Внедрение и использование выбранных мер защиты

В этой главе

- *Выбор основных решений по обеспечению ЗИ*
- *Обеспечение ЗИ на стадиях проектирования ИС*
- *Содержание и последовательность работ по защите информации*
- *Построение системы защиты информации*
- *Порядок проведения работ по ЗИ*
- *Реализация организационных мер защиты*
- *Реализация технических мер защиты*
- *Приемка, определение полноты и качества работ*

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

Выбор основных решений по обеспечению ЗИ (600)

Комплекс мер по внедрению СЗИ должен быть рассмотрен на трех уровнях:

- административном (система поддержки руководством организации работ по обеспечению ЗИ);
- организационном (конкретные организационные мероприятия по обеспечению режима ЗИ);
- техническом (реализация механизмов защиты программно-техническими средствами).

Административный уровень обеспечения ЗИ (603)

Должны быть выработаны:

- система поддержки руководством организации мероприятий по обеспечению ЗИ, выполнению правовых и договорных требований в области ЗИ;
- процедура доведения до сведения сотрудников основных положений концепции ЗИ, требования по обучению персонала соответствующим правилам;
- система контроля за реализацией принятых решений и назначение ответственных должностных лиц.

Организационный уровень обеспечения ЗИ (603)

На данном уровне должны быть рассмотрены:

- организационная структура службы, ответственной за обеспечение режима ЗИ, распределение обязанностей;
- комплекс профилактических мер (предупреждение появления вирусов, и неумышленных действий, ведущих к нарушению ЗИ);
- организация доступа сотрудников сторонних организаций к ресурсам ИС;
- организация доступа пользователей и персонала к конкретным ресурсам ИС;
- политика по отношению к отдельным аспектам:
  - удаленный доступ в ИС,
  - использование открытых ресурсов,
  - использование несертифицированного ПО и т.д.

Технический уровень обеспечения ЗИ (604)

Рассматриваются программно-технические средства, реализующие заданные требования.

Если требования сформулированы в терминах функций (сервисов) безопасности, рассматриваются механизмы безопасности и соответствующие им варианты программных и аппаратных реализаций.

Если требования сформулированы по подсистемам ИС, рассматриваются варианты программно-аппаратной реализации этих подсистем.

При рассмотрении вариантов рекомендуется учитывать следующие аспекты:

- управление доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- регистрацию значительных событий в журнале для повседневного контроля или специальных расследований;
- проверку и обеспечение целостности критически важных данных на всех стадиях их обработки;
- защиту конфиденциальных данных от НСД, в том числе использование средств шифрования;
- резервное копирование критически важных данных;
- восстановление работы ИС после отказов, особенно для систем с повышенными требованиями к доступности;
- защиту от внесения несанкционированных дополнений и изменений;
- обеспечение средств контроля, например посредством использования программы для выборочного контроля и альтернативные варианты программного обеспечения для повторения критически важных вычислений.

Обеспечение ЗИ на стадиях проектирования ИС (603)

На стадиях проектирования должны быть разработаны проектные решения, реализующие механизмы ЗИ. Проектные решения описываются в пояснительной записке к техническому проекту.

При этом ***должны быть рассмотрены решения по структуре и функционированию СЗИ:***

- технические решения по структуре системы и подсистем, уровни иерархии и система управления ЗИ;
- технические решения по режимам функционирования и диагностике состояний СЗИ;
- описание показателей, характеризующих качество СЗИ и методы их измерения
- перечень угроз, для которых обеспечивается защита в рамках предлагаемого проектного решения;
- обоснование выбора технических и программных средств защиты, функционирование в составе комплекса технических средств автоматизированной системы, в том числе в пусковом, нормальном и аварийном режимах;

- технические решения по программному обеспечению
- технические решения по информационному обеспечению СЗИ

При подготовке ИС к вводу в действие описываются:

- мероприятия по обучению персонала правилам ЗИ;
- мероприятия по изменению объекта автоматизации, связанные с обеспечением ЗИ;
- планирование восстановительных работ.
- вопросы выявления критически важных функций и систем;
- составление перечня возможных аварий;
- разработка защитных мероприятий;
- подготовка планов действий персонала на случай аварий.

Рабочая документация, относящаяся к СЗИ (601)

На стадии разработки рабочей документации должны быть составлены:

- должностные инструкции персонала, регламентирующие вопросы доступа в помещения и к оборудованию, работу с носителями информации, доступ к информации;
- правила администрирования в ИС,
- правила работы пользователей в ИС,
- правила работы со сторонними организациями,
- план мероприятий по обеспечению режима ЗИ. В этом плане должны быть рассмотрены основные составляющие части комплексной системы защиты:
  - организация работы персонала,
  - физическая защита и контроль СЗИ,
  - организация доступа в многопользовательской системе,
  - поддержание работоспособности и обеспечение СЗИ в сетях,
  - планирование восстановительных работ.

ЗИ в процессе подготовки ИС к эксплуатации (620)

В процессе подготовки ИС к эксплуатации должны быть решены вопросы обучения пользователей и персонала, организации физической защиты и контроля за соблюдением режима, доступа пользователей к ресурсам ИС.

Обучение пользователей по вопросам обеспечения ЗИ

В соответствии с утвержденными планами по обеспечению режима ЗИ, пользователи и обслуживающий персонал должны пройти обучение.

Организация физической защиты и контроль за соблюдением режима ЗИ

В процессе эксплуатации ИС должен быть организован контроль за:

- доступом в помещения,
- сохранением конфиденциальности,
- ведением журналов регистрации событий,
- организацией доступа к носителями информации,
- доступом к документации по ИС.

Организация доступа в многопользовательской системе

При подготовке к эксплуатации должны быть рассмотрены вопросы доступа в ИС:

- регистрация пользователей,
- управление паролями пользователей,
- управление привилегиями,
- пересмотр прав доступа пользователей,
- управление привилегированным доступом для администрирования системы, в том числе системы ЗИ.

ЗИ при эксплуатации ИС (650)

Процесс ЗИ требует постоянного контроля за СЗИ. Основными направлениями являются контроль за работой пользователей, защита целостности данных и программ, управление доступом к приложениям.

Контроль за работой пользователей предусматривает следующие аспекты:

- управление доступом к рабочим местам в ИС,
- контроль за использованием паролей,
- контроль за оборудованием, оставленным без присмотра,
- отслеживание времени простоя терминалов,
- ограничение доступа к сервисам.

