности и персонала;
- работа систем электронного документооборота;
- планы эксплуатационных и сервисных .мероприятий;
- выделение критичных для предприятия процессов обработки и передачи данных;
- проекты развития и доработки информационных систем;
- информация о размещении критичных помещений, места хранения ценностей и данных;
- информация об управлении и контроле доступа в критичные помещения.

Информация об имеющихся средствах вычислительной техники

Серверные платформы:

- количество серверов;
- применяемые аппаратные платформы, аппаратное обеспечение;
- операционные системы, в том числе наименование, полная версия, полные версии «заплат» (patch, service pack);
- поддерживаемые системные задачи с привязкой к серверам;
- используемые сетевые протоколы;
- документация производителей средств вычислительной техники;
- собственная технологическая документация;
- использование встроенных средств защиты информации и возможностей по архивированию.

Информация о топологии сети и сетевых соединениях:

- карта сети;
- наложение информационных потоков на карту сети;
- распределение серверов по сегментам сети, наличие на них критичной информации;
- распределение рабочих станций по сегментам сети, наличие на них критичной информации, наличие доступа к критичной информации в сети;
- используемые Internet-сервисы, организация выхода в Internet;
- наличие собственного внутреннего/внешнего WWW-узла;
- доступ с WWW-узла к системам управления базами данных и системам электронного документооборота;
- поддерживаемые протоколы обмена данными;
- системное сетевое программное обеспечение, в том числе наименование, полная версия, полная версия «заплат» (patch);
- типы применяемого сетевого оборудования, версии прошивок/операционных систем маршрутизаторов, коммутаторов и пр. особенности их настройки;
- системы управления сетевым оборудованием;
- документация производителей на сетевое оборудование;
- собственная технологическая документация;
- использование встроенных средств защиты информации (наличие криптографических протоколов и специального канального

оборудования для шифрования критичного трафика);

- проекты развития и изменения информационной системы предприятия;
- наложение информационных потоков циркуляции информации на карту сети.

Информация об используемых клиентских и не включенных в сеть рабочих местах:

- количество, тип, место установки и назначение;
- аппаратные платформы, аппаратное обеспечение, фирма-производитель, фирма-поставщик, описание;
- операционные системы, в том числе наименование, полная версия, полные версии «заплат» (patch, service pack);
- использование штатных (приобретенных) средств защиты от несанкционированного доступа.

Информация о программном обеспечении:

- перечень специальных систем: управления базами данных, электронного документооборота, «банк-клиент» с привязкой к конкретным серверам и клиентским рабочим местам;
- перечень прикладных программ сторонних производителей с привязкой к конкретным серверам и клиентским рабочим местам;
- перечень прикладных программ собственной разработки с привязкой к конкретным серверам и клиентским рабочим местам;
- решаемые задачи программного обеспечения;
- производитель, Internet-ссылка на сайт производителя;
- полная версия программного продукта и «заплат» (patch);
- операционные системы, в том числе наименование, полная версия, полные версии «заплат» (patch, service pack);
- сертификаты и документация производителя;
- доступные различным категориям пользователей функции;
- специальные возможности прикладного программного обеспечения;
- наличие критичных для предприятия процессов электронной обработки и передачи данных.

Информация о специальных системах, поддерживающих и контролирующих работу информационной системы:

- имеющиеся средства архивирования, режим их работы, места

хранения архивов;

- системы протоколирования действий пользователей, в том числе встроенные системы протоколирования СУБД, клиент-банка и пр.;
- средства системного аудита, авторизации и аутентификации;
- системы мониторинга сети.

Общие данные о функционировании информационной системы:

- наличие ответственного администратора сети;
- наличие ответственного администратора безопасности сети;
- порядок назначения прав доступа к критичным ресурсам;
- регламент резервирования и восстановления критичной информации;
- регламент функционирования в критических и нештатных ситуациях.

Данные о критичности информационных ресурсов по отношению к технологии предприятия.

Информация об имеющихся средствах обеспечения информационной безопасности

Информация о существующих или планируемых к внедрению технических средствах защиты информации *(производитель, Internet-ссылка на сайт производителя – полная версия, полная версия «заплат» (patch), операционная система, сертификаты и документация производителей, схема установки):*

- межсетевые экраны;
- системы мониторинга безопасности;
- системы сканирования безопасности сети и передаваемой информации;
- криптографические средства;
- средства предотвращения НСД;
- средства аудита безопасности;
- механические средства защиты от взлома и краж;
- анализаторы протоколов и трафика.

Принятая политика генерирования, смены и блокировки реквизитов для разрешения доступа к информационным ресурсам ЛВС

в различных ситуациях, в том числе при увольнении, переводе, совместительстве, отпуске сотрудника.

***Сведения о существующих или планируемых к внедрению технических средствах управления и контроля доступа**, видеонаблюдения, пожарно-охранной сигнализации на объекте:*

- перечень средств управления и контроля доступа, видеонаблюдения, пожарно-охранной сигнализации на объекте;
- техническая документация на технические средства;
- методические материалы по использованию технических средств.

7.8. Рекомендации по подготовке отчетных документов

Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита.

В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты.

В то же время наивно ожидать от аудитора в качестве результата проведения аудита выдачи технического проекта подсистемы информационной безопасности, либо детальных рекомендаций по внедрению конкретных программно-технических средств защиты информации. Это требует более детальной проработки конкретных вопросов организации защиты, хотя, внутренние аудиторы могут принимать в этих работах самое активное участие.

Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Структура отчета может существенно различаться в зависимости от характера и целей проводимого аудита. Однако определенные разделы

должны обязательно присутствовать в аудиторском отчете. Он должен, по крайней мере, содержать описание целей проведения аудита, характеристику обследуемой ИС, указание границ проведения аудита и используемых методов, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие ее требованиям стандартов, и, конечно, рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты.

Для примера, приведем образец структуры аудиторского отчета по результатам анализа рисков, связанных с осуществлением угроз безопасности в отношении обследуемой ИС [3].

