1.3. Концепция построения системы информационной безопасности

Несмотря на большое количество публикаций по рассматриваемой проблеме [20], к сожалению, до настоящего времени отсутствует единный подход к разработке концепции системы информационной безопасности (СИБ) АИС. Сложившееся положение в данном вопросе имеет множество объясняющихся причин, среди которых основными являются следующие:

а) не отработана единная методология построения системы информационной безопасности АИС;

б) отсутствует комплексный анализ потенциальных угроз и степени риска при реализации программных злоупотреблений, и,

в) отсутствует единый подход к определению уровня защищенности АИС.

В основу исследования выделенных причин и задач построения СИБ могут быть заложены работы [139,65,98,10,7,37,38,79,92,102, 101,58, 113,127,40,23 и др.].

В свете изложенного остановимся более подробно на существующие подходы к концепции построения рассматриваемой системы безопасности АИС.

Так, в работе [65] авторы выделяют четыре этапа ее построения: 1) определение необходимого набора функций защиты для каждой спецификации; 2) выбор соответствующих мероприятий для каждого набора функций защиты; 3) выбор и/или разработка средств защиты, наиболее полно удовлетворяющих установленным требованиям; 4) объединение разработанных или выбранных средств защиты в подчиненную общему управлению систему.

Анализируя данный подход следует отметить, что он ориентирован на обеспечение безопасности локального компонента АИС и реализацию механизмов противостояния угрозам конкретной направленности. При

этом, не предусматривается анализ риска и определение эффективности используемых средств защиты информации.

Автор [98] исследует задачи обеспечения информационной безопасности АИС на этапах проектирования и эксплуатации и выделяет:

а) на этапе проектирования: определение перечня и стоимости данных, подлежащих защите; анализ системы как объекта защиты и определение модели поведения потенциального нарушителя, возможных каналов несанкционированного доступа к информации и возможных воздействий случайного характера; разработка средств защиты, перекрывающих выявленные каналы несанкционированного доступа и обеспечивающих заданный уровень безопасности информации; разработка средств функционального контроля системы централизованного управления безопасностью; оценка уровня ожидаемой эффективности защиты;

б) на этапе эксплуатации: контроль и поддержка функционирования системы безопасности информации в компьютерной системе; своевременное предупреждение, обнаружение и блокировка наиболее вероятных угроз с наибольшими материальными и экономическими потерями; регистрация и учет обращений к защищаемой информации, документирование, ведение статистики и прогнозирование наиболее вероятных угроз.

В [10] концепция защиты сформулирована в виде последовательности этапов технологической цепочки:

1. Анализ объекта и выделение элементов, требующих обеспечения их безопасности.

2. Определение возможных угроз выделенным элементам, оценка вероятности их появления и формирование перечня требований по защите.

3. Выбор и разработка адекватных угрозам мер и средств защиты элементов и формирование системы защиты компьютерных систем.

Авторы [139] рассматривают концепцию безопасности, предназначенную для разработки системы обеспечения безопасности информации на предприятиях военной конверсии. В рамках данной концепции рассматриваются следующие этапы: постановка задачи обеспечения безопасности информации (ОБИ) на конверсируемом предприятии; создание на предприятии рабочей группы ОБИ; анализ финансовых и ресурсных ограничений на создание ОБИ; определение общей концепции ОБИ на предприятии; выявление каналов утечки информации и определение защищаемых объектов АИС; разработка и утверждение системы критериев оценки эффективности средств ОБИ; разработка методов и средств ОБИ; анализ степени риска; разработка процедур обнаружения попыток несанкционированного доступа и обработки событий; разработка вариантов проекта СОБИ применительно к конкретному предприятию; анализ проекта по критерию “эффективность/стоимость” и утверждение; реализация СОБИ, тестирование и разработка документации; сертификация СОБИ; ввод СОБИ в эксплуатацию; развитие СОБИ при модификации используемых ИТ.

Следует отметить, что приведенный авторами подход ориентирован на создание системы обеспечения информационной безопасности на конверсируемом предприятии и предполагается, что АИС уже существует, что видоизменяет проблему.

Авторы [92] рассматривают стадии создания системы защиты информации в следующей последовательности:

1. Предпроектная стадия: анализ состава и содержания конфиденциальной информации, определение ее ценности; описание объекта защиты, его элементов: рабочих мест, помещений, зданий, территории, средств обработки инфорамции, связи, сигнализации, имеющихся средств защиты информации. Измерение характеристик элементов объекта защиты.

2. Стадия технического предложения / задания (ТЗ): формулировка целей системы защиты информации конкретной АИС, требований и ограничений.

3. Эскизного / технического проекта.

4. Рабочего проекта.

5. Испытаний.

6. Эксплуатации.

При разработке ТЗ на комплексную защиту АИС решаются вопросы, связанные с требованиями защищенности объектов. При этом, осуществляются научно-исследовательские и опытно-конструкторсике работы (НИОКР), в рамках которых проводятся специальные исследования, результаты которых находит свое отражение в техническом задании.