В плане защиты целостности данных и программ от вредоносного программного обеспечения администраторы ИС и пользователи должны быть всегда готовы к возможности проникновения вредоносного программного обеспечения в ИС и к принятию мер по обнаружению его внедрения и ликвидации последствий его атак.

Управление доступом к сервисам включает следующие аспекты:

- контроль за соблюдением правил использования электронной почты и электронного документооборота;
- управление доступом к приложениям и сервисам,
- контроль за использованием системных программ,
- изоляция уязвимых мест в защите ИС,
- отслеживание событий, представляющих угрозу ЗИ.

Содержание работ предпроектной стадии (403)

Должны быть сформулированы требования к СЗИ при реализации функций и задач проектируемой ИС:

- условия создания и функционирования системы,
- описание требований в области ЗИ,
- ограничения допустимых затрат на поддержание ЗИ.

Требования формулируются по задачам и функциям в терминах:

- доступности (период недоступности, время доступа, другие показатели, определяемые предметной областью);
- целостности (показатели надежности хранения, доставки);
- конфиденциальности (градации конфиденциальности или гриф секретности).

На этапах изучения ИС как объекта защиты:

- выявляются основные угрозы (классы рисков), которым подвергаются информационные ресурсы,
- фиксируются правовые и договорные требования, которым должна удовлетворять СЗИ.

Разработка концепции ПИБ осуществляется на основе анализа следующих групп факторов:

- правовые и договорные требования,
- требования к СЗИ по функциям и задачам ИС,
- угрозы (классы рисков), которым подвергаются информационные ресурсы.

В результате анализа формулируются общие СЗИ, затрагивающие организацию в целом:

- цели и приоритеты, которые преследует организация в области ЗИ;
- общие направления в достижении этих целей;
- аспекты программы ЗИ, которые должны решаться на уровне организации в целом;
- должностные лица, ответственные за реализацию программы создания СЗИ.

Концепция политики ЗИ должна быть оформлена в виде отчета.

Обучение пользователей и персонала

Пользователи и персонал должны быть обучены соблюдению режима ЗИ, правильному обращению с информационными ресурсами. Они должны знать об угрозах информации и иметь необходимые навыки для работы. Рекомендуется утвердить права и ограничения на доступ пользователям в письменной форме.

Организация физической защиты и контроля за соблюдением режима ЗИ (403)

Контроль доступа в помещения

Контроль доступа в помещения и общие меры по защите оборудования являются составной частью мер по обеспечению ЗИ. Оборудование и критически важные или уязвимые элементы системы должны быть размещены в защищенных областях, ограниченных периметром безопасности, с надлежащим контролем. Для уменьшения риска несанкционированного доступа или повреждения документации и носителей информации рекомендуется задать правила использования рабочего стола.

Обеспечение конфиденциальности

Пользователи информационных ресурсов организации должны подписать обязательство о сохранении конфиденциальности. Особое внимание следует уделить процедуре предоставления доступа к информационным ресурсам пользователям из сторонних организаций. Для этого должны быть разработаны специальные правила.

Журналы регистрации событий

Необходимо подготовить журнал регистрации выполняемых заданий, который будут вести операторы ИС. В этом журнале следует фиксировать:

- время запуска и останова систем;
- системные ошибки, сбои и предпринятые меры.

Обеспечение защиты документации по ИС

Документация по ИС может содержать описание прикладных процессов, структур данных и процессов подтверждения полномочий. В этом случае система должна быть защищена от несанкционированного доступа. Рекомендуются следующие средства контроля:

- список лиц с правом доступа к документации должен быть максимально ограничен, а разрешение на ее использование должно выдаваться владельцем приложения;
- печатные материалы, создаваемые в процессе работы ИС, следует хранить отдельно от прочих документов и распространять на них правила ограничения доступа.

Доступ к носителями информации и их защита

Необходимо организовать контроль доступа к носителям информации и обеспечить их физическую защиту. Для доступа к носителям с конфиденциальной информацией необходимо иметь утвержденные правила. При организации системы доступа следует учитывать следующее:

- система идентификации носителей должна быть такова, чтобы по меткам, используемым для их идентификации, нельзя было определить характер и содержание хранимой информация;
- необходимо своевременно стирать ненужное содержимое повторно используемых носителей информации;
- вынос носителей информации из хранилища необходимо фиксировать в контрольном журнале;
- хранение всех носителей информации в надежном, защищенном месте в соответствии с инструкциями.

Все процедуры и уровни полномочий должны быть задокументированы.

Организация работы персонала (603)

Должностные инструкции персонала (601)

Для персонала, допущенного к работе в ИС, должны существовать должностные инструкции, в которых устанавливаются обязанности и ответственность за обеспечение информационной безопасность в соответствии с принятой политикой.

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 и действий по защите. При разработке инструкций рекомендуется учитывать следующие аспекты.

Работа с носителями информации (604)

Должны быть подготовлены инструкции по работе со всеми носителями конфиденциальных данных: документов, магнитных лент, дисков, отчетов и др. Предлагается рассмотреть:

- правила работы с носителями информации и их маркировку;
- регистрацию получателей данных, имеющих соответствующие полномочия;
- обеспечение полноты входных данных;
- подтверждение получения переданных данных (по необходимости);
- предоставление доступа к данным минимальному числу лиц;
- маркировку всех копий данных для получателя, имеющего соответствующие полномочия;
- своевременное обновление списков получателей с правом доступа к данным.

Уничтожение носителей информации (603)

Должны существовать инструкции по уничтожению носителей информации. Предлагаются следующие рекомендации.

Носители данных, содержащих конфиденциальную информацию, необходимо уничтожать путем сжигания или измельчения (бумажных носителей) или стирать (для магнитных носителей) при повторном использовании.

Для идентификации носителей данных, которые могут потребовать уничтожения, предлагаются специальные идентификаторы.

В некоторых случаях будет проще уничтожать все ненужные носители данных, чем пытаться выделить из них носители, на которых записана конфиденциальная информация.

Каждый случай удаления носителей конфиденциальной информации необходимо (по возможности) регистрировать в контрольном журнале.

При накоплении информации, подлежащей удалению, следует учитывать, что зачастую большое количество несекретной информации содержит более важную информацию, чем малое количество секретной информации.

Администрирование ИС (603)

Администратор ИС должен обеспечивать надежную работу ИС и соответствие требованиям информационной безопасности.

Обязанности администратора ИС и процедуры по администрированию должны быть изложены в должностной инструкции.