Структура отчета по результатам аудита безопасности ИС и анализу рисков

1. Вводная часть

1.1. Введение
1.2. Цели и задачи проведения аудита
1.3. Описание ИС
1.3.1 Назначение и основные функции системы
1.3.2 Группы задач, решаемых в системе
1.3.3 Классификация пользователей ИС
1.3.4 Организационная структура обслуживающего персонала ИС
1.3.5 Структура и состав комплекса программно-технических средств ИС
1.3.6 Виды информационных ресурсов, хранимых и обрабатываемых в системе
1.3.7 Структура информационных потоков
1.3.8 Характеристика каналов взаимодействия с другими системами и точек входа
1.4 Границы проведения аудита
1.4.1 Компоненты и подсистемы ИС, попадающие в границы проведения аудита
1.4.2. Размещение комплекса программно-технических средств ИС по площадкам (помещениям)
1.4.3. Основные классы угроз безопасности, рассматриваемых в ходе проведения аудита
1.5 Методика проведения аудита
1.5.1 Методика анализа рисков
1.5.2 Исходные данные

7.9. Экономическая оценка обеспечения ИБ

Уже сейчас в отечественных информационных системах с повышенными требованиями в области ИБ (банковские системы, ответственные производства, и т.д.) затраты на обеспечение режима ИБ составляют до 30% всех затрат на ИС, и владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения ИБ [24]. Даже в тех ИС, уровень ИБ которых явно недостаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством (владельцами информационных ресурсов) затрат на повышение этого уровня.

Начальники служб автоматизации, исполнительные директора, начальники служб информационной безопасности должны иметь понятные для бизнеса аргументы для обоснования инвестиций в ИБ, т.е., по сути, представлять обоснование стоимости системы ИБ для бизнеса.

В обосновании затрат на ИБ существует два основных подхода [24].

Первый подход, **назовем его наукообразным**, заключается в том, чтобы освоить, а затем и применить на практике необходимый инструментарий измерения уровня ИБ. Для этого необходимо привлечь руководство компании (как ее собственника) к оценке стоимости информационных ресурсов, определению оценки потенциального ущерба от нарушений в области ИБ. От результатов этих оценок будет во многом зависеть дальнейшая деятельность руководителей в области ИБ. Если информация ничего не стоит, существенных угроз для информационных активов компании нет, а потенциальный ущерб минимален (руководство это **подтверждает**), проблемой обеспечения ИБ можно не заниматься. Если информация обладает определенной стоимостью, угрозы и потенциальный ущерб ясны, тогда встает вопрос о внесении в бюджет расходов на подсистему ИБ. В этом случае становится необходимым заручиться поддержкой руководства компании в осознании проблем ИБ и построении корпоративной системы защиты информации.

Второй подход, назовем его практическим, состоит в следующем: можно попытаться найти инвариант разумной стоимости корпоративной системы защиты информации. Ведь существуют

аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер. Например, на рынке автострахования оценка стоимости этой услуги составляет – 5-15% от рыночной стоимости автомобиля в зависимости от локальных условий его эксплуатации, стажа водителя, интенсивности движения, состояния дорог и т.д.

По аналогии, ИБ в компании можно вообще не заниматься, и не исключен такой вариант, что принятый риск себя вполне оправдает. А можно потратить на создание корпоративной системы защиты информации немало денег, и при этом останется некоторая уязвимость, которая рано или поздно приведет к утечке или хищению конфиденциальной информации.

Эксперты-практики в области защиты информации нашли некое оптимальное решение, при котором можно чувствовать себя относительно уверенно – стоимость системы ИБ должна составлять примерно 10-20% от стоимости ИС, в зависимости от конкретных требований к режиму ИБ [24]. Это и есть та самая оценка на основе практического опыта (best practice), которой можно уверенно оперировать, если не производить детальные расчеты.

Этот подход, очевидно, не лишен недостатков. В данном случае, скорее всего, не удастся вовлечь руководство в глубокое осознание проблем ИБ. Но зато можно обосновать объем бюджета на ИБ путем ссылки на понятные большинству владельцев информационных ресурсов общепринятые требования к обеспечению режима информационной безопасности «best practice», формализованные в ряде стандартов, например ISO 1 7799.

Реализация этих подходов (конкретные методы оценки эффективности системы ИБ) на практике зависит от ряда факторов, среди которых основными являются степень зрелости организации и специфика ее деятельности.

Наиболее известной расчетной методикой оценки экономической целесообразности затрат на ИБ предприятии является **методика совокупной стоимости владения** (ССВ), которая была изначально предложена аналитической компанией Gartner Group в конце 80-х годов (1986-1987) для оценки затрат на информационные технологии [24]. Методика Gartner Group позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные

затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т. д.

Данная методика может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она позволяет руководителям служб информационной безопасности обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников службы ИБ. Поскольку оценка экономической эффективности корпоративной системы защиты информации становится «измеримой», появляется возможность оперативно решать задачи контроля и коррекции показателей экономической эффективности и, в частности, показателя ССВ. Таким образом, показатель ССВ можно использовать как инструмент для оптимизации расходов на обеспечение требуемого уровня защищенности КИС и обоснование бюджета на ИБ. При этом в компании эти работы могут выполняться самостоятельно, с привлечением системных интеграторов в области защиты информации или совместно предприятием и интегратором.

В целом методика ССВ компании Gartner Group позволяет:

- Получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации.
- Сравнить подразделения службы ИБ компании как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли.
- Оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ССВ.

Показатель ССВ может использоваться практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и позволяет «навести порядок» в существующих и планируемых затратах на ИБ. С этой точки зрения показатель ССВ дает возможность объективно и независимо обосновать экономическую целесообразность внедрения и использования конкретных организационных и технических мер и средств защиты информации. Для объективности решения также необходимо дополнительно учитывать состояние внешней и внутренней среды предприятия, например, показатели технологического, кадрового и финансового развития

предприятия, так как не всегда наименьший показатель ССВ корпоративной системы защиты информации может быть оптимален для компании.

Сравнение определенного показателя ССВ с аналогичными показателями ССВ по отрасли (с аналогичными компаниями) и с «лучшими в группе» позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто оказывается довольно трудно или даже практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же «родственных»показателей ССВ позволяет убедиться в том, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли. Указанные сравнения можно проводить, используя усредненные показатели ССВ по отрасли, рассчитанные экспертами Gartner Group или собственными экспертами компании с помощью методов математической статистики и обработки наблюдений.

Методика ССВ Gartner Group позволяет ответить на следующие вопросы [24]:

- Какие ресурсы и денежные средства расходуются на ИБ?
- Оптимальны ли затраты на ИБ для бизнеса компании?
- Насколько эффективна работа службы ИБ компании по сравнению с другими?
- Как эффективно управлять инвестированием в защиту информации?
- Какие выбрать направления развития корпоративной системы защиты информации?
- Как обосновать бюджет компании на ИБ?
- Как доказать эффективность существующей корпоративной системы защиты информации и службы ИБ компании в целом?
- Какова оптимальная структура службы ИБ компании?
- Как оценить эффективность нового проекта в области защиты информации?