Типовые вопросы, рассматриваемые в рамках НИР по оценке защищенности объектов ЭВТ и разработке мер по их защите, следующие:

1. Оценка степени соответствия условий объекта требованиям регламентирующих документов по защите объектов от возможной утечки обрабатываемой средствами ЭВТ (СВТ) информации за счет перехвата побочных электромагнитных излучений и наводок (ПЭМИН);

2. Оценка спецсвойств (размеры зон 1 и 2, уровней инфорамтивных сигналов в отходящих проводах и кабелях) СВТ, устанавливаемых на объекте (проведение выборочных специальных исследований СВТ - не менее 3-4 экземпляров СВТ каждого типа);

3. Измерение реального затухания сигналов в токопроводящих коммуникациях, имеющих выход за пределы охраняемой территории объекта;

4. Разработка вариантов защиты объекта с указанием полной стоимости предлагаемых мер защиты;

5. Выбор и согласование с Заказчиком окончательного варианта защиты;

6. Исследование надежности системы защиты. Расчет периодичности контроля защищенности объекта.

Типовые вопросы, решаемые в рамках ОКР по построению защиты объектов ЭВТ, следующие: проведение индивидуальной защиты СВТ (доработка) до уровня защищенности, соответствующего выбранному на этапе НИР варианту защиты; проведение специальных исследований доработанных СВТ и выдача предписаний на их эксплуатацию; построение объектной системы защиты согласно выбранному варианту; проведение контроля объектной системы защиты; разработка предписания на эксплуатацию объекта.

Следует отметить, что данный подход ориентирован, в первую очередь, на покрытие, технических каналов утечки информации, в частности, за счет перехвата ПЭМИН. При этом, основной акцент ставится на обеспечение конфиденциальности информации, что в большей степени соответствует СИБ государственных АИС. Для коммерческих же АИС реализация таких СИБ является экономически нецелесообразной из-за большой стоимости соответствующего оборудования и других видов обеспечения.

Другим важным моментом является и то, что в коммерческих АИС на первом месте стоит вопрос об обеспечении целостности данных, что меняет концепцию выбора механизмов и средств обеспечения информационной безопасности.

Авторы [101] рассматривают концепцию обеспечения безопасности информационных технологий с выделением следующих видов работ: анализ уязвимых элементов объекта; анализ возможных угроз; оценка риска; выбор необходимых функций защиты; определение методов реализации функций защиты; определение средств защиты и системы защиты; поддержка безопасности на заданном уровне.

В рамках данного подхода из поля зрения выпадают вопросы, связанные с экономическими аспектами информационной безопасности,

которые для коммерческих АИС являются весьма важными и должны рассматриваться в первую очередь.

В [102] предлагаются следующие этапы построения комплексной системы защиты информации, реализуемые в следующей последовательности:

1. Проведение предварительного обследования состояния объекта и организации защиты информации. Определение факторов, анализ условий и осуществление выбора и обоснования требований по защите информации на заданном объекте.

2. Определение функций защиты, обеспечивающих требуемый уровень в потенциально возможных условиях функционирвоания объекта.

3. Определение потенциально возможных угроз информации и вероятностей их появления.

4. Обоснование перечня задач защиты информации, их классификации и эффективности их реализации с точки зрения предотвращения возможных сбоев АИС.

5. Определение эффективности защиты информации с помощью оценки степени ее защищенности. Сравнение полученных результатов с требуемыми и анализ стоимостных затрат на обеспечение защиты.

6. Корректировка, уточнения, изменение защиты.

7. Обоснование структуры и технологии функционирования комплексной системы защиты информации. Определение состава технического, математического, программного, информационного и лингвистического обеспечения, нормативно-методических документов и организационо-технических мероприятий по защите информации.

8. Определение технико-экономических оценок разработанного проекта. На этом этапе оцениваются: надежность всех компонентов комплексной системы защиты информации и надежность выполнения функций защиты; живучесть системы защиты, экономическая оценка комплексной системы защиты информации.

9. Отработка организационно-правовых и нормативно-методических вопросов защиты информации, разработка правил выполнения процедур и мероприятий по защите информации, определение прав и обязанностей подразделений и лиц, участвующих в работе комплексной системы защиты информации. Установление правил и порядка контроля работы системы защиты.

10. Внедрение.

Автор [57] рассматривает методологию построения безопасных процессов обработки информации и предлагает следующие этапы:

1. Определение организационно-штатной единицы, которая отвечает за безопасность, ее технические и оперативные возможности, место в системе обработки информации.

2. Формирование понятия “безопасности”.

3. Определение зон доверия и недоверия с позиций сформулированного понятия “безопасность”.

4. Проверка совместимости технических и оперативных возможностей администратора безопасности с определенными зонами доверия и недоверия. При этом должны быть даны ответы на следующие вопросы: достаточны ли средства, выделеные администратору для выполнения поставленных задач; будет ли обеспечиваться безопасность информации при условии, что она передается через зону недоверия; соответствуют ли характеристики технических средств и организационно-методические характеристики администратора ситуациям, которые могут возникнуть в результате воздействия на информацию.

5. В случае несовместимости проверяются возможности корректировки состава технических средств и оперативных возможностей оператора, корректировки понятия “безопасность” в пределах возможного, переопределение зон доверия и недоверия.

Представленная методология ориентирована на обеспечение безопасности отдельных процессов. Для комплексного обеспечения

информационной безопасности АИС необходимо разработать комплексный подход.

Б.И. Скородумов анализирует зарубежную практику разработки и реализации планов безопасности и выделяет следующие разделы [127, с. 23-24]:

- политика безопасности;
- текущее состояние автоматизированной системы;
- реализация системы безопасности;
- организационные положения и мероприятия;
- внедрение и сервисное обслуживание средств защиты;
- развитие и уточнение плана.

В работе [113] рассматриваются четыре этапа разработки системы защиты информации:

1. Проведение аналитического обследования АИС. Осуществляется с целью оценки возможной уязвимости обрабатываемой в ней конфиденциальной информации и выработки необходимых требований по ее защите.