Должны быть описаны инструкции по выполнению каждого задания, в том числе:

- допустимые процедуры оперирования с файлами данных;
- требования к планированию выполнения заданий;
- инструкции по обработке ошибок и других исключительных ситуаций, которые могут возникнуть во время выполнения заданий, в том числе ограничения на использование системных утилит;
- обращение за помощью в случае возникновения технических и других проблем, связанных с эксплуатацией ИС;
- порядок получения выходных данных и обеспечение их конфиденциальности, включая процедуры на-

дежного удаления выходной информации в случае сбоев заданий;

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

Должны быть подготовлены инструкции для работ по обслуживанию систем, связанных с администрированием ИС, в том числе процедуры запуска и останова ИС, резервное копирование данных, техническое обслуживание оборудования.

Работа с представителями сторонних организаций (603)

Привлечение представителей сторонних организаций к работе в ИС может привести к дополнительному риску нарушения режима информационной безопасности.

Необходимо заблаговременно выявить такой риск и принять меры по его уменьшению. Следует рассмотреть следующие вопросы:

- выявление особо уязвимых или критически важных приложений, вынос которых за пределы организации нежелателен;
- получение санкции на использование приложений от их владельцев;
- изложение в инструкциях правил работы с представителями сторонних организаций, проверка соблюдения требований информационной безопасности.

Установка и внедрение средств защиты (600)

В большинстве случаев СЗИ устанавливаются на уже реально функционирующую ИС. Так как защищаемая ИС используется для решения важных задач, часто в непрерывном технологическом цикле, ее владельцы и пользователи неодобрительно относятся к любому, даже кратковременному, перерыву в ее работе, необходимому для установки и настройки СЗИ.

Надо знать

Следует учитывать, что с первого раза правильно настроить систему защиты не представляется возможным. Обычно это связано с отсутствием в организации полного детального списка всех аппаратных, программных и информационных ресурсов системы, подлежащих защите, и готового непротиворечивого перечня прав доступа и полномочий каждого пользователя ИС. Поэтому этап внедрения СЗИ обязательно предусматривает первоначальное выявление, последовательное уточнение и соответствующее изменение настроек устанавливаемой СЗИ.

Очевидно, что те же действия администратору безопасности придется неоднократно повторять и на этапе эксплуатации СЗИ при изменениях состава технических средств, программного обеспечения, пользователей и т.д. Такие изменения происходят довольно часто, поэтому средства управления СЗИ должны обеспечивать удобство осуществления необходимых при этом настроек СЗИ.

В том случае, если средства управления СЗИ не приспособлены к этому, а сама СЗИ не обладает достаточной гибкостью, то очень скоро СЗИ становится не помощником, а обузой для всех, и в первую очередь для администраторов безопасности, и в конце концов такая СЗИ обречена на отторжение.

Необходим ряд дополнительных механизмов, облегчающих установку и внедрение СЗИ, а именно:

- специальные механизмы, позволяющие автоматизировать деятельность администратора безопасности по типовой установке и тиражированию значений параметров СЗИ с эталонной станции на все рабочие станции данного типа;
- специальные режимы «мягкого» функционирования СЗИ. Эти режимы позволяют устанавливать СЗИ на ИС в организациях, у которых первоначально отсутствует детальный перечень прав пользователей по доступу к ресурсам. Они позволяют выявлять некорректные настройки средств защиты (и затем корректировать их) без нарушения работоспособности ИС. Помогает «мягкий» режим и при формировании списков программ, разрешенных для запуска конкретным пользователям (при создании замкнутой программной среды), позволяя накапливать в системных журналах необходимые сведения для их корректировки.

В условиях информатизации общества и интенсивного развития информационных технологий сохранение информации, ее целостность, защита от копирования и модификации представляют собой задачи государственной важности и обеспечивают приоритеты государства в политической, военной, экономической и научно-технической областях.

В предыдущих главах рассмотрены различные аспекты проблемы защиты информации в ИС, концептуальные подходы к решению этих проблем, а также различные средства и мероприятия, которые могут быть использованы для создания СЗИ.

Приемы злоупотребления с информацией совершенствовались быстрее, чем средства их предупреждения и пресечения. Проблема приняла характер игровой ситуации, и притом в антагонистической ее постановке. Из теории игр известно, что решение игровых задач заключается не просто в определении некоторого решения, а в формировании стратегии поведения игроков. Из сказанного следует, что ***процесс создания СЗИ — не разовое мероприятие и требует решения целого ряда задач по внедрению выбранных***

мер защиты. Вот некоторые вопросы на которые предстоит ответить прежде чем приступить к реализации выбранных мер защиты.

1. Каков приоритет объектов ИС, требующих защиты?
2. Как будет влиять реализация программы защиты на планы по развитию информационной системы?
3. Какие дополнительные ресурсы ИС потребуются для СЗИ?
4. Кто несет ответственность за согласование и реализацию проекта создания СЗИ?

Основные проблемы, требующие решения на этом этапе таковы:

- Предотвращение конфликтов из-за ресурсов ИС.
- Сложность разработки плана реализации мер по ЗИ.
- Необходимость предотвращения конфликтов на почве ограничений при развитии информационных систем.

Содержание и последовательность работ по защите информации (600)

Защита информации в компьютерных системах это многоаспектная задача, требующая системного подхода к оценке угроз информации и комплексного использования всего арсенала средств защиты информации.

Надо знать

Работы по созданию систем защиты информации, как и любых других сложных систем, выполняются в три этапа: подготовительные работы, основные работы и заключительные работы. Назначение и общее содержание названных этапов – общепринятое: на предварительном этапе изучаются и оцениваются все факторы, влияющие на защиту информации, принимается и осуществляется принципиальное проектирование системы защиты; на этапе основных работ проектные решения реализуются в ИС, а на заключительном – осуществляется оценка системы защиты, причем как по критериям эффективности, так и по технико-экономическим показателям.

Общее содержание и последовательность работ, выполняемых в процессе создания систем защиты информации, представлено в табл. 22.1.

В таблице приняты следующие обозначения:

СЗ — система защиты;

ВР — высшее руководство (руководители того ранга, который уполномочен принимать решения на разработку СЗ);

ПР — принятие решений;

РР — руководитель разработки всей СЗ;

П — планирование;

ИО — инспекционный отдел (подразделение, уполномоченное производить инспекционный контроль проводимых работ);

ОП — отдел подготовки персонала;

Р — реализация;

К — контроль;

ОЗ — отдел защиты (подразделение, непосредственно отвечающее за защиту информации в ИС);

ГУ — группа управления (подразделение, осуществляющее руководство всеми разработками);

РП — руководитель проекта СЗ.

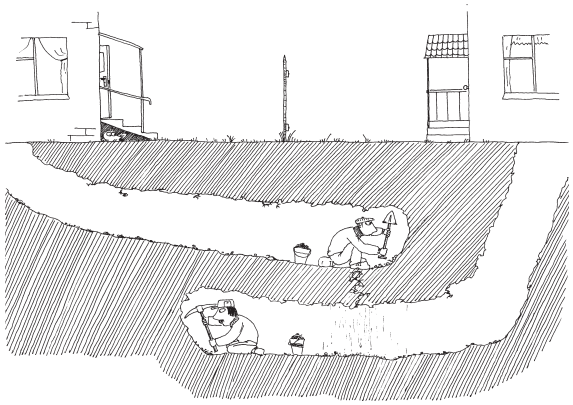
Этапы выполнения работ по созданию СЗИ (600)

Процесс создания системы защиты информации целесообразно разделить на три основных этапа: подготовительный, проектирования и разработки СЗИ, проведения испытаний и сдачи в эксплуатацию СЗИ.

Подготовительный этап (600)

Основные работы подготовительного этапа таковы:

- классификация информации, обрабатываемой в ИС (определение перечня секретных и конфиденциальных сведений, подлежащих защите, вида представления информации, места ее хранения, технологии обработки и передачи и т.п.);
- классификация и описание компонент ИС (СВТ, средств связи и коммуникаций, помещений, ПО, данных, обслуживающего персонала и пользователей и т.п.), участвующих в процессе обработки информации;
- разработка информационной модели, т.е. описание (формальное или неформальное) информационных потоков ИС, а также интерфейса между пользователем и ИС;



Выбранные меры защиты требуют длительного и трудоемкого внедрения...

Таблица 22.1. Содержание работ.

Содержание работ (событий)	Тип работы	Ответственный	Исполнитель
Предварительный этап			
1.Принятие решения о предварительном исследовании проблем, связанных с созданием СЗ	ПР	ВР	
2.Определение основных обязанностей	П	ВР	
3.Назначение РР	ПР	ВР	
4.Определение основных направлений разработки СЗ	П	РР	
5.Подготовка РР и персонала ИО по теоретическим и практическим вопросам в области защиты информации	Р	ВР	ОП
6.Информация подразделений организации о целях СЗ и о начале работ	Р	РР	ОП
7.Определение целей проекта и объектов защиты (ЭВМ, базы данных и т.п.)	Р	РР	отделы-исполнители
8.Определение внешних и внутренних требований к СЗ. Определение политики организации в вопросах защиты	Р	РР, ВР	ИО
9.Исследование и составление документов по организации защиты внутри организации	Р	РР	
10.Исследование и составление документов о реализуемых мерах защиты.	Р	РР	ОЗ
11.Определение, какие гарантии (страхование) существуют и какие нужны	Р	РР	ИО
12.Изучение аварийных мер и планов восстановления внутри организации	Р	РР	
13.Дополнительная подготовка РР (путем визитов, курсов, семинаров и т.п.)	Р	РР	ОП
14.Определение, какие информационные системы разрабатываются или планируются	Р	РР	
15.Выработка основных предложений для общей системы защиты, включая информацию и подготовку персонала.	Р	РР	
16.Определение и описание областей защиты	Р	РР	
17.Определение основных направлений разработки СЗ. Оценка необходимых капиталовложений.	П	РР	ИО
18.Проверка выработанных предложений в ИО	К	РР	ИО
19.Выработка общих предложений по политике в области СЗ.	Р	ВР	РР
20. Выработка общих предложений по созданию руководств и справочников по СЗ	Р	РР	ОЗ
21.Информация ВР о состоянии СЗ, о намечаемых планах продолжения работы, о намечаемых целях	Р	РР	
22.Принятия решения, будет ли продолжаться работа по созданию СЗ. Назначение руководителя и набор персонала ОП.	ПР	ВР	
Этап основных разработок			
1.Создание плана разработки СЗ	П	РР	
2.Создание ГУ разработкой	Р	РР	
3.Определение основных направлений разработки СЗ. Назначение РП и подбор персонала	П	ГУ	
4.Подготовка РП и персонала по вопросам теории и практики СЗ	Р	РР	ОП
5.Информация всех заинтересованных подразделений о начале разработки СЗ	Р	ГУ	РП
6.Изучение требований к подготовке всех сотрудников, которые будут связаны с СЗ	П	РП	ОП
7.Разработка плана работ и грубая оценка их стоимости	П	РП	ИО
8.Представление результатов в ГУ	Р	РП	
9.Принятие решения о продолжении работ, оценки материальных возможностей организации	ПР	ГУ	
10.Составление плана подготовки и распространение информации о нем в подразделениях	П	РП	

Таблица 22.1. Содержание работ (продолжение).

Содержание работ (событий)	Тип работы	Ответственный	Исполнитель
11.Пересмотр плана действий с учетом решения о продолжении работ	К	РП	
12.Определение, оценка характеристик и описание информационных сетей	Р	РП, ОЗ	ИО
13.Определение наиболее важных задач, выполняемых информационными сетями	Р	РП, ОЗ	ИО
14.Изучение возможных угроз	Р	РП, ОЗ	ИО
15.Описание областей, не охваченных исследованием	Р	РП	
16.Представление результатов в ГУ	Р	РП	
17.Принятие решения о продолжении работ	ПР	ГУ	
18.Пересмотр плана действий и плана подготовки персонала	Р	РП	ОП
19.Расчет возможных потерь	Р	РП	ИО
20.Представление результатов в (в том числе и оценка затрат)	Р	РП	
21.Принятие решения о продолжении работ	ПР	ГУ	
22.Проверка, соблюдаются ли все требования законов в области защиты	К	РП	ИО
23.Разработка мер против непредумышленных нарушений и угроз	Р	РП	ОЗ
24.Проверка, не нужно ли изменить или дополнить идентификацию, оценку и классификацию информационных сетей для отражения умышленных угроз	Р	РП	ИО
25.Проверка,не нужно ли изменить список и оценку наиболее важных задач	Р	РП	ИО
26.Проведение анализа внешних угроз	Р	РП, ИО	ОЗ
27.Идентификация и описание любых областей, неохваченных исследованием	Р	РП	
28.Распределение приоритетов между проблемами	Р	РП	ИО
29.Представление результатов в ГУ	Р	РП	
30.Принятие решения о продолжении работ	ПР	ГУ	
31.Пересмотр плана работ и плана подготовки	К	РП	ОП
32.Проверка, соблюдаются ли все требования законов в области защиты	К	РП	ИО
33.Разработка мероприятий по отражению преднамеренных угроз	Р	РП	ОЗ
34.Составление списка разработанных мероприятий	Р	РП	
35.Оценка необходимых ресурсов и затрат на создание СЗ	П	РП	
36.Проведение проверки совместно с ИО	К	РП	ИО
37.Представление результатов в ГУ	Р	РП	ИО
38.Определение направления и целей дальнейшей работы	П	ГУ	
39.Сбор предложений о свойствах СЗ	П	ГУ	все подразделения
40.Сбор предложений о распределении персональной ответственности	П	Начальники подразделений	
41.Представление проекта и предложений по проведению организационных мероприятий ВР	Р	ГУ	
42.Принятие решения о продолжении работ и о распределении ответственности	ПР	ВР	
43.Распространение информации о предложенных мероприятиях по защите по всем подразделениям организации	Р	РП	ОП
44.Распределение персональной ответственности	К	Начальники подразделений	
45.Пересмотр плана работ и плана подготовки	П	РП	
46.Составление планов проверки СЗ	П	ИО	
47.Разработка и испытания разработанных по назначению мероприятий	П	По назначению	
48.Проведение подготовки всего персонала, связанного с работой СЗ	Р	РР	
49.Реализация мероприятий по защите по назначению	Р	По назначению	

Таблица 22.1. Содержание работ (окончание).

Содержание работ (событий)	Тип работы	Ответственный	Исполнитель
50.Проверка правильности функционирования реализованных мероприятий по защите	К	РП	ИО
51.Проверка, все ли поставленные задачи решены. Проведение расчета финансовых затрат	К	ИО	РП
52.Описание опыта эксплуатации СЗ	К	РП	
53.Представление окончательных результатов в ГУ	Р	РП	
54. Составление плана работ по завершению реализации СЗ и представление предложений по продолжению разработки мероприятий по усовершенствованию СЗ	П	ГУ	
55.Представление результатов по усовершенствованию СЗ	Р	ГУ	
56.Принятие решения о прекращении работ по ее усовершенствованию	ПР	ВР	

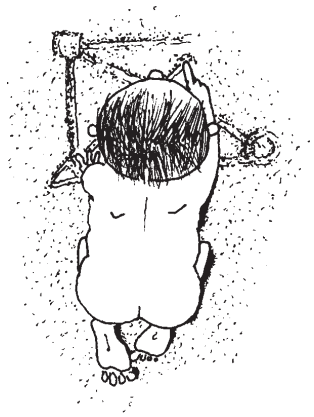
- определение перечня угроз и возможных каналов утечки информации;
- экспертная оценка величины ожидаемых потерь в случае осуществления угрозы;
- обоснование необходимости проведения спецпроверок и специсследований СВТ и других технических средств, а также специального оборудования помещений;
- определение требований к метрологическому обеспечению работ;
- определение перечня разрабатываемых макетов и технологических стендов;
- определение критериев выбора методов и средств защиты;
- выбор методов и средств реализации конкретных механизмов защиты;
- оценка стоимости и эффективности выбранных средств;
- принятие окончательного решения о составе СЗИ.

По результатам подготовительного этапа можно уточнять требования к СЗИ в целом либо к отдельным ее подсистемам.

Проектирование (600)

В перечень работ этапа проектирования и разработки СЗИ включаются работы по выбору и модернизации штатных средств защиты используемых ПО, и аппаратуры, архитектуры СВТ, стандартных интерфейсов и протоколов обмена, а также — по разработке дополнительных ПО и аппаратной части средств защиты.

Испытания и сдача в эксплуатацию (600)



Подготовительный этап определяет успех всего дела...

Этап испытаний и сдачи в эксплуатацию СЗИ состоит из работ, связанных с обеспечением организации и проведения испытаний, включая, при необходимости, разработку специальной аппаратуры, ПО и соответствующей документации.

Все сроки проведения основных работ каждого этапа отражаются в календарном плане.

Для каждого вида испытаний (предварительных, государственных, сертификационных и др.) системы (подсистемы, компонента) защиты исполнитель разрабатывает ***"Программу и методику испытаний системы (подсистемы, компонента) защиты информации в ИС"***, которая утверждается в установленном порядке. Сроки представления проекта Программы, его рассмотрения и утверждения следует согласовать с заказчиком.

Для проведения испытаний заказчиком назначается комиссия, состав которой согласовывается с разработчиком СЗИ.

Испытания проводятся с использованием условной информации (несекретной).

Для проведения испытаний необходима нормативная, методическая и другая документация, программ-

РИСУНОК 22.1. *Цикл работ по ЗИ.*

ные и технические средства, метрологическое, специальное и другое оборудование, создание иных условий; сторона, его предоставляющая, порядок устранения замечаний и т.п.

На стадии завершения испытаний (этапа испытаний) представляются документы: акт приемки, сертификат (аттестат) соответствия классу защищенности, предписание на эксплуатацию и т.п.

Процесс создания механизмов защиты ИС (600)

Специалисты представляют себе процесс создания механизмов защиты информации как реализацию программы различных мероприятий. ***Перечень и содержание этих мероприятий*** выглядят так:

1. Установление необходимой степени защиты информации.

2. Назначение лица, ответственного за выполнение мероприятий по защите информации.

3. Определение возможных причин (каналов) утечки информации.

4. Выделение необходимых средств на защиту информации.

5. Выделение лиц (подразделений), которым поручается разработка механизмов защиты.

6. Установление мер контроля и ответственности за соблюдение всех правил защиты информации.

По мере того, как становилось ясно, что проблема защиты не может быть эффективно решена чисто формальными средствами и в форме разового мероприятия, начали существенно меняться и подходы к организации механизмов защиты. Для повышения эффективности функционирования механизмов защиты был предложен ряд мер организационного характера, направленных как на обеспечение физической целостности информации, так и на предотвращение несанкционированного доступа к ней. По мере того как росло число зарегистрированных преступлений, связанных с информацией в ИС, увеличилось число и разнообразие мероприятий, рекомендованных для повышения эффективности защиты.

Построение системы защиты информации (600)

Как известно, цель ЗИ — предотвращение утечки или нарушения целостности информации. Эта цель может быть достигнута построением системы защиты информации, которая представляет собой организованную совокупность методов и средств обеспечения ЗИ (рис. 22.1).

Защита информации осуществляется поэтапно:

1 — определение и анализ угроз;

2 — разработка системы защиты информации;

3 — реализация плана защиты информации;

4 — контроль функционирования и управление системой защиты информации.

1 этап: Определение и анализ угроз (600)

На этом этапе необходимо осуществить анализ объектов ЗИ, ситуационного плана, условий функционирования предприятия, учреждения, организации, оценить вероятность проявления угроз и ожидаемый ущерб от их реализации, подготовить исходные данные для построения частной модели угроз.

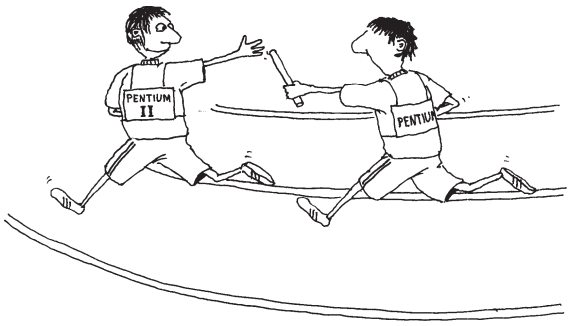
Угрозы могут осуществляться:

- по техническим каналам, включающим каналы побочных электромагнитных излучений и наводок, акустические, оптические, радио-, радиотехнические, химические и другие каналы;
- по каналам специального воздействия путем формирования полей и сигналов в целях разрушения системы защиты или нарушения целостности информации;
- несанкционированным доступом в результате подключения к аппаратуре и линиям связи, маскировки под зарегистрированного пользователя, преодоления мер защиты для использования информации или навязывания ложной информации, применения закладных устройств и программ и внедрения компьютерных вирусов.

Описание угроз и схематическое представление путей их осуществления составляют частную модель угроз.

2 этап: Разработка системы защиты информации (600)

На этом этапе следует осуществить разработку плана ЗИ, включающего организационные, первичные и основные технические меры защиты информации, определить зоны безопасности информации.



Защита информации осуществляется поэтапно...

Организационные меры регламентируют порядок информационной деятельности с учетом норм и требований по ЗИ для всех периодов жизненного цикла объекта ЗИ.

Технические меры предусматривают защиту информации блокированием угроз с использованием технических средств обеспечения ЗИ.

Меры защиты информации должны:

- быть адекватны угрозам;
- быть разработаны с учетом возможного ущерба от их реализации и стоимости защитных мер и вносимых ими ограничений;
- обеспечивать заданную эффективность защиты информации в течение периода ограничения доступа к ней.

Уровень защиты информации определяется системой количественных и качественных показателей, обеспечивающих решение задачи защиты информации на основе норм и требований по ЗИ.

Минимально необходимый уровень защиты информации обеспечивается ограничительными и фрагментарными мерами противодействия наиболее опасной угрозе.

Повышение уровня защиты информации достигается наращиванием технических мер противодействия множеству угроз.

3 этап: Реализация плана защиты информации (600)

На третьем этапе следует реализовать организационные и основные технические меры защиты информации, установить необходимые зоны безопасности информации, провести аттестацию технических средств обеспечения информационной деятельности, технических средств защиты информации, рабочих мест (помещений) на соответствие требованиям по безопасности информации.

Техническая защита информации обеспечивается применением защищенных программ и технических средств обеспечения информационной деятельности, программных и технических средств защиты информации контроля эффективности защиты, а также применением специальных инженерно-технических сооружений, средств и систем.

Средства ЗИ могут функционировать автономно или совместно с техническими средствами обеспечения информационной деятельности в виде отдельных устройств или встроенных в них составных элементов.

Состав средств обеспечения ЗИ, перечень их поставщиков, а также услуг по установке, монтажу, наладке и обслуживанию определяются лицами, которые вла-

деют, пользуются и распоряжаются информацией самостоятельно или по рекомендациям специалистов по ЗИ в соответствии с нормативными документами системы ЗИ.

Предоставление услуг по ЗИ, аттестацию и обслуживание средств обеспечения ЗИ могут осуществлять юридические и физические лица, имеющие соответствующую лицензию.

4 этап: Контроль функционирования и управление системой защиты информации (650)

На заключительном этапе следует провести анализ функционирования системы защиты информации, проверку выполнения мер ЗИ, контроль эффективности защиты, подготовить и выдать исходные данные для управления системой защиты информации.

Управление системой защиты информации заключается в адаптации мер ЗИ к текущей задаче. По фактам изменения условий осуществления или выявления новых угроз меры ЗИ реализуются в кратчайший срок.

В случае необходимости повышения уровня защиты информации необходимо выполнить работы по модернизации системы защиты информации.

Нормативные документы системы СЗИ (600)

Нормативные документы должны обеспечивать:

- проведение единой технической политики;
- создание и развитие единой терминологической системы;
- функционирование многоуровневых систем защиты информации на основе взаимоувязанных положений, правил, методик, требований и норм;
- функционирование систем сертификации, лицензирования и аттестации согласно требованиям безопасности информации;
- развитие сферы услуг в области ЗИ;
- установление порядка разработки, изготовления, эксплуатации средств обеспечения ЗИ и специальной контрольно-измерительной аппаратуры;
- организацию проектирования строительных работ в части обеспечения ЗИ;
- подготовку и переподготовку кадров в системе ЗИ.

Нормативные документы системы ЗИ подразделяются на:

- нормативные документы по стандартизации в области ЗИ;
- государственные стандарты или приравненные к ним нормативные документы;
- нормативные акты межведомственного значения;
- нормативные документы ведомственного значения.

Порядок проведения работ по ЗИ (600)

Уязвимость информации определяется степенью подверженности ее воздействию угроз.

Защищенность информации определяется способностью СЗИ противостоять воздействию угроз.

Содержание и последовательность работ по противодействию угрозам или их нейтрализации должны соответствовать этапам функционирования системы защиты информации и заключаться в следующих процессах:

- проведении обследования предприятия, учреждения, организации (далее — предприятие);
- разработке и реализации организационных и технических мер с использованием средств обеспечения ЗИ;
- приемке работ по ЗИ;
- аттестации средств (систем) обеспечения информационной деятельности на соответствие требованиям нормативных документов по ЗИ.

Порядок проведения работ по ЗИ или отдельных их этапов устанавливается приказом (распоряжением) руководителя предприятия. Работы могут выполняться силами предприятия под руководством специалистов по ЗИ. Для участия в мероприятиях по оказанию методической помощи, оценки полноты и качества реализации мер защиты можно привлекать специалистов по ЗИ из других организаций, имеющих соответствующую лицензию.

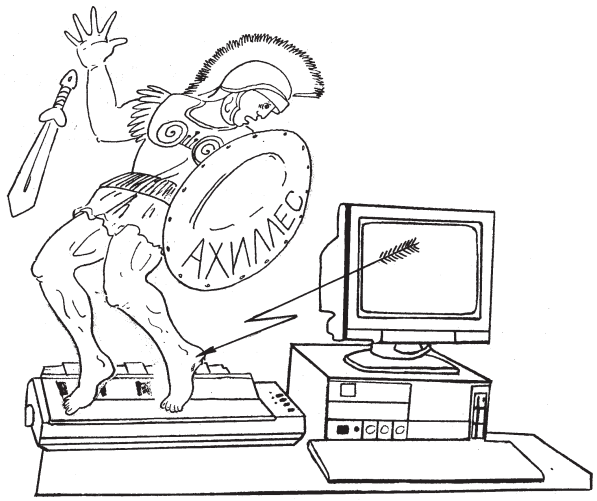
Организация проведения обследования (640)

Целью обследования предприятия есть изучение его информационных потоков, определение объектов защиты информации, выявление угроз, их анализ и построение частной модели угроз.

Обследование должно быть проведено комиссией, состав которой определяется ответственным за ЗИ лицом и утверждается приказом руководителя предприятия.

В ходе обследования необходимо:

- провести анализ условий функционирования предприятия, его расположения на местности (ситуационного плана) для определения возможных источников угроз;
- исследовать средства ИС, имеющие выход за пределы контролируемой территории;
- изучить схемы средств и систем жизнеобеспечения предприятия (электропитания, заземления, автоматизации, пожарной и охранной сигнализации), а также инженерных коммуникаций и металлоконструкций;



Модель угроз разрабатывается на основе материалов обследования...

- исследовать информационные потоки, технологические процессы передачи, получения, использования, распространения и хранения (далее — обработка) информации и провести необходимые измерения;
- определить наличие и техническое состояние средств обеспечения ЗИ;
- проверить наличие на предприятии нормативных документов, обеспечивающих функционирование системы защиты информации, организацию проектирования строительных работ с учетом требований по ЗИ, а также нормативной и эксплуатационной документации;
- выявить наличие транзитных, незадействованных (воздушных, настенных, наружных и заложенных в канализацию) кабелей, цепей и проводов;
- определить технические средства и системы, применение которых не обосновано служебной или производственной необходимостью и которые подлежат демонтажу;
- определить технические средства, требующие переоборудования и установки средств ЗИ.

По результатам обследования необходимо составить акт, который должен быть утвержден руководителем предприятия.

Материалы обследования используются при разработке **модели угроз**, которая должна учитывать:

- генеральный и ситуационный планы предприятия, схемы расположения оборудования ИС, а также инженерных коммуникаций, выходящих за пределы контролируемой территории;
- схемы и описания каналов утечки информации, каналов специального воздействия и путей несанкционированного доступа к информации ;
- оценку предполагаемого ущерба от реализации угроз.

Организация разработки системы защиты информации (600)

На основании материалов обследования и частной модели угроз необходимо определить главные задачи защиты информации и составить техническое задание (ТЗ) на разработку системы защиты информации.

ТЗ должно содержать основные разделы:

- требования к системе защиты информации;
- требования к составу проектной и эксплуатационной документации;
- этапы выполнения работ;
- порядок внесения изменений и дополнений к разделам ТЗ;
- требования к порядку проведения испытаний системы защиты.

Основой функционирования системы защиты информации является **план ЗИ**, который должен состоять из следующих документов:

- перечень распорядительных, организационно-методических, нормативных документов по ЗИ и указания по их применению;
- инструкции о порядке реализации организационных, первичных технических и основных технических мер защиты;
- инструкции, устанавливающие обязанности, права и ответственность персонала;
- календарный план ЗИ.

ТЗ и план ЗИ разрабатывают специалисты по ЗИ, согласуют с заинтересованными подразделениями (организациями). Утверждает их руководитель предприятия.

Реализация организационных мер защиты (600)

Организационные меры защиты информации — комплекс административных и ограничительных мер, направленных на оперативное решение задач защиты путем регламентации деятельности персонала и порядка функционирования средств (систем) обеспечения ИД и средств (систем) обеспечения ЗИ.

Определение

В процессе разработки и реализации организационных мер необходимо:

- определить частные задачи защиты информации;
- обосновать структуру и технологию функционирования системы защиты информации;
- разработать и внедрить правила реализации мер ЗИ;
- определить и установить права и обязанности подразделений и лиц, участвующих в обработке информации;
- приобрести средства обеспечения ЗИ и нормативные документы, обеспечить ими предприятие;
- установить порядок внедрения защищенных средств обработки информации, программных, технических и контролирующих средств;
- установить порядок контроля функционирования системы защиты информации и ее качественных характеристик;
- определить зоны безопасности информации;
- установить порядок проведения аттестации системы технической защиты информации, и ее элементов, разработать программы аттестационных испытаний;
- обеспечить управление системой защиты информации.

Оперативное решение задач ЗИ достигается организацией **управления системой защиты информации,** для чего необходимо:

- изучать и анализировать технологию прохождения информации в процессе ИД;
- оценивать подверженность информации воздействию угроз в конкретный момент;
- оценивать ожидаемую эффективность применения средств обеспечения ЗИ;
- определять (при необходимости) дополнительную потребность в средствах обеспечения ЗИ;
- осуществлять сбор, обработку и регистрацию данных, относящихся к ЗИ;
- разрабатывать и реализовывать предложения по корректировке плана ЗИ в целом или отдельных его элементов.

Реализация технических мер защиты (640)

Для реализации первичных технических мер защиты требуется обеспечить:

- блокирование каналов утечки информации и несанкционированного доступа к ее носителям;
- проверку исправности и работоспособность технических средств ИС;
- установить средства выявления и индикации угроз, проверить их работоспособность;
- установить защищенные средства обработки информации, средства ЗИ и проверить их работоспособность;
- применить программные средства защиты в средствах вычислительной техники, автоматизированных системах, осуществить их функциональное тестирование и тестирование на соответствие требованиям защищенности;
- использовать специальные инженерно-технические сооружения и средства (системы).

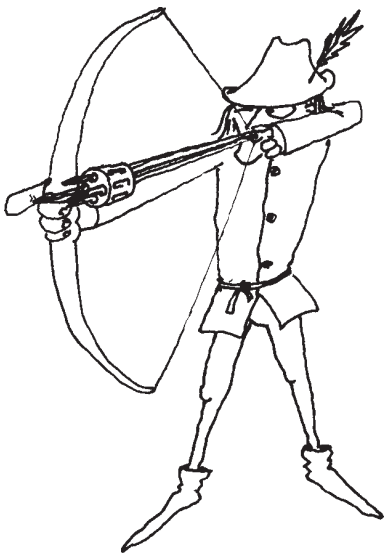
Выбор средств обеспечения ЗИ обусловлен фрагментарным или комплексным способом защиты информации.

Фрагментарная защита обеспечивает противодействие определенной угрозе.

Комплексная защита обеспечивает одновременное противодействие множеству угроз.

Блокирование каналов утечки информации может осуществляться:

- демонтажем технических средств, линий связи, сигнализации и управления, энергетических сетей, использование которых не связано с жизнеобеспечением предприятия и обработкой информации;
- удалением отдельных элементов технических средств, представляющих собой среду распространения полей и сигналов, из помещений, где циркулирует информация;
- временным отключением технических средств, не участвующих в обработке информации, от линий связи, сигнализации, управления и энергетических сетей;



Реализация технических мер защиты...

- применением способов и схемных решений по защите информации, не нарушающих основные технические характеристики средств обеспечения ИД.

Блокирование несанкционированного доступа к информации или ее носителям может осуществляться:

- созданием условий работы в пределах установленного регламента;
- исключением возможности использования не прошедших проверку (испытания) программных, программно-аппаратных средств.

Проверку исправности и работоспособности технических средств и систем обеспечения ИД необходимо проводить в соответствии с эксплуатационными документами.

Выявленные неисправные блоки и элементы могут способствовать утечке или нарушению целостности информации и подлежат немедленной замене (демонтажу).

Средства выявления и индикации угроз применяются для сигнализации и оповещения владельца (пользователя, распорядителя) информации об утечке информации или нарушении ее целостности.

Средства ЗИ применяются для пассивного или активного скрытия информации.

Для пассивного скрытия применяются фильтры-ограничители, линейные фильтры, специальные абонентские устройства защиты и электромагнитные экраны.

Для активного скрытия применяются узкополосные и широкополосные генераторы линейного и пространственного зашумления.

Программные средства применяются для обеспечения:

- идентификации и аутентификации пользователей, персонала и ресурсов системы обработки информации;
- разграничения доступа пользователей к информации, средствам вычислительной техники и техническим средствам автоматизированных систем;
- целостности информации и конфигурации автоматизированных систем;
- регистрации и учета действий пользователей;
- маскирования обрабатываемой информации;
- реагирования (сигнализации, отключения, приостановки работ, отказа в запросе) на попытки несанкционированных действий.

Специальные инженерно-технические сооружения, средства и системы применяются для оптического, акустического, электромагнитного и другого экранирования носителей информации. К ним относятся специально оборудованные светопроницаемые, технологические и санитарно-технические проемы, а также специальные камеры, перекрытия, навесы, каналы и т.п.

Размещение, монтаж и прокладку специальных инженерно-технических средств и систем, в том числе систем заземления и электропитания средств обеспечения ИД, следует осуществлять в соответствии с требованиями нормативных документов по ЗИ.

Технические характеристики, порядок применения и проверки средств обеспечения ЗИ приводятся в соответствующей эксплуатационной документации.

Приемка, определение полноты и качества работ (640)

По результатам выполнения рекомендаций акта обследования и реализации мер защиты информации следует составить в произвольной форме акт приемки работ по ЗИ, который должен быть подписан исполнителем работ, лицом, ответственным за ЗИ, и утвержден руководителем предприятия. При необходимости акт приемки работ может быть согласован с заинтересованными организациями.

Для определения полноты и качества работ по ЗИ следует провести аттестацию.

Аттестация выполняется организациями, имеющими лицензии на право деятельности в области ЗИ. Объектами аттестации являются компоненты ИС и их отдельные элементы, в которых циркулирует информация, подлежащая технической защите.

В ходе аттестации требуется:

- установить соответствие аттестуемого объекта требованиям ЗИ;
- оценить качество и надежность мер защиты информации;
- оценить полноту и достаточность технической документации для объекта аттестации;
- определить необходимость внесения изменений и дополнений в организационно-распорядительные документы.

Порядок аттестации устанавливается соответствующими нормативными документами.

Резюме

В условиях информатизации общества и интенсивного развития информационных технологий сохранение информации, и ее целостности, защита от копирования и модификации являются задачами государственной важности и обеспечивают приоритеты государства в политической, военной, экономической и научно-технической областях.

Защита информации в компьютерных системах это — многоаспектная задача, требующая системного подхода к оценке угроз информации, и комплексное использование всего арсенала средств защиты информации.

Работы по созданию систем защиты информации, как и любых других сложных систем, выполняются в три этапа: подготовительные, основные и заключительные работы.

Специалисты представляют себе процесс создания механизмов защиты информации как реализацию программы различных мероприятий. Перечень и содержание этих мероприятий выглядят следующим образом:

1. Установление необходимой степени защиты информации.

2. Назначение лица, ответственного за выполнение мероприятий по защите информации.

3. Определение возможных причин (каналов) утечки информации.

4. Выделение необходимых средств на защиту информации.

5. Выделение лиц (подразделений), которым поручается разработка механизмов защиты.

6. Установление мер контроля и ответственности за соблюдение всех правил защиты информации.

Для повышения эффективности функционирования механизмов защиты необходимы меры организационного характера, направленные как на обеспечение физической целостности информации, так и на предотвращение несанкционированного доступа к ней.

Для определения полноты и качества работ по ЗИ следует провести аттестацию. Она выполняется организациями, которые имеют лицензии на право деятельности в области ЗИ. Объектами аттестации являются компоненты ИС и их отдельные элементы, в которых циркулирует информация, подлежащая технической защите.

В ходе аттестации требуется:

- установить соответствие аттестуемого объекта требованиям ЗИ;
- оценить качество и надежность мер защиты информации;
- оценить полноту и достаточность технической документации для объекта аттестации;
- определить необходимость внесения изменений и дополнений в организационно-распорядительные документы.