Основные положения методики

ИБ обеспечивается комплексом мер на всех этапах жизненного цикла ИС, совокупная стоимость владения для системы ИБ в общем случае складывается из стоимости:

- Проектных работ.
- Закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и AAA (средства аутентификации, авторизации и администрирования).
- Затрат на обеспечение физической безопасности.
- Обучения персонала.
- Управления и поддержки системы (администрирование безопасности).
- Аудита ИБ.
- Периодической модернизации системы ИБ.

Под показателем ССВ понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года. ССВ может рассматриваться как ключевой количественный показатель эффективности организации ИБ в компании, так как позволяет не только оценить совокупные затраты на ИБ, но управлять этими затратами для достижения требуемого уровня защищенности КИС.

При этом **прямые затраты** включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей и др., связанные с поддержкой деятельности организации.

В свою очередь, **косвенные затраты** отражают влияние ИС и подсистемы защиты информации на сотрудников компании посредством таких измеримых показателей, как простои и «зависания» корпоративной системы защиты информации и ИС в целом, затраты на операции и поддержку (не относящиеся к прямым затратам).

Методика ССВ позволяет оценить и сравнить состояние защищенности ИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, а именно: «сейчас мы тратим на ИБ столько-то, если будем тратить

столько-то по конкретным направлениям ИБ, то получим такой-то эффект».

В целом определение затрат компании на ИБ подразумевает решение следующих трех задач:

1. Оценка текущего уровня ССВ корпоративной системы защиты информации и КИС в целом.
2. Аудит ИБ компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня ССВ.
3. Формирование целевой модели ССВ.

Рассмотрим каждую из перечисленных задач.

Оценка текущего уровня ССВ. В ходе работ по оценке ССВ проводится сбор информации и расчет показателей ССВ организации по следующим направлениям:

- Существующие компоненты ИС (включая систему защиты информации) и информационные активы предприятия (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства).
- Существующие расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация).
- Существующие расходы на организацию ИБ на предприятии (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработку концепции и политики безопасности и пр.).
- Существующие расходы на организационные меры защиты информации.
- Существующие косвенные расходы на организацию ИБ на предприятии, в частности, обеспечение непрерывности или устойчивости бизнеса.

Аудит ИБ предприятия. По результатам собеседования с TOP-менеджерами предприятия и проведения инструментальных проверок уровня защищенности организации проводится анализ следующих основных аспектов:

- Политики безопасности.
- Организационных вопросов управления подсистемой безопасности.
- Классификации и управления информационными ресурсами.

- Управления персоналом.
- Физической безопасности.
- Администрирования компьютерных систем и сетей.
- Управления доступом к системам.
- Разработки и сопровождения систем.
- Планирования бесперебойной работы организации.
- Проверки системы на соответствие требованиям ИБ.

На основе проведенного анализа выбирается модель ССВ, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

Сравнение текущего показателя ССВ проверяемой компании с модельным значением показателя ССВ позволяет провести анализ эффективности организации ИБ компании, результатом которого является определение «узких» мест в организации, причин их появления и выработка дальнейших шагов по реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности ИС.

Формирование целевой модели ССВ. По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы «лучшей практики», квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку.

При применении экономических методов анализа эффективности инвестиций в ИБ для аргументации принятия тех или иных решений, необходимо проводить оценку дополнительных затрат.

Для примера приведем перечень статей расходов при модернизации корпоративной системы защиты и системы доступа на объекте информатизации. В наиболее общем виде эти расходы можно разделить по следующим статьям.

Расходы на аппаратные средства и программное обеспечение. Эта категория модели ССВ включает серверы, компьютеры клиентов (настольные и мобильные компьютеры), периферийные устройства и сетевые компоненты. Также в эту категорию входят расходы на аппаратно-программные средства ИБ.

Расходы на операции ИС. Прямые затраты на содержание персонала, стоимость работ и аутсорсинг, произведенные компанией в целом, бизнес-подразделениями или ИС службой для осуществления технической поддержки и операций по поддержанию инфраструктуры для пользователей распределенных вычислений.

Административные расходы. Прямые затраты на персонал, обеспечение деятельности и расходы внутренних/внешних поставщиков (вендоров) на поддержку ИС операций, включающих управление, финансирование, приобретение и обучение ИС.

Расходы на операции конечных пользователей. Это затраты на самоподдержку конечных пользователей. Затраты включают: самостоятельную поддержку, официальное обучение конечных пользователей, нерегулярное (неофициальное) обучение, самостоятельные прикладные разработки, поддержку локальной файловой системы.

Расходы на простои. Данная категория учитывает ежегодные потери производительности конечных пользователей от запланированных и незапланированных отключений сетевых ресурсов, включая клиентские компьютеры, совместно используемые серверы, принтеры, прикладные программы, коммуникационные ресурсы и ПО для связи.

При разработке методики оценки затрат на ИБ должны определяться прямые (бюджетные) и косвенные затраты на выполнение мероприятий по ИБ.

Предположим, что руководство компании проводит работы по внедрению на предприятии системы защиты информации (СЗИ). Уже определены объекты и цели защиты, угрозы информационной безопасности и меры по противодействию им, приобретены и установлены необходимые средства защиты информации. Для того, чтобы требуемый уровень защиты ресурсов реально достигался и соответствовал ожиданиям руководства предприятия, необходимо

ответить на следующие основные вопросы, связанные с затратами на информационную безопасность:

- Что такое затраты на информационную безопасность?
- Неизбежны ли затраты на информационную безопасность?
- Какова зависимость между затратами на информационную безопасность и достигаемым уровнем информационной безопасности?
- Представляют ли затраты на информационную безопасность существенную часть от оборота компании?
- Какую пользу можно извлечь из анализа затрат на информационную безопасность?

Рассмотрим возможные ответы на поставленные вопросы [24].

Что такое затраты на информационную безопасность?

Как правило, затраты на информационную безопасность подразделяются на следующие категории:

- Затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты).
- Затраты на контроль, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия.
- Внутренние затраты на ликвидацию последствий нарушения политики информационной безопасности (НПБ) — затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут.
- Внешние затраты на ликвидацию последствий нарушения политики информационной безопасности — компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т. п.
- Затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

При этом обычно выделяют **единовременные** и **систематические** затраты. К единовременным относятся затраты на формирование политики безопасности предприятия: организационные затраты и затраты на приобретение и установку средств защиты.

Классификация затрат условна, так как сбор, классификация и анализ затрат на ИБ – внутренняя деятельность предприятий, и детальная разработка перечня зависят от особенностей конкретной организации. Самое главное при определении затрат на систему безопасности – взаимопонимание и согласие по статьям расходов внутри предприятия. Кроме того, категории затрат должны быть постоянными и не должны дублировать друг друга.

Неизбежны ли затраты на информационную безопасность?

Невозможно полностью исключить затраты на безопасность, однако они могут быть приведены к приемлемому уровню. Некоторые виды затрат на безопасность являются абсолютно необходимыми, а некоторые могут быть существенно уменьшены или исключены. Последние – это те, которые могут исчезнуть при отсутствии нарушений политики безопасности или сократятся, если количество и разрушающее воздействие нарушений уменьшатся.

При соблюдении политики безопасности и проведении профилактики нарушений можно исключить или существенно уменьшить следующие затраты:

- На восстановление системы безопасности до соответствия требованиям политики безопасности.
- Восстановление ресурсов информационной среды предприятия.
- Переделки внутри системы безопасности.
- Юридические споры и выплаты компенсаций.
- Выявление причин нарушения политики безопасности.

Необходимые затраты – это те, которые необходимы даже если уровень угроз безопасности достаточно низкий. Это затраты на поддержание достигнутого уровня защищенности информационной среды предприятия.

Неизбежные затраты могут включать:

- Обслуживание технических средств защиты.
- Конфиденциальное делопроизводство.
- Функционирование и аудит системы безопасности.
- Минимальный уровень проверок и контроля с привлечением специализированных организаций.
- Обучение персонала методам информационной безопасности.

Зависимость между затратами на ИБ и уровнем защищенности ИС.

Сумма всех затрат на повышение уровня защищенности предприятия от угроз информационной безопасности составляет общие затраты на безопасность.

Взаимосвязь между всеми затратами на безопасность, общими затратами на безопасность и уровнем защищенности информационной среды предприятия обычно имеет вид функции (рис. 7.1).

Общие затраты на безопасность складываются из затрат на предупредительные мероприятия, затрат на контроль и восполнение потерь (внешних и внутренних). С изменением уровня защищенности информационной среды изменяются величины составляющих общих затрат и, соответственно, их сумма – общие затраты на безопасность.

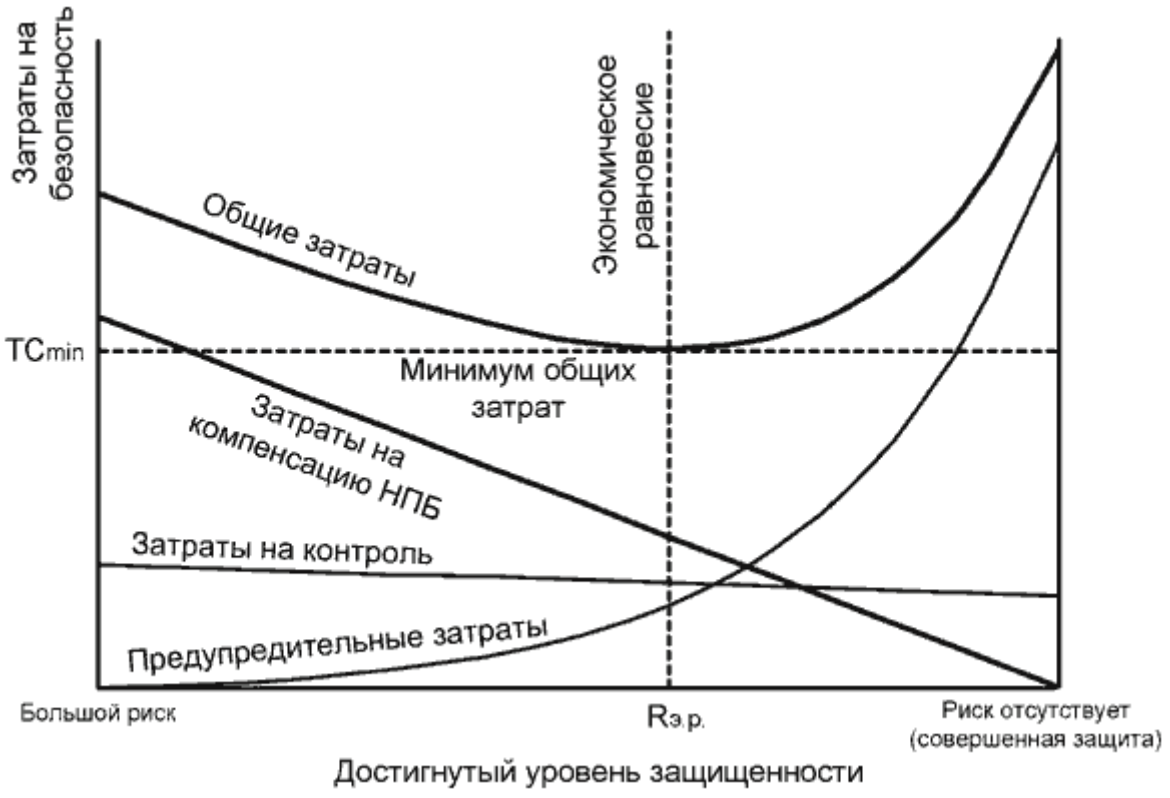

Рис. 7.1. **Взаимосвязь между затратами на безопасность и достигаемым уровнем защищенности**

В примере (рис. 7.1.) показано, что достигаемый уровень защищенности измеряется в категориях «большой риск» и «риск отсутствует» («совершенная защита»). Рассматривая левую сторону

графика («большой риск»), мы видим, что общие затраты на безопасность высоки в основном потому, что высоки потери на компенсацию при нарушениях политики безопасности. Затраты на обслуживание системы безопасности очень малы.

Если мы будем двигаться вправо по графику, то достигаемый уровень защищенности будет увеличиваться (снижение информационного риска). Это происходит за счет увеличения объема предупредительных мероприятий, связанных с обслуживанием системы защиты. Затраты на компенсацию НПБ уменьшаются в результате предупредительных действий. Как показано на графике, на этой стадии затраты на потери падают быстрее, нежели возрастают затраты на предупредительные мероприятия. Как результат – общие затраты на безопасность уменьшаются. Изменения объема затрат на контроль незначительны.

Если двигаться по графику вправо за точку экономического равновесия (т.е. достигаемый уровень защищенности увеличивается) ситуация начинает меняться. Добиваясь устойчивого снижения затрат на компенсацию нарушений политики безопасности, мы видим, что затраты на предупредительные работы резко возрастают и при приближении к зоне «Отсутствия риска» они становятся экономически не оправданными.

Как оценить долю затрат на ИБ в обороте предприятия?

Там, где затраты на обеспечение ИБ должным образом учтены, они могут составлять от 2 % до 20 % и более от объема продаж (оборота). Приведенная оценка получена из опыта работы ряда российских компаний, специализирующихся в области защиты информации на основе анализа состояния защищенности информационной среды предприятий металлургической отрасли и отрасли связи [24].

Контрольные вопросы

1. Какие практические подходы используются при проведении аудита ИБ?

2. Назовите задачи аудита ИБ на предприятии.

3. Что необходимо сделать при подготовке предприятия к проведению аудита ИБ?

4. Какие документы должны подготовить предприятия для внешнего аудита ИБ?

5. Дайте характеристику четырех этапов планирования аудита.

6. Опишите назначение и процедуру составления «Ведомости соответствия».

7. Как организуется работа с руководителями и сотрудниками предприятия до и после проведения аудита ИБ?

8. Охарактеризуйте последовательность (алгоритм) проведения внешнего аудита ИБ компанией.

9. Назовите виды информации (структуру данных), необходимую для проведения аудита.

10. Опишите структуру отчета по результатам аудита ИБ.

11. Какие подходы можно использовать для экономической оценки обеспечения ИБ.

12. Назовите основные виды затрат на создание системы ИБ предприятия?

ЗАКЛЮЧЕНИЕ

Результаты проведения аудита ИБ позволяют:

– выявить значимые угрозы для информации, циркулирующей в пределах предприятия;

– оценить вероятность каждого события, представляющего угрозу для безопасности, и ущерб от него;

– составить неформальную модель нарушителя; определить основные требования к системе защиты;

– оценить с точки зрения этих требований эффективность применяемых организационных мер и инженерно-технических средств защиты;

– разработать предложения и рекомендации по совершенствованию комплексной системы обеспечения безопасности.

На основе полученных результатов аудита ИБ проводится подготовка распорядительных документов, которые создают основу для проведения защитных мероприятий *("Концепция информационной безопасности", "План защиты", "Положение о категорировании ресурсов автоматизированной системы" и некоторые другие),* а также внести *пункты, касающиеся защиты, в должностные инструкции и положения об отделах и подразделениях.* Разработанные документы в зависимости от результатов обследования могут предусматривать решение следующих задач:

– защиту от проникновения в корпоративную сеть и от утечки информации из сети по каналам связи;

– защиту наиболее критичных ресурсов сети от вмешательства в нормальный процесс функционирования;

– защита важных рабочих мест и ресурсов от несанкционированного доступа;

– криптографическую защиту наиболее важных информационных ресурсов.

Результаты проведения аудита безопасности предприятия дают возможность:

1. **Руководителям организаций и предприятий** обеспечить формирование единой политики и концепции безопасности

предприятия; рассчитать, согласовать и обосновать необходимые затраты на защиту предприятия; объективно и независимо оценить текущий уровень информационной безопасности предприятия; обеспечить требуемый уровень безопасности и в целом повысить экономическую эффективность предприятия; эффективно создавать и использовать профили защиты конкретного предприятия на основе неоднократно апробированных и адаптированных качественных и количественных методик оценки информационной безопасности предприятий заказчика.

2. **Начальникам служб автоматизации и информационной безопасности предприятия** – получить оперативную и объективную качественную и количественную оценку состояния информационной безопасности предприятия на всех основных уровнях рассмотрения вопросов безопасности: организационно-управленческом, техноло–гическом и техническом; выработать и обосновать необходимые меры организационного характера (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции действий в нештатных ситуациях); составить экономическое обоснование необходимых инвестиций в защиту информации, обоснованно выбрать те или иные аппаратно-программные средства защиты информации в соответствии с концепцией безопасности, а также на основании требований распоряжений и руководящих документов Гостехкомиссии России, ФАПСИ и отечественных и международных стандартов ISO 17799, 9001, 15408, BSI; адаптировать и использовать в своей работе предложенные количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической составляющей эффективности предприятия.

3. **Системным, сетевым администраторам и администраторам безопасности предприятия** – объективно оценить безопасность всех основных компонентов и сервисов корпоративной информационной системы предприятия заказчика, техническое состояние аппаратно-программных средств защиты информации (межсетевые экраны, маршрутизаторы, хосты, серверы, корпоративные БД и приложения); успешно применять на практике рекомендации, полученные в ходе выполнения аналитического исследования, для

нейтрализации и локализации выявленных уязвимостей аппаратно-программного уровня.

4. **Сотрудникам и работникам предприятий и организаций** – определить основные функциональные отношения и, что особенно важно, зоны ответственности, в том числе финансовой, за надлежащее использование информационных ресурсов и состояние политики безопасности предприятия.

Содержание представленного материала отражает основные виды работ по организации подготовки и проведению аудита ИБ. Одна из главных задач, которая стояла перед автором, наряду с изложением общей теоретической основы, необходимой для подготовки специалистов в области организации и технологии защиты информации, дать необходимые сведения студентам для проведения работ по анализу состояния ИБ предприятий в период прохождения производственных практик и последующего выполнения курсовых проектов и дипломных работ.

Автор выражает надежду, что эти задачи в определенной мере выполнены в предлагаемом учебном пособии.

Глоссарий

Автоматизированная информационная система – информационная система, реализованная с использованием средств вычислительной техники и связи.

Администратор – должностное лицо, управляющее чем-нибудь; ответственный распорядитель.

Администратор безопасности – полномочный представитель (лицо или группа лиц), ответственный за обеспечение безопасности в автоматизированных системах и сетях.

Активное средство защиты – средство, обеспечивающее создание активных помех средствам технической разведки (промышленного шпионажа) или разрушение нормального функционирования этих средств.

Анализ – логическая операция разделения исследуемого предмета, явления, ситуации на составные элементы, расчленения совокупности фактов, относящихся к предмету, на отдельные, обособленные группы. Такая операция облегчает изучение предмета, явления, ситуации, позволяет изучить их более глубоко, выявить закономерности, которые не проявляются при рассмотрении предмета как целого. Анализ – широко распространенный познавательный прием, он необходим для перехода на следующую ступень процесса познания – ступень синтеза.

Анализ риска – процесс определения угроз безопасности системы и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также разработка мер защиты.

Аппаратные средства защиты – механические, электромеханические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации.

Атака – попытка преодоления системы защиты ИС. Степень "успеха" атаки зависит от уязвимости и эффективности системы защиты.

Аттестация – оценка на соответствие определенным требованиям. С точки зрения защиты аттестации подлежат объекты, помещения,

технические средства, программы, алгоритмы на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

Аудит – форма независимого, нейтрального контроля какого-либо направления деятельности коммерческого предприятия.

Безопасность – состояние защищенности жизненно важных интересов личности, предприятия, общества и государства от внутренних и внешних угроз. Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Безопасность информации – защита информации от случайного или преднамеренного доступа лиц, не имеющих на это права, ее получения, раскрытия, модификации или разрушения. Реализация требований и правил по защите информации, поддержанию информационных систем в защищенном состоянии, эксплуатация специальных технических и программно-математических средств защиты и обеспечение организационных и инженерно-технических мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется службами безопасности информации.

Безопасность информационная – это проведение правовых, организационных и инженерно-технических мероприятий при формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов, защите информации высокой значимости и прав субъектов, участвующих в информационной деятельности.

Безопасность информационной сети – меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных.

Безопасность предприятия – стабильно прогнозируемое во времени состояние окружения, в котором предприятие может осуществлять свои действия без нарушения и перерывов.

Безопасность экономическая – обеспечение экономического развития РФ с целью удовлетворения экономических потребностей граждан при оптимальных затратах труда и природоохранном использовании сырьевых ресурсов и окружающей среды.

Вирус компьютерный – небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям. Обычно создается для нарушения работы компьютера различными способами – от "безобидной" выдачи какого-либо сообщения до стирания, разрушения файлов. Выявление "вирусов" и "лечение" инфицированных файлов осуществляется различными методами, в том числе специальными антивирусными программами.

Владелец информации, информационной системы – субъект, в непосредственном ведении которого в соответствии с законом находится информация, информационная система.

Гриф конфиденциальности – специальная отметка на носителе информации, либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставленные на самом носителе и (или) в сопроводительной документации на него. Установлено три степени секретности сведений, составляющих гостайну, и соответствующие грифы секретности: "особой важности", "совершенно секретно" и "секретно".

Данные – сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их проявления, отображенные на материальном носителе, используемые в целях сохранения знаний.

Документ – документированная информация, снабженная определенными реквизитами.

Документооборот – процесс прохождения документов внутри определенной организационной системы с момента их получения или создания до завершения использования или отправки.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну,

а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

Доступ – специальный тип взаимодействия между субъектом и объектом, в результате которого создается поток информации от одного к другому.

Доступ к конфиденциальной информации – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную или коммерческую тайну.

Задания по безопасности – совокупность требований и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта.

Закрытые данные – данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа осуществляется системой разграничения с помощью определенных правил (паролей).

Защита – поддержка дисциплины доступа, исключающая несанкционированное получение информации.

Защита данных – меры сохранения данных от нежелательных последствий, которые неумышленно или преднамеренно ведут к их модификации, раскрытию или разрушению.

Защита информации – совокупность мероприятий, обеспечивающих предупреждение разглашения, утечки и несанкционированного доступа к конфиденциальной информации.

Защищенность – способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению.

Защищенность информации можно рассматривать как с позиций технической защиты от несанкционированного доступа (свойство недоступности), так и социально-психологических по степени конфиденциальности и секретности (свойство конфиденциальности).

Злоумышленник – лицо или организация, заинтересованное в получении возможности несанкционированного доступа к конфиденциальной информации, представляющей промышленную и коммерческую тайну, предпринимающее попытку такого доступа или совершившее его.

Инженерно-техническая защита – совокупность организационных, организационно-технических и технических мероприятий, обеспечивающих защиту информации и физических ценностей.

Инструкция – организационный документ, регламентирующий какую-либо сторону деятельности системы защиты информации (СЗИ), содержащий указания по организации защиты конкретных сведений или действий. Например, инструкция о порядке учета, хранения и выдачи документов с грифом "коммерческая тайна".

Информация – сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их представления, используемые в целях получения знаний, принятия решений.

Информационные ресурсы – документы и массивы документов (библиотеки, архивы, фонды, базы данных, базы знаний), другие формы организации информации по всем направлениям жизнедеятельности общества.

Канал проникновения – физический путь от злоумышленника к источнику конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям.

Канал распространения информации – физический путь от источника конфиденциальной информации к субъекту (субъектам) общения, посредством которого возможно разглашение охраняемых сведений.

К каналам распространения относятся средства информационной коммуникации и массовой информации, такие как связь, почта, конференции, выставки, радио, телевидение, пресса и т.д. и т.п.

Канал утечки информации – неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное овладение злоумышленниками конфиденциальной информацией. Для образования канала утечки необходимы определенные пространственные, временные и энергетические условия и соответствующие средства приема, накопления и обработки информации на стороне злоумышленников.

Класс защищенности средств – определенная совокупность требований по обеспечению безопасности информационного обмена от несанкционированного доступа к информации.

Коммерческая тайна – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью

предприятия, разглашение или утечка которых может нанести ущерб его интересам. Не могут составлять коммерческую тайну учредительные документы и устав; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности; документы о платежеспособности; сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных мест; документы об уплате налогов и обязательных платежей; сведения о загрязнении окружающей среды; сведения об участии должностных лиц предприятий в кооперативах, малых предприятиях, товариществах и т.д.

Комплекс средств защиты – совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения защиты объекта, автоматизированных систем и средств вычислительной техники.

Контроль доступа – предупреждение несанкционированного доступа к защищенным данным.

Концепция защиты информации – система взглядов, требований и условий организации защиты охраняемых сведений от разглашения, утечки и несанкционированного доступа к ним через различные каналы.

Незаконные действия – воровство, умышленный обман, взяточничество, нарушение обязанностей по сохранению секретности информации, электронный или другие виды шпионажа.

Несанкционированный доступ к конфиденциальной информации – это неправомерный преднамеренный доступ к источникам конфиденциальной информации лицами, не имеющими права доступа к ним. Основными способами НСД являются: сотрудничество, выведывание, подслушивание, наблюдение, хищение, копирование, подделка, уничтожение, перехват, фотографирование и др.

Обнаружение – момент, когда наблюдатель (злоумышленник) обнаружил (увидел) интересующий его объект или его отображение на экране технических средств наблюдения и определил его положение на местности (космосе, под водой или на водной поверхности) относительно себя или какого-либо объекта, а также характер его действий. Обнаружение осуществляется визуально или с помощью технических средств: оптических, радиоэлектронных, акустических и др.

Обследование – изучение реальных объектов (помещений, оборудования, технических средств) как возможных источников конфиденциальной информации. В процессе обследования определяются структура, тип объекта (помещение, оборудование, технические средства) на предмет отнесения его к какой-либо группе конфиденциальности, выявляются возможные каналы утечки коммерческих секретов и вырабатываются необходимые защитные мероприятия.

Организационная защита – регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет организационных мероприятий.

Организационно-технические мероприятия – мероприятия, обеспечивающие блокирование возможных каналов утечки информации через технические средства обеспечения производственной и трудовой деятельности с помощью специальных технических средств.

Охраняемая зона – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих на это права.

Политика безопасности – набор законов, правил и практического опыта, на основе которых строится управление, защита и распределение конфиденциальной информации.

Полномочия – право пользователя или уполномоченного им субъекта осуществлять определенные процедуры над охраняемыми сведениями.

Правовая защита информации –специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Правонарушение – противоправное, виновное (умышленное или неосторожное) действие или бездействие, за которое законодательством предусмотрена административная ответственность.

Преступление – общественно-опасное деяние, предусмотренное уголовным законом (действие или бездействие), посягающее на общественный строй государства, его экономическую и политические системы, собственность, личность, политические, трудовые, имущественные и другие права и свободы граждан, а равно иное,

посягающее на правопорядок, общественно опасное деяние, предусмотренное уголовным законом.

Преступление компьютерное – преступление, совершенное средствами вычислительной техники и вычислительных сетей, направленное на незаконное похищение информации или приводящее к ее модификации или разрушению.

Проверка безопасности – независимый просмотр, изучение системных журналов и наблюдение за функционированием с целью определения достаточности средств контроля системы, соответствия принятой методике безопасности и процедурам обработки данных, обнаружения нарушений безопасности, выработки рекомендаций по изменению средств контроля и процедур безопасности.

Программная защита информации – система специальных программ, включаемых в состав программного обеспечения, реализующих функции защиты информации.

Проникновение – успешное преодоление механизмов защиты.

Профиль защиты – независимая от реализации совокупность требований безопасности для некоторой категории объектов, отвечающая специфическим требованиям проекта и потребителя.

Профиль полномочий – полный профиль полномочий соответствующего объекта (субъекта) относительно всех элементов охраняемых сведений.

Разглашение – умышленные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по службе или работе, приведшие к ознакомлению с ними лиц, не допущенных к этим сведениям.

Разграничение доступа – система мероприятий, обеспечивающих предоставление пользователям только той информации, которая необходима им для выполнения работы.

Режим – совокупность правил, мероприятий, норм, обеспечивающих контролируемый доступ на территорию, в помещения, к информации.

Режим конфиденциальности – защищенный законодательством страны порядок обеспечения безопасности носителей конфиденциальной информации.

Ресурс. В широком смысле это все, что представляет ценность с точки зрения организации и является объектом защиты. В узком смысле ресурс – часть информационной системы. В прикладных методах анализа рисков обычно рассматриваться следующие классы ресурсов:

- оборудование (физические ресурсы);
- информационные ресурсы (базы данных, файлы, все виды документации);
- программное обеспечение (системное, прикладное, утилиты, другие вспомогательные программы);
- сервис и поддерживающая инфраструктура (обслуживание СВТ, энергоснабжение, обеспечение климатических параметров и т.п.).

Рубежи защиты информации представляют собой совокупность методов и средств, обеспечивающих многоуровневую, иерархическую систему допуска к информации с помощью различных средств, таких как физические, технические, программные и т.п. Иерархическая последовательность доступа к информации реализуется по принципу "чем выше уровень доступа, тем уже круг допущенных лиц".

Секретность – ограничения, накладываемые автором на доступ к его информации другим лицам. Оформляется присвоением информации определенного грифа и достигается закрытием ее паролем, шифрованием или другими методами.

Система защиты информации – организованная совокупность мероприятий, методов, органов и средств, создаваемых с целью защиты информации. К системе защиты информации предъявляются следующие основные требования:

—защита информации есть непрерывный процесс, заключающийся в систематическом контроле защищенности, выявлении узких и слабых мест в системе защиты, обосновании и реализации наиболее рациональных путей ее совершенствования и развития;

—комплексное использование всего арсенала имеющихся средств защиты;

—надлежащая подготовка пользователей и обслуживающего персонала в соблюдении всех правил сохранности информации;

—учет того, что никакая система защиты не может считаться абсолютно надежной.

Система защиты информации, обладающая по крайней мере одним средством защиты на каждый возможный канал утечки информации, называется системой с полным перекрытием. Такая система обладает оптимальной надежностью.

Система контроля доступа – совокупность мероприятий и технических средств, исключающих неконтролируемое проникновение злоумышленника на охраняемую территорию, помещение. Такие системы могут быть построены на различных принципах: от систем с идентификацией личности по предъявленному документу до систем на базе персональных ЭВМ с использованием в качестве идентификаторов отпечатков пальцев, особенностей голоса, строения сетчатки глаз и т.п.

Система обеспечения безопасности – совокупность средств, методов и мероприятий, создаваемая и поддерживаемая для предупреждения или исключения случайного или преднамеренного доступа, получения, раскрытия, модификации или разрушения ин-, формации.

Система разграничения доступа – совокупность правил, методов и средств, реализующих разграничение доступа к конфиденциальной информации в информационных системах.

Способы действий по защите информации – выявление возможных каналов утечки информации, поиск и обнаружение реальных каналов утечки информации, оценка степени опасности каждого реального канала, локализации (подавление) опасных каналов и контроль надежности защитных мероприятий.

Способы несанкционированного доступа – приемы и порядок действий с целью получения (добывания) охраняемых сведений незаконным путем. К ним в том числе относятся: инициативное сотрудничество (предательство, измена); склонение (принуждение, побуждение) к сотрудничеству (подкуп, шантаж); подслушивание переговоров; незаконное ознакомление; хищение; подделка (модификация); уничтожение (порча, разрушение); незаконное подключение к системам и линиям связи и передачи информации; перехват акустических и электромагнитных сигналов; визуальное наблюдение; фотографирование; сбор и анализ документов, публикаций и промышленных отходов.

Средства защиты информации –технические, криптографические, программные и другие средства, предназначенные

для защиты сведений, составляющих государственную (коммерческую) тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средства защиты от несанкционированного доступа – программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа.

Технические средства защиты – аппаратные (встроенные в аппаратуру) и функционирующие автономно (независимо от аппаратуры) технические средства, обеспечивающие техническую защиту конфиденциальной информации.

Угроза – реально или потенциально возможные действия или условия преднамеренного или случайного (неумышленного) нарушения режима функционирования предприятия путем нанесения материального (прямого или косвенного) ущерба, приводящие к финансовым потерям, включая и упущенную выгоду.

Угроза безопасности активная – угроза намеренного несанкционированного изменения состояния системы.

Управление безопасностью – система регулярных защитных мероприятий, направленных на обеспечение безопасности в соответствии с изменяющимися условиями внутренней и внешней среды.

Управление доступом – способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных и т.п.). Управление доступом включает следующие функции защиты: идентификацию пользователей, персонала и ресурсов; проверку полномочий; разрешение и создание условий работы в пределах установленного регламента; регистрацию (протоколирование) обращения к защищаемой информации; реагирование при попытках несанкционированного действия.

Управление рисками – процесс определения контрмер в соответствии с оценкой рисков.

Уровень безопасности – компоненты иерархической структуры защиты информации, которая состоит из подсистем одного ранга.

Уровень полномочий – максимальный уровень секретности сведений, к которым разрешен доступ соответствующему субъекту (объекту).

Утечка информации – неконтролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

Уязвимость – слабость в средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для проникновения в систему.

Физическая безопасность – реализация физических барьеров и контрольных процедур, как превентивная или контрмера, против физических угроз (взлома, кражи, террористического акта, а также пожара, подтопления и т.д.) ресурсам системы и конфиденциальной информации.

Физические средства защиты информации – технические устройства, инженерные сооружения и организационные мероприятия, затрудняющие или исключающие проникновение потенциальных нарушителей в места, где они могут иметь доступ к защищаемой информации. К ним относятся: физическая изоляция сооружений и помещений, ограждение территории на расстояниях, исключающих эффективную регистрацию электромагнитных излучений аппаратуры; развертывание систем управления доступом у входов в охраняемые помещения; использование специальных запирающих устройств; наблюдение за охраняемыми помещениями и развертывание системы охранной сигнализации.

Экономические преступления – уголовно наказуемые деяния, совершаемые в сфере производства, распределения и потребления товаров и услуг, в том числе связанные с незаконным использованием служебного статуса; хищения, совершаемые путем присвоения, растраты, злоупотребления служебным положением; обман потребителей, нарушение правил торговли; нарушение государственной дисциплины цен, уклонение от уплаты налогов, выпуск или продажа товаров, оказание услуг, не отвечающих требованиям безопасности, и др.

Список использованной и рекомендуемой литературы

1. Аверченков, В.И. Организационная защита информации: учеб. пособие/В.И. Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2005 – 184с.

2. Аверченков, В.И., Служба защиты информации: организация и управление: учеб. пособие / В.И. Аверченков, М.Ю. Рытов – Брянск: БГТУ, 2005 – 186с.

3. Астахов, А. Аудит безопасности информационных систем / А.Астахов // www.networkdoc.ru/it-press/audit-safery.html

4. Галатенко, В.А. Основы информационной безопасности: учеб. пособие/В.А. Галатенко – М: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2004. – 264с.

5. Домарев, В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев – Киев: ООО «ТиД», 2004. – 914с.

6. Линаев, В.В. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств / В.В. Линаев. – 2004. – №3 (130).

7. Мак-Мак, В.П. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности/В.П. Мак-Мак – М.: ИД МБ, 1999. –160 с.

8. Медведовский, И.Д. Практическое применение международного стандарта безопасности информационных систем ISO 17799 www.dsec.ru/cd-courses/iso 17799 cd.php/

9. Медведовский, И.Д. Современные методы и средства анализа и контроля рисков информационных компаний www.daily.sec.ru

10. Петренко, С.А. Аудит безопасности Iuranrt / С.А. Петренко, А.А.Петренко – М: Академии АиТи: ДМК Пресс, 2002. – 438с.

11. Петренко, С.А. Управление информационными рисками. Экономически оправданная безопасность/ С.А. Петренко, С.В. Симонов – М: Академия АиТи: ДМК Пресс, 2004. – 384с.

12. Петренко, С.А. Возможная методика построения системы информационной безопасности предприятия www.bre.ru/security/13985.html/.

13. Покровский, П. Оценка информационных рисков/ П. Покровский – 2004. – №10. Изд-во «Открытые системы» (www.osp.ru).

14. Симонов, С. Анализ рисков, управление рисками www.jefinfo.ru/1999/1/1/article 1.1.1999.html#AEN8.

15. Хованов, В.И. О системном подходе к проблеме страхования информационных рисков//Information Security. – 2004.–№3, (www.itsec.ru).

16. Ярочкин, В.И. Система безопасности фирмы / В.И. Ярочкин – М: «Ось-89», 2003 – 352с.

17. http: // bezpeka.mk.ua/articles/seminar/html/web-4html.

18. http: // www.gammassl.co.uk./topics/hots.html.

19. Астахов, А. Анализ защищенности корпоративных автоматизированных систем / А. Астахов // Jet Info online. – 2002.– №7(10), www.jet.info.ru/2002//article.7.2002

20. Бетелин, В.Б. и др. Профили защиты на основе «Общих критериев» / В.Б. Бетелин, В.А. Галатенко [и др.]// Jet Info on line. – 2003.– №3 (118), 2003/3/1/фкешсду1.3. 2003.

21. Галатенко, А. Активный аудит/ А. Галатенко // Jet Info on line.– 1999.– №8(75). article 1.8. 1999……

22. Гузик, С. Зачем проводить аудит информационных систем? /С. Гузик // Jet Info on line. – 2000. – 10 (89). articlel.10.2000.

23. Кобзарев, М Методология оценки безопасности информационных технологий по общим критериям / М. Кобзарев, А. Сидак // Jet Info on line. – 2004. – 6 (133). article 1.6.2004.

24. Петренко, С Информационная безопасность: Экономические аспекты / С. Петренко, С. Симонов, Р. Кислов // Jet Info on line. – 2003 – №10 (125). article 1.10.2003.

Оглавление

Учебное издание

Аверченков Владимир Иванович

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Подписано в печать 21.11.2011.
Электронное издание для распространения через Интернет.