2. Проектирование системы защиты информации. В процессе проектирования на основании установленных требований по защите информации от несанкционированного доступа и побочных электромагнитных излучений и наводок с учетом условий работы АИС и заданных собственником (владельцем) информации ограничений на финансовые, материальные, трудовые и другие ресурсы осуществляется набор или/и разработка конкретных методов и средств защиты. Результатом данного этапа является законченный комплекс сертифицированных средств и методов защиты информации, имеющий соответствующую необходимую проектную и эксплуатационную документацию.

3. Приемка системы защиты в эксплуатацию. На данном этапе осуществляется внедрение средств и методов системы защиты информации в АИС, их комплексная проверка и тестирование,

необходимое обучение и освоение персоналом. Устраняются выявленные в процессе проверки и тестирования недостатки. Результатом этого этапа является общая аттестация системы защиты информации.

4. Эксплуатация системы защиты информации. В процессе эксплуатации АИС проводится регулярный контроль эффективности, при необходимости осуществляется доработка в условиях изменения состава программно-аппаратных средств, оперативной обстановки и окружения АИС. Контролируются и анализируются изменения состава АИС и систем защиты информации. Отклоняются все модификации АИС, снижающие установленную эффективность защиты информации. Периодически проводится контроль на соответствие нормативно-техническим требованиям.

Наибольшая детализация и проработка концепции системы защиты информации характерна для работ В.А. Герасименко [34,36,38,40 и др.]. Например, в работах [34,38 и др.], предлагается унифицированная концепция защиты информации в автоматизированных системах обработки данных (АСОД).

В рамках данного подхода рассматривается взаимодействие следующих компонентов: концепция построения и эксплуатации АСОД; методология структурированного описания АСОД; система показателей уязвимости (защищенности) информации; система дестабилизирующих факторов; методология определения показателей уязвимости; методология определения требований к защите; система концептуальных решений, с выделением функций защиты, задач защиты, средств защиты, системы защиты; требования к концептуальным решениям; система условий, способствущих повышению эффективности защиты.

Одним из подходов к формированию концепции СИБ может служить метод “OPSEC” (Operation Security) [79], включающий несколько этапов.

На первом этапе данного метода проводится анализ объекта защиты с выделением следующих направлений: установление состава

информации нуждаеющкйся в защите; определение наиболее важных элементов (критические) защищаемой информации; срок жизни критической информации (время, необходимое конкуренту для реализации добытой информации); ключевых элементов информации (индикаторов), отражающих характер охраняемых сведений; проведение классификации индикаторов по функциональным зонам (производственно-технологические процессы, система материально-технического обеспечения, подразделения управления и т.д.).

Второй этап метода предполагает “выявление угроз” в следующей последовательности: определяется, кого может заинтересовать защищаемая информация; оцениваются методы, используемые конкурентами для получения этой информации; оцениваются вероятные каналы утечки информации; разрабатывается система мероприятий по пересечению действий конкурента.

В рамках третьего этапа анализируется эффективность принятых и постоянно действующих подсистем обеспечения безопасности, в том числе таких, как физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.

На основании проведенных аналитических исследований предыдущих трех этапов определяют необходимые меры защиты, что составляет содержание работ четвертого этапа.

На пятом этапе рассматриваются представленные предположения по всем необходимым мерам безопасности, определяются стоимость и эффективность.

Шестой этап предусматривает реализацию принятых дополнительных мер безопасности с учетом установления приоритетов.

Заключительный (седьмой) этап сводится к осуществлению контроля и доведению до персонала реализуемых мер безопасности.

В качестве основы для построения концепции СИБ следует рассматривать, прежде всего, преднамеренные угрозы -

несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами и самими системами.

Построение концепции СИБ требует разработки специальной методологии, позволяющей не ограничиваться простым выбором технических и организационных решений, а концентрировать внимание разработчиков и пользователей на таких составляющих, как правовое, организационно-техническое и технологическое обеспечение.

В основу системы информационной безопасности должны быть положены цели, определенные в законодельческих актах государства, как например, в законое “Об информации, информатизации и защите информации” [140]:

- предотвращение утечки, хищения, искажения, подделки;
- обеспечение безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
- защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны и конфиденциальности информации.

По нашему мнению, данный закон не полностью охватывает вопросы использования информационных ресурсов. Такой вывод сделан на основании того, что под его действие не попадают вопросы защиты недокументированной информации. Другим важным моментом является незаконное использование вычислительных ресурсов и т.п.

В работе [106] основные цели информационной безопасности сформулированы и сводятся к двум моментам:

- обеспечение целостности компьютерной информации как в виде данных (пассивная часть), так и программ, обеспечивающих их обработку (активная часть);
- обеспечение конфиденциальности критической информации состоящей из данных, программ их обработки и защиты.

Как видно, подход преследует только цели системы защиты данных АИС, в связи с чем, его важно дополнить таким компонентом, как *обеспечение доступности авторизированных пользователей* ко всем составным частям ИР.

По нашему мнению, в [115] определяется главная цель защиты информации - обеспечение ее конфиденциальности и устойчивости к интелектуальным “диверсионным” воздействиям в процессе передачи, обработки и хранения.

Изложенное дает основание утверждать, что рассмотренные до сих пор подходы не исчерпывают все определения целей СИБ, а их широкий состав, что обусловлено характером их многоуровневой структуры, которые могут быть разделены [111,145] (рис. 4): на первом уровне - обеспечение безопасности информационных ресурсов конкретных АИС, обусловленные физической и логической целостностью и доступностью; на втором уровне - обеспечение технологической и организационной целостности АИС, объектов управления и их парнеров; на третьем (последнем) уровне - информационная безопасность общества и государства. При проектировании системы безопасности информации в качестве основных необходимо принимать цели первого и второго уровней.

Рис. 4. *Иерархическая структура целей информационной безопасности.*

Для достижения рассмотренных целей должны решаться следующие задачи [2 и др.]:

- защита элементов вычислительной среды, с обеспечением целостности данных, процедур обработки, секретности информации;

- контроль элементов операционной среды (ОСр) (внешних компонентов ОСр; целостности внутренних ее компонентов; семантики данных;

- защита элементов вычислительной среды, за счет обеспечения целостности и конфиденциальности критических данных; хранимых программ их обработки и защиты;

- контроль элементов ОСр, (задача контроля целостности и семантики: программ - внешних и внутренних компонентов; используемых данных);

- регламентирование производства, потребления и распространения информации и компонентов информационных и коммуникационных технологий.

В основу проектирования и функционирования систем безопасности информации должны быть положены следующие основные принципы [38,65,10,7,37]:

- принцип *законности* - заключается в соответствии принимаемых мер законодательству о защите информации, а при отсутствии соответствующих законов - другим государственным нормативным документом по ее защите;

- принцип *комплексности* - с позиций предотвращения разноплановых угроз и используемых методов. Имеется ввиду полнота защиты по соответствующему методу и по перечню угроз; а также взаимовлияние методов и средств защиты;

- принцип *минимальной достаточности* состоит в использовании набора средств, обеспечивающих выполнение комплекса установленных требований по защите информации при заданной степени риска ее нарушения. При этом необходима увязка функционирования различных средств защиты по месту и времени, хранения и преобразования информации;

- принцип *обоснованности.* Под названным принципом подразумевается наличие достаточных доказательств актуальности выдвинутых требований или оценка риска нарушения защиты информации;

- принцип *тактической организации защиты* - предусматривает *необходимость упреждающих действий* в виде методов предотвращения, а не ограничения последствий (исключение метода “первой атаки”); *саморегулируемость сложности защиты*, состоящая в ее структурированности, позволяющей использовать более простые методы для оперативного контроля и наращивания ресурсов при возникновении угрозы для ее максимального отражения; *автотестируемость*, предусматривающая осуществление контроля правильности функционирования системы защиты; возможность самообучения, подразумевая ее адаптацию; степень моделируемости ситуаций, то есть

система защиты должна строится по технологии исскусственного интелекта (база знаний, машина вывода, подсистема советчик);

- принцип *непрерывности* состояний во времени и пространстве, предполагающий невозможность функционирования объекта при исключении защиты (необходимость резервирования систем защиты).

По нашему мнению к рассмотренным принципам, следует добавить принцип *восстановления нормальной работы*, предполагающий обеспечение восстановление нормальной работы АИС в случае реализации угрозы.

Анализ приведенных подходов позволяет сделать несколько основных выводов, состоящих в следующем:

1. Обеспечение безопасности информации должно проводится системно и комплексно на всех этапах проектирования, внедрения и эксплуатации АИС.

2. Система обеспечения безопасности информации функционально должна перекрывать все существующие угрозы безопасности информации в АИС.

3. Система обеспечения безопасности информации в АИС должна быть ориентирована на тактическое опережение возможных угроз.

4. В системе безопасности АИС должны быть разработаны механизмы восстановления нормальной работы АИС в случае реализации угроз.

Исходя из результатов анализа существующих подходов и приведенных выводов считаем необходимым предложить общую схему построения системы безопасности информации АИС, которая включает пять последовательных этапов (рис.5):

- подготовительный;
- аналитический;
- исследовательский;
- рекомендательный;
- этап внедрения.

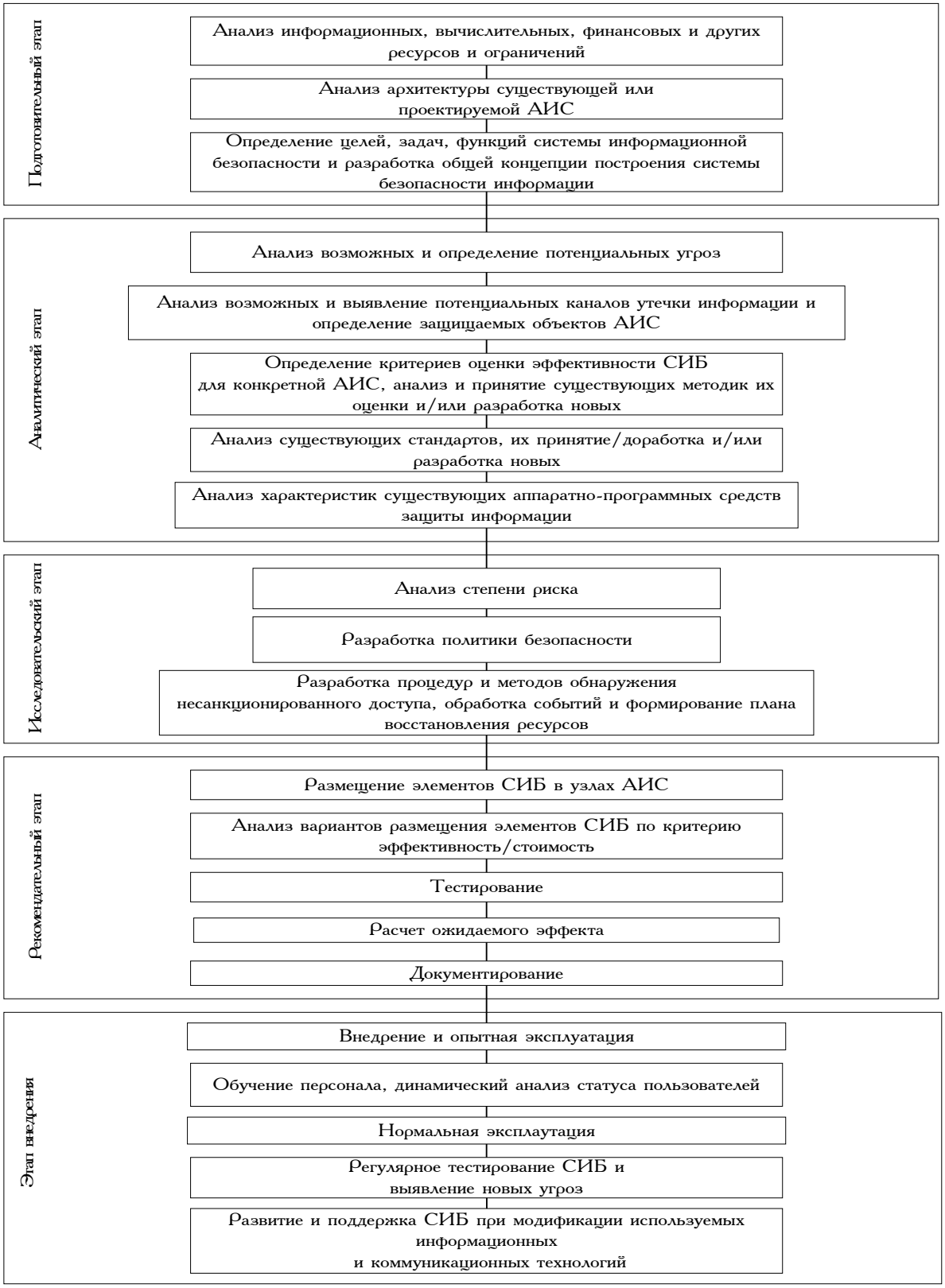

Рис. 5. *Общая схема построения системы информационной безопасности*

На **подготовительном** этапе выбираются и обосновываются объект (АИС в целом, отдельные компоненты, подсистемы), цели и задачи, общая концепция системы безопасности.

Основной задачей **аналитического** этапа является сбор, систематизация и обработка информации о потенциальных угрозах, каналах утечки информации, а также разработка эталонов и критериев эффективности защиты информации, рассмотрение характеристик существующих аппаратно-программных средств защиты.

На **исследовательском** этапе определяется политика безопасности, допустимая степень риска, набор процедур и методов исключения несанкционированного доступа к ресурсам АИС.

Содержание **рекомендательного** этапа заключается в дальнейшей проработке вариантов размещения элементов системы информационной безопасности АИС, выбор оптимального по критерию “эффективность-стоимость”, документирование, оформление окончательных рекомендаций к внедрению.

Этап **внедрения** включает работы по обучению персонала, дальнейшее развитие и поддержку составных частей системы информационной безопасности, а также регулярное тестирование.

Рассмотрим подробнее содержание приведенных этапов.

Подготовительный. На данном этапе проводят системный анализ ресурсов и ограничений, методов подготовки, приема-передачи и обработки информации, особенностей архитектуры АИС и содержащейся в ней информации. Одновременно с этим дается описание ресурсов системы, которые объединяют в следующие категории: вычислительная и коммуникационная техника; программное обеспечение; данные; персонал; дополнительные ресурсы.

На основании проведенного анализа разрабатывается общая концепция СИБ, определяются цели, формируются основные требования, учитывающие не только текущие потребности, но и перспективу развития АИС в целом, а также технологий обработки, хранения и передачи данных.

Аналитический этап. Выявляются возможные угрозы системе, с выделением потенциальных. Определяются каналы несанкционированного доступа и утечки информации, и выделяют категории объектов, подлежащих защите. При этом следует рассматривать не только каналы утечки информации, обусловленные свойствами технических средств и несовершенством программного обеспечения, но и возможностью осуществления несанкционированного доступа и реализации программных злоупотреблений. Такой подход к выявлению потенциальных каналов несанкционированного доступа и утечки информации определяется необходимостью комплексного решения проблемы защиты информации, включая борьбу с промышленным шпионажем.

При анализе возможных и потенциальных угроз основное внимание должно уделяться степени полноты и достоверности информации, поступающей из внешней среды (рис. 6). Это связано с необходимостью разработки комплекса перспективных мероприятий, основной целью которого является углубление тематики исследований, распределение ресурсов, подготовка методического обеспечения и кадров, мониторинг программно-технических средств и т.д.

Проверка степени достоверности сведений о новых угрозах включает оценку источников информации и оценку достоверности фактографической информации. Оценка источников предполагает фиксацию и анализ сообщений, нашедших отражение в:

- периодических изданиях (специализированные газеты и журналы);
- высказываниях лидеров научных направлений (материалы научных и практических конференций, “круглых столов”, презентаций и др.);
- публикациях ведущих научных центров по основным проблемам и перспективам;
- сообщениях электронной почты;

- нетрадиционных источниках информации.

Во внимание принимаются также сообщения о конфликтах, сбоях и задержках, отмеченных в АИС (внутренняя статистика).

В ходе анализа и синтеза поступившей информации определяется ее достоверность (низкая или удовлетворительная) с использованием широкого спектра формальных и экспертных методов. Последние реализуются на основе разнообразного состава операций по обработке информации: концентрация, фильтрация (выделение), классификация, ранжирование, систематизация и др. При наличии достоверной информации формируется комплекс оценочных показателей (например, статистические, прогнозные и т.д.) и разрабатывается комплекс мероприятий.

В случае оценки возможности перехода возможных угроз в потенциальные представляется необходимым развить, представленный в [1] подход анализа оценки привлекательности реализации конкретной угрозы (или класса угроз) для потенциального нарушителя.

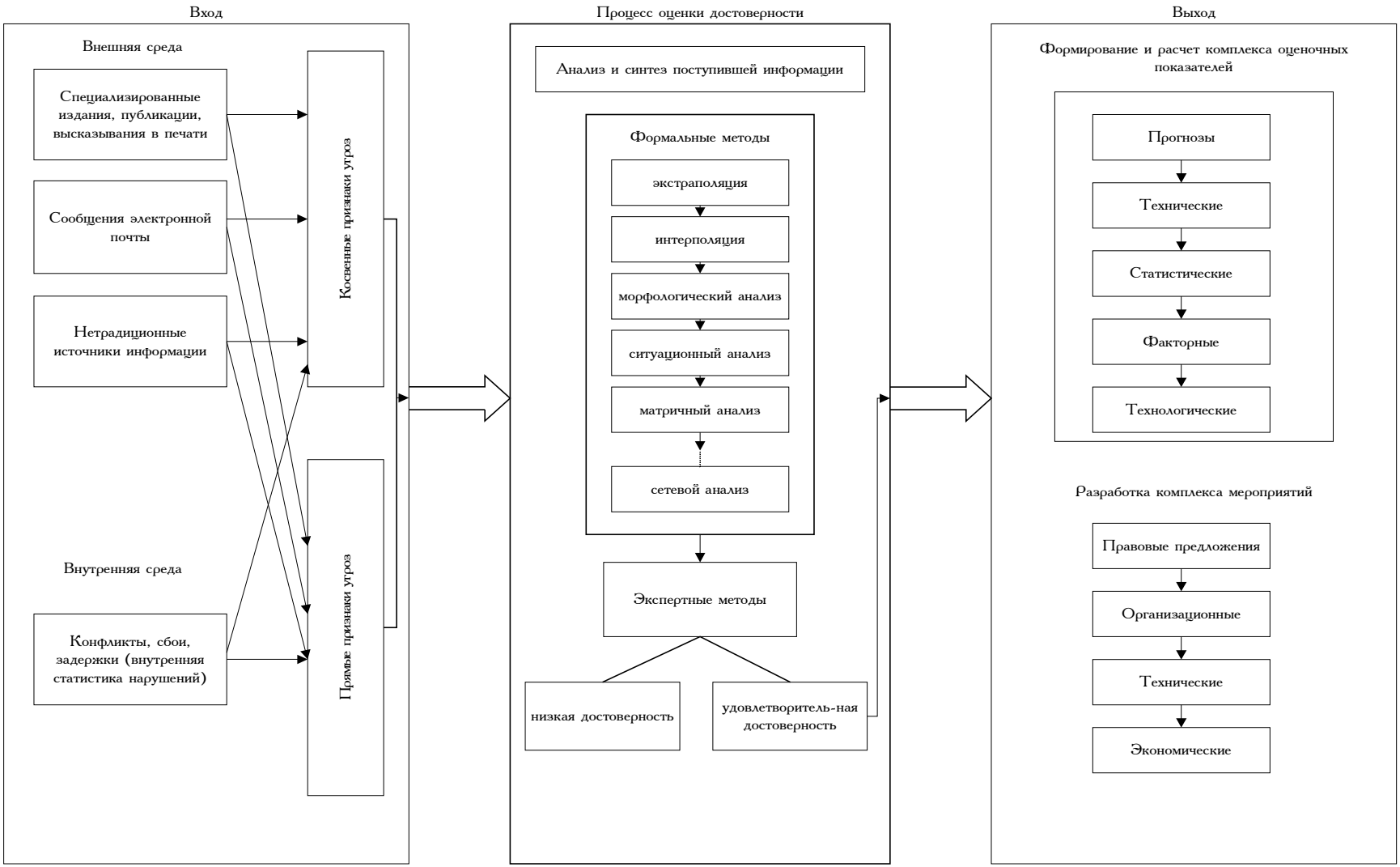

Рис. 6. *Функциональная схема блока “Анализ возможных и потенциальных угроз”.*

Используем следующие обозначения:

C_0 - выигрыш нарушителя от реализации угрозы;

B_0 - затраты нарушителя для подготовки и реализации угрозы.

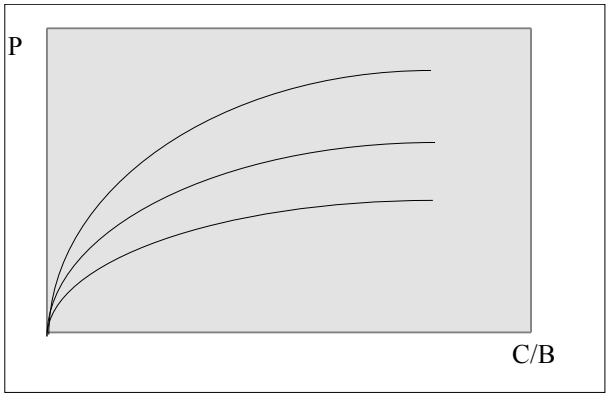

Рис. 7. Кривые привлекательности угроз.

Следовательно можно утверждать, что чем больше значение отношения $C_0/B_0>1$ (рис. 7), тем больше экономических оснований для реализации угрозы.

Тогда, $g=\frac{(1-P^W)*C_0}{B_0}$ - показатель привлекательности угрозы для нарушителя, где P^W -вероятность обнаружения угрозы системой информационной безопасности и противостояние.

Выражение $(1-P^W)$ - определяет среднюю меру успеха реализации угрозы.

Представленный подход является многоитерационным и осуществляется для каждой угрозы с рассмотрением всех возможностей реализации угроз.

В рамках аналитического этапа определяются также критерии эффективности СИБ, в их числе выделяют: целевые; технические; эффективности жизненного цикла; экономические; эффективности управления; социальные.

На аналитическом этапе определяются также допустимые ограничения, накладываемые системой информационной безопасности

на компьютерную систему (например, уменьшение производительности аппаратной и программной составляющих, ограничения административно-организационного плана и др.).

При разработке эталонов информационной безопасности определяются основные требования с точки зрения производительности. К ним относят требования технического, правового и экономического характера.

В качестве технических требований рассматривают эффективность системы защиты, время реагирования на нарушение и т.д.

К правовым требованиям относят соблюдение правовых актов и законов, относящихся к области защиты информации и обработки данных.К экономическим требованиям относят параметры соотношения “стоимость-производительность”, затраты на создание, поддержку и эксплуатацию СИБ, недополученную прибыль.

При анализе характеристик существующих аппаратно-программных средств защиты определяются те, которые удовлетворяют требованиям разработанного эталона информационной безопасности. Определяются системы шифрования, используемые при обработке, приеме-передаче и хранении информации в системе.

Важно отметить, что чем больше охват рассматриваемых систем и методов, тем надежнее будет функционировать СИБ. Другим важным моментом является совместимость рассматриваемых средств с функционирующей системой (в т.ч. аппаратная часть, операционная система, прикладные программы).

Исследовательский этап. При анализе степени риска и определении величин возможных потерь в случае нарушения целостности СИБ проводится анализ состояния системы и оценка видов угроз, с учетом имеющихся механизмов защиты.

Разрабатываются специальные шкалы оценок допустимых потерь в натуральном и денежном эквивалентах. Это обусловлено тем, что в каждой АИС, и в каждом узле, существует своя граница "допустимости" потерь, определяемая ценностью информации, масштабами разработок, бюджетом и множеством других политических, организационных, экономических и этических факторов. В случае, если потери меньше, чем затраты, требуемые на

разработку, внедрение и эксплуатацию средств защиты, и если с точки зрения интересов АИС возможный несанкционированный доступ не приведет к существенным изменениям в работе, то такой риск считается допустимым. Однако, необходимо учитывать, что в большинстве случаев исключается даже незначительная утечка информации, как например, когда идет речь о содержании конфиденциальной информации, связанной с анализом коньюктуры рынка, новых технологий или оригинальных технических решений.

Считаем необходимым отметить, что анализ риска и возможных потерь надлежащим образом основывается на следующих основных факторах:

1. Определение структуры организационных, технических, программных и экономических средств противодействия.

2. Создание соответствующих резервов и разработкой плана восстановления.

3. Достижение необходимой компетентности персонала.

Кроме того, при создании СИБ следует выделять следующие управляемые виды риска:

1. ***Финансовый***. Данный вид риска является основным. Слишком высокий финансовый риск допустим только в случае уникальности защищаемой информации. Следует отметить, что не для всех АИС (даже государственных организаций и учреждений) могут быть выделены достаточно большие денежные и материальные средства на создание и поддержку СИБ. Снижение финансового риска допускается за счет управления другими видами риска и сведения их значений к минимально допустимым.

2. ***Технический***. Этот вид риска присутствует повсеместно и распространяется на весь спектр аппаратных и программных средств защиты.

3. ***Проектный***. Техническая сложность проектируемой СИБ должна соответствовать квалификации и опыту персонала и обеспечивать завершенность и целостность системы.

4. ***Функциональный***. При завершении проектирования СИБ может оказаться, что функциональное наполнение не соответствует заданным требованиям. В результате возникает потребность в дополнительных исследованиях и разработках по уточнению и совершенстованию функционального наполнения.

5. ***Системный***. Если система спроектирована таким образом, что она отвечает основным требованиям окружающей среды и обеспечивает сохранность информации и ресурсов от несанкционированного доступа, использования и распространения и все предварительные допущения относительно основных функций выполнимы, то СИБ считается законченной. Следует учитывать, что система должна быть открытой по отношению к нововведениям в области вычислительной техники, коммуникаций и программного обеспечения, а также защиты информации, одновременно с этим, недопустимы частые и радикальные изменения системы информационной безопасности.

Результаты анализа риска служат основой и способствуют выполнению следующих работ по реализации СИБ[30]:

- *улучшение осведомленности персонала.* Обсуждение вопросов защиты может повысить интерес сотрудников к данной проблеме и приведет к более точному выполнению ими требований политики безопасности;
- *определение сильных и слабых сторон системы контроля*. Многие экономические агенты не имеют полной информации о своей вычислительной базе и ее слабых сторонах. Систематический анализ позволит сформировать всестороннюю информацию о состоянии вычислительной системы и степени риска;
- *подготоваи и принятие решений по выбору средств контроля*. Система контроля снижает производительность системы и вносит дополнительные ограничения в работу пользователей. Некоторые виды контроля достаточно сложны и их применение не может быть оправдано теми преимуществами, которые они обеспечивают. С другой стороны, существуют настолько серьезные виды риска, что поиск и разработка новых, более эффективных средств контроля является необходимой мерой. В любом случае выявленная степень риска определяет уровень необходимых средств контроля;
- *определение затрат на организацию защиты.* Реализация механизмов защиты требует достаточных ресурсов и их работа скрыта от пользователей. Анализ риска помогает определить главные требования к механизмам защиты. При этом необходимо отметить, что чем меньше затраты на организацию защиты, тем выше риск потери информации.

Одним из основных и весьма сложных вопросов создания СИБ является разработка и принятие политики безопасности. Под политикой безопасности понимают комплекс законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение критической информации в АИС. Она должна охватывать все особенности процесса обработки информации, определять поведение системы в различных ситуациях.

При разработке политики безопасности в первую очередь определяется способ управления доступом, порядок доступа субъектов системы к объектам.

Важным моментом является разработка механизмов обнаружения попыток несанкционированного доступа к защищаемым ресурсам, которые могут базироваться на экспертных системах и включать регистрацию, распознавание и обработку событий, связанных с доступом к информации, а также проверку в реальном масштабе времени соответствия всех условий доступа, принятых в концепции СИБ и защиты данных.

Последним шагом, реализованном на данном этапе является разработка и/или адаптация процедур и методов обнаружения несанкционированного доступа, обработки событий в АИС.

В рамках данного этапа разрабатывается план восстановления нормальной работы АИС в случае реализации угрозы нарушителем.

Рекомендательный этап. Выполняется комплекс работ, связанный с размещением элементов СИБ в узлах АИС по критерию эффективность/стоимость. Проводится анализ полученных результатов.

Основное внимание уделяется тестированию СИБ с использованием комплекса многофункциональных тестов покрытия, обеспечивающих предотвращение проникновения программных злоупотреблений, а также снижения потенциальной опасности потери ресурсов.

В рамках работ по тестированию СИБ реализуется комплекс следующих основных работ (рис. 8):

- определение компонентов и объектов, подлежащих тестированию на заданным требованиям безопасности;

- определение временных, трудовых и финансовых ресурсов и ограничений на проведение работ по тестированию (исходя из ресурсов и ограничений всего проекта СИБ);

- на основании анализа ресурсов и ограничений определяется целесообразность проведения комплекса тесто объекта, определенного считывается й эффект от проведения мые затраты

Рис. 8. Структура работ по тестированию системы информационной безопасности

- проводится анализ, доработка сушествующих и/или разработка новых методик и метрик тестирования для конкретных объектов, принимая во внимание совокупность ресурсов и ограничений;

- разрабатываются функциональные тесты покрытия для всех объектов;

- проводится анализ достигнутых результатов, который оформляется в виде специального отчета. В случае, если результаты не соответствуют ожиданиям, определяется качество проведенных тестов, после чего могут быть реализованы работы по доработке методик тестирования и/или самих тестов.

На основе отчета об испытаниях принимается решение об использовании объетов СИБ, или решение о доработке/замене.

Следуюшим шагом является расчет ожидаемого эффекта от использования конкретной СИБ. Но основе расчетов принимается решение об использовании/доработке конкретной конфигурации СИБ.

Последним шагом в рамках исследовательского этапа является документирование СИБ, сотоящий в разработке комплекса методических и инструктивных материалов, описывающих реализацию СИБ и содержащий следующие разделы [112]:

- *политика* - описание конечных целей защиты и подготовки персонала, а также мер, направленных на достижение целей защиты и обеспечивающих адекватную защиту (требования к защите и ее стоимость должны соответствовать ценности обрабатываемой информации);

- *текущее состояние* - описание статуса объектов, субъектов и механизмов защиты в момент составления плана;

- *рекомендации* - описание основных шагов для достижения целей защиты, обеспечивающих достижение целей политики безопасности, способов и механизмов ее реализации в конкретной системе;

- *ответственность* - список лиц, ответственных за функционирование средств защиты, а также установление зон ответственности;

- *расписание* - описание порядка работы механизмов СИБ, включая меры контроля;

- *пересмотр* - описание положений плана, которые периодически подвергаются пересмотру, а также содержание конкретных организационно-технических мероприятий.

- *план восстановления* - описание комплекса действий по восстановлению ресурсов АИС.

Ввод СИБ в эксплуатацию. В рамках заключительного этапа реализуется внедрение и опытная эксплуатация СИБ.

Реализуется комплекс работ по обучению персонала и динамическому анализу их статуса.

Тестирование СИБ должно проводится регулярно на протяжении всего ее жизненного цикла для выявления новых видов угроз, которые не были предусмотрены при разработке СИБ.

На основе информации о новых угрозах и каналах утечки информации, модификации информационных и коммуникационных технологий должна проводиться своевременная модификация и развитие отдельных компонентов или всей СИБ.

Расмотренная схема построения СИБ, содержание приведенных этапов, по нашему мнению, может явиться достаточной основой для развертывания работ по организации проектирования систем безопасности конкретных информационных систем.