Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра интеллектуальных информационных технологий

Ю.И. Иванченко, А.Ю. Деев, А.В. Заговалко

ИНТЕЛЛЕКТУАЛЬНЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие
для студентов специализации
«Интеллектуальные компьютерные технологии защиты информации»
специальности «Искусственный интеллект»

В 3-х частях

Часть 1
Общие положения защиты информации

Минск 2003

УДК 681.3.067 (075.8)
ББК 32.973я73
И 23

Р е ц е н з е н т :
профессор кафедры сетей и устройств телекоммуникаций БГУИР,
канд. техн. наук М.Н. Бобов

Иванченко Ю.И.

И 23 Интеллектуальные компьютерные технологии защиты информации: Учеб. пособие для студ. специализации «Интеллектуальные компьютерные технологии защиты информации» специальности «Искусственный интеллект»: В 3-х ч. Ч.1: Общие положения защиты информации / Ю.И. Иванченко, А.Ю. Деев, А.В. Заговалко. – Мн.: БГУИР, 2003. – 71 с.: ил.
ISBN 985-444-560-7 (ч. 1).

Учебное пособие предназначено для студентов вузов, обучающихся по специализации «Интеллектуальные компьютерные технологии защиты информации», специальности «Искусственный интеллект». Написано по материалам лекций, практических и лабораторных работ, проводимых для студентов БГУИР, в рамках учебных курсов: «Теоретические основы защиты информации», «Средства и методы обеспечения информационной безопасности», «Проектирование защищенных систем», «Управление защитой информации».

УДК 681.3.067 (075.8)
ББК 32.973я73

ISBN 985-444-560-7 (ч. 1)

ISBN 985-444-561-5

Содержание

Введение

В настоящее время компьютерные технологии высокими темпами внедряются во все сферы человеческой деятельности. Не вызывает сомнения тот факт, что на современном этапе развития общества многие традиционные ресурсы, определяющие развитие человечества, постепенно утрачивают свое первоначальное значение, вместе с этим все большее значение приобретает информация. Бесспорно, информация становится сегодня главным ресурсом научно-технического прогресса и социально-экономического развития мирового сообщества.

Вследствие все большего расширения влияния СМИ, лавинообразного распространения компьютерных систем и их взаимодействия посредством сетей наблюдается все большая зависимость как организаций, так и отдельных людей от информации.

Именно поэтому в последние годы среди ученых и специалистов различного профиля, представителей бизнеса, общественных и политических деятелей усиливается интерес к содержанию и методологии решения информационных проблем, возникающих в различных сферах человеческой деятельности.

Вместе с тем переход информации в разряд важнейших ресурсов человечества вызывает к жизни проблему борьбы за обладание этим ресурсом, и как следствие – появление средств нападения, а соответственно и средств защиты.

В пособии использовались материалы лекций, прочитанных студентам БГУИР на кафедре интеллектуальных информационных технологий, в рамках учебных курсов: «Теоретические основы защиты информации», «Средства и методы обеспечения информационной безопасности», «Проектирование защищенных систем», «Управление защитой информации». Также в пособии использовались материалы из источников, представленных в разделе «Литература».

1. Организационно-административное обеспечение информационной безопасности

Организационно-административное обеспечение безопасности информационных ресурсов организации включает организационно-штатную структуру и официально действующие правила безопасной работы и взаимоотношений пользователей в корпоративной информационной системе (КИС).

Вся совокупность таких правил имеет целью обеспечить поддержку и управление информационной безопасностью и составляет политику информационной безопасности организации.

1.1. Политика информационной безопасности

Политика безопасности (security policy) – множество условий, при которых пользователи могут получить доступ к информации и ресурсам системы. Политика безопасности определяет множество требований (правил), которые должны быть выполнены в конкретной реализации системы.

Высшее руководство организации, предприятия должно выработать четкое руководство и демонстрировать свою поддержку и участие в обеспечении информационной безопасности посредством проведения политики информационной безопасности во всей организации.

1.1.1. Документ с изложением политики информационной безопасности

Высшее руководство должно издать в письменной форме положение об информационной политике для всех подразделений организации. Оно должно содержать, как минимум, следующие принципы:

- определение информационной безопасности, ее целей и сферы применения, а также ее значимости как механизма, обеспечивающего совместное использование информации;
- заверение руководства о его намерении поддерживать цели и задачи информационной безопасности;
- разъяснение специфических направлений политики безопасности, принципов, стандартов и соответствия требованиям, включая:
    a) соответствие нормативно-правовым и договорным, контрактным требованиям;
    b) требования по обучению в области обеспечения безопасности;
    c) предотвращение воздействия деструктивных программ и мероприятия по их обнаружению;
    d) политику планирования бесперебойной работы.
- определение общей и особой ответственности для всех аспектов информационной безопасности;
- разъяснение процедуры сообщения о подозрительных инцидентах, затрагивающих проблемы безопасности.

1.2. Выработка официальной политики предприятия в области информационной безопасности

1.2.1. Краткий обзор

1.2.1.1. Организационные вопросы

Целью разработки официальной политики предприятия в области информационной безопасности является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности. Чтобы достичь данной цели, следует учесть специфику конкретной организации.

Во-первых, необходимо принять во внимание цели и основные направления деятельности организации. Например, в Генеральном штабе Министерства обороны и в университете существенно разные требования к конфиденциальности.

Во-вторых, разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организации. Значит, эти законы и правила необходимо выявить и принять во внимание при разработке политики.

В-третьих, если локальная сеть организации не является изолированной, вопросы безопасности следует рассматривать в более широком контексте. Политика должна освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны, а также удаленные проблемы, причиной которых является локальный хост или пользователь.

1.2.1.2. Кто делает политику?

Политика безопасности должна стать результатом совместной деятельности технического персонала, способного понять все аспекты политики и ее реализации, а также руководителей, способных влиять на проведение политики в жизнь. Нереализуемая или неподдерживаемая политика бесполезна.

Поскольку политика безопасности так или иначе затрагивает всех сотрудников организации, следует позаботиться о том, чтобы у вас было достаточно полномочий для принятия политических решений. Хотя некоторой группе (например отделу технического обслуживания) может быть поручено проведение политики (или некоторой ее части) в жизнь, возможно, нужна группа более высокого ранга для поддержки и одобрения политики.

1.2.1.3. Кого затрагивает политика?

Политика безопасности потенциально затрагивает всех пользователей компьютеров в организации, причем по нескольким аспектам. Пользователи могут отвечать за администрирование собственных паролей. Системные администраторы или администраторы безопасности обязаны ликвидировать слабые места в защите и следить за работой всех систем.

Важно с самого начала работы над политикой безопасности правильно подобрать состав коллектива разработчиков. Возможно, на предприятии уже есть подразделение информационной безопасности; естественно, люди из этой группы считают безопасность своей вотчиной. Однако к разработке политики безопасности следует привлечь также специалистов по аудиту и управлению, физической безопасности, информационным системам и т.п. Тем самым будет подготовлена почва для понимания и одобрения политики.

1.2.1.4. Распределение ответственности

Ключевым элементом политики является доведение до каждого его обязанностей по поддержанию режима безопасности. Политика не может предусмотреть всего, однако она обязана гарантировать, что для решения каждого вида проблем существует ответственное лицо.

В связи с информационной безопасностью можно выделить несколько уровней ответственности. На первом уровне каждый пользователь компьютерного ресурса обязан заботиться о защите своего ресурса. Пользователь, допустивший компрометацию своего ресурса, увеличивает вероятность компрометации ресурсов, которыми владеют другие пользователи.

Системные администраторы образуют другой уровень ответственности. Они должны обеспечивать защиту компьютерных систем. Сетевых администраторов можно отнести к еще более высокому уровню. Администраторы безопасности – еще более высокий уровень обеспечения информационной безопасности.

1.2.2. Оценка рисков

1.2.2.1. Общие положения

Один из главных побудительных мотивов выработки политики безопасности состоит в получении уверенности, что деятельность по защите информации построена экономически оправданным образом.

Данное положение кажется очевидным, но, вообще говоря, возможны ситуации, когда усилия прикладываются не там, где нужно. Например, много говорят и пишут о хакерах; в то же время в большинстве обзоров по информационной безопасности утверждается, что в типичной организации ущерб от внутренних, «штатных» злоумышленников значительно больше.

Процесс анализа рисков включает в себя определение того, что следует защищать, от чего защищать и как это делать. Необходимо рассмотреть все возможные риски и ранжировать их в зависимости от потенциального размера ущерба. Этот процесс состоит из множества экономических решений. Давно замечено, что затраты на защиту не должны превышать стоимости защищаемого объекта.

Полное рассмотрение проблемы анализа рисков будет дано ниже. Тем не менее в следующих пунктах будут затронуты два этапа процесса анализа рисков:

- идентификация активов,
- идентификация угроз.

Главной целью деятельности в области информационной безопасности является обеспечение доступности, целостности и конфиденциальности каждого информационного актива. При анализе угроз следует принимать во внимание их воздействие на активы по трем названным направлениям.

1.2.2.2. Идентификация активов

Один из этапов анализа рисков состоит в идентификации всех объектов, нуждающихся в защите. Некоторые активы (например аппаратура) идентифицируются очевидным образом. Про другие (например, про людей, использующих информационные системы) нередко забывают. Необходимо принять во внимание все, что может пострадать от нарушений режима безопасности.

Может быть использована следующая классификация активов:

- Аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, мосты, маршрутизаторы.
- Программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы.
- Данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, данные, передаваемые по коммуникационным линиям.
- Люди: пользователи, обслуживающий персонал.
- Документация: по программам, по аппаратуре, системная, по административным процедурам, по безопасности.
- Расходные материалы: бумага, формы, бланки, красящая лента, магнитные носители.

1.2.2.3. Идентификация угроз

После того как выявлены активы, нуждающиеся в защите, необходимо идентифицировать угрозы этим активам и размеры возможного ущерба. Эта работа должна быть направлена на то, чтобы понять, каких угроз следует опасаться больше всего. В следующих пунктах перечисляются некоторые из возможных видов угроз.

Несанкционированный доступ

Несанкционированный доступ к компьютерным ресурсам – угроза, типичная для большинства организаций. Несанкционированный доступ может принимать различные формы. Иногда это нелегальное использование счета другого пользователя для получения доступа к системе. В других случаях ресурсами пользуются без предварительно полученного разрешения.

Степень важности проблемы несанкционированного доступа для разных организаций разная. Порой передача прав доступа неавторизованному пользователю может привести к разрушению магнитных носителей. Чаще несанкционированный доступ облегчает исполнение других угроз. Разнится и реальность нападения: некоторые организации (известные университеты, правительственные и военные учреждения) как бы притягивают к себе злоумышленников. Следовательно, риск несанкционированного доступа меняется от предприятия к предприятию.

Нелегальное ознакомление с информацией

Нелегальное ознакомление с информацией – другая распространенная угроза. Определите степень конфиденциальности информации, хранящейся в ваших компьютерах. Расшифровка файла паролей откроет дорогу несанкционированному доступу. Мимолетный взгляд на ваше коммерческое предложение может дать конкуренту решающее преимущество. Техническая статья способна вместить в себя годы напряженных исследований.

Отказ в обслуживании

Компьютеры и сети предоставляют своим пользователям множество ценных услуг, от которых зависит эффективная работа многих людей. Когда услуги вдруг становятся недоступными, возникают потери – прямые и косвенные.

Отказ в обслуживании возникает по разным причинам и проявляется по-разному. Сеть может прийти в неработоспособное состояние от поддельного пакета, перегрузки или по причине отказа компонента. Вирус способен замедлить или парализовать работу компьютерной системы. Каждая организация должна определить для себя набор необходимых сервисов и для каждого из них проанализировать последствия его недоступности.

1.2.3. Распределение прав пользователей

При разработке политики безопасности необходимо дать ответы на ряд вопросов, а именно:

- Кто имеет право использовать ресурсы?
- Как правильно использовать ресурсы?
- Кто наделен правом давать привилегии и разрешать использование?
- Кто может иметь административные привилегии?
- Каковы права и обязанности пользователей?
- Каковы права и обязанности администраторов безопасности (системных и сетевых администраторов) по отношению к другим пользователям?
- Как работать с конфиденциальной информацией?

Кроме того, представляется целесообразным отразить в политике этические аспекты использования вычислительных ресурсов.

1.2.3.1. Кто имеет право использовать ресурсы?

Одним из шагов в разработке политики безопасности является определение того, кто может использовать ваши системы и сервисы. Должно быть явно сказано, кому дается право использовать те или иные ресурсы.

1.2.3.2. Как правильно использовать ресурсы?

После определения круга лиц, имеющих доступ к системным ресурсам, необходимо описать правильные и неправильные способы использования ресурсов. Для разных категорий пользователей (студенты, внешние пользователи, штатные сотрудники и т.д.) эти способы могут различаться. Должно быть явно сказано, что допустимо, а что – нет. Могут быть описаны также ограничения на использование определенных ресурсов. При этом вам придется специфицировать уровни доступа разных групп пользователей.

Пользователи должны знать, что они несут ответственность за свои действия независимо от применяемых защитных средств и что использовать чужие счета и обходить механизмы безопасности запрещено.

Для регламентации доступа к ресурсам нужно дать ответы на следующие вопросы:

- Разрешается ли использование чужих ресурсов?
- Разрешается ли отгадывать чужие пароли?
- Разрешается ли разрушать сервисы?
- Должны ли пользователи предполагать, что если файл доступен всем на чтение, то они имеют право его читать?

- Имеют ли право пользователи модифицировать чужие файлы, если по каким-либо причинам у них есть доступ на запись?
- Должны ли пользователи разделять ресурсы?

В большинстве случаев ответы на подобные вопросы должны быть отрицательными.

В политике могут найти отражение авторские и лицензионные права на программное обеспечение. Лицензионное соглашение с поставщиком налагает на организацию определенные обязательства; чтобы не нарушить их, необходимо приложить некоторые усилия. Кроме того, вы, возможно, захотите проинформировать пользователей, что присваивать защищенное авторскими правами программное обеспечение запрещено законом.

Более точно, вы должны довести до сведения пользователей, что:
- копировать авторское и лицензионное программное обеспечение запрещено, за исключением явно оговоренных случаев;
- они всегда могут узнать авторский/лицензионный статус программного обеспечения;
- в случае сомнений копировать не следует.

Политика в области правильного использования ресурсов очень важна. Если явно не сказано, что запрещено, вы не сможете доказать, что пользователь нарушил политику безопасности.

Бывают исключительные случаи, когда в исследовательских целях пользователи или администраторы пытаются «расколоть» защиту сервиса или лицензионной программы. Политика должна давать ответ на вопрос, разрешены ли подобные исследования в вашей организации и каковы могут быть их рамки.

Применительно к исключительным случаям следует дать ответы на следующие вопросы:
- Разрешены ли вообще подобные исследования?
- Что именно разрешено: попытки проникновения, создание и/или запуск червей и вирусов и т.п.?
- Какие регуляторы должны использоваться для контроля за подобными исследованиями (например, их изоляция в рамках отдельного сегмента сети)?
- Как защищены пользователи (в том числе внешние) от подобных исследований?
- Как получать разрешение на проведение исследований?

В случае, когда получено разрешение на исследование, следует изолировать тестируемые сегменты от основной сети предприятия. Черви и вирусы не должны выпускаться в «живую» сеть.

Следует определить порядок и условия исследований системы на предмет ее защищенности. Это может быть контракт с отдельными людьми или сторонней организацией на предмет проверки защищенности сервисов. Частью проверки могут стать попытки взлома систем. Это также должно найти отражение в политике предприятия.

1.2.3.3. Кто наделен правом давать привилегии и разрешать использование?

Политика безопасности должна давать ответ на вопрос, кто распоряжается правами доступа к сервисам. Кроме того, необходимо точно знать, какие именно права им позволено распределять. Если вы не управляете процессом наделения правами доступа к вашей системе, вы не контролируете и круг пользователей. Если вы знаете, кто отвечает за распределение прав, вы всегда сможете узнать, давались ли определенные права конкретному пользователю или он получил их нелегально.

Существует много возможных схем управления распределением прав доступа к сервисам. При выборе подходящей целесообразно принять во внимание следующие моменты:
- Будут ли права доступа распределяться централизованно или из нескольких мест? Можно установить единый распределительный пункт или передать соответствующие права подразделениям и отделам. Все зависит от того, какое соотношение между безопасностью и удобством вы считаете допустимым. Чем сильнее централизация, тем проще поддерживать режим безопасности.
- Какие методы предполагается использовать для заведения учетных записей пользователей и запрещения доступа? Вы должны проверить механизм заведения учетных записей с точки зрения безопасности. В наименее ограничительном режиме уполномоченные лица непосредственно входят в систему и заводят учетные записи вручную или с помощью утилит. Обычно подобные утилиты предполагают высокую степень доверия к использующим их лицам, которые получают значительные полномочия. Если вы останавливаете свой выбор на таком режиме, вам необходимо найти достаточно надежного человека. Другой крайностью является применение интегрированной

системы, которую запускают уполномоченные лица или даже сами пользователи. В любом случае, однако, остается возможность злоупотреблений.

Следует разработать и тщательно документировать специальные процедуры заведения новых счетов, чтобы избежать недоразумений и уменьшить число ошибок. Нарушение безопасности при заведении счетов возможно не только по злому умыслу, но и в результате ошибок. Наличие ясных и хорошо документированных процедур дает уверенность, что подобные ошибки не случатся. Кроме того, необходимо удостовериться, что люди, исполняющие процедуры, понимают их.

Наделение пользователей правами доступа – одна из самых уязвимых процедур. Прежде всего следует позаботиться, чтобы начальный пароль не был легко угадываемым. Целесообразно избегать использования начальных паролей, являющихся функцией от имени пользователя или его полного имени. Не стоит автоматически генерировать начальные пароли, если результат генерации легко предсказуем. Далее, нельзя разрешать пользователям до бесконечности полагаться на начальный пароль. По возможности следует принуждать пользователей менять начальный пароль при первом входе в систему. Правда, даже такая мера бессильна против людей, которые вообще не пользуются своим счетом, сохраняя до бесконечности уязвимый начальный пароль. В некоторых организациях неиспользуемые счета уничтожают, заставляя их владельцев повторно проходить процедуру регистрации.

1.2.3.4. Кто может иметь административные привилегии?

Одно из решений, которое должно быть тщательно взвешено, относится к выбору лиц, имеющих доступ к административным привилегиям и паролям для ваших сервисов. Очевидно, подобный доступ должны иметь системные администраторы, но неизбежны ситуации, когда за привилегиями будут обращаться другие пользователи, что следует с самого начала предусмотреть в политике безопасности. Ограничение прав – один из способов защититься от угроз со стороны своих пользователей. Необходим, однако, сбалансированный подход, когда ограничение прав не мешает людям делать свое дело. Разумнее всего давать пользователям ровно те права, которые нужны им для выполнения своих обязанностей.

Далее, сотрудники, имеющие специальные привилегии, должны быть подотчетны некоторому должностному лицу, и это также необходимо отразить в политике безопасности предприятия. Если «привилегированные» люди перестают быть подотчетными, вы рискуете потерять контроль над своей системой и лишиться возможности расследовать случаи нарушения режима безопасности.

1.2.3.5. Каковы права и обязанности пользователей?

Политика безопасности должна содержать положения о правах и обязанностях пользователей применительно к использованию компьютерных систем и сервисов предприятия. Должно быть явно оговорено, что пользователи обязаны понимать и выполнять правила безопасной эксплуатации систем. Ниже приведен перечень тем, которые целесообразно осветить в данном разделе политики безопасности:

- Каковы общие рамки использования ресурсов? Существуют ли ограничения на ресурсы и каковы они?
- Что является злоупотреблением с точки зрения производительности системы?
- Разрешается ли пользователям совместное использование счетов?
- Как «секретные» пользователи должны охранять свои пароли?
- Как часто пользователи должны менять пароли? Каковы другие аналогичные ограничения и требования?
- Как обеспечивается резервное копирование – централизованно или индивидуально?
- Как реагировать на случаи просмотра конфиденциальной информации?
- Как соблюдается конфиденциальность почты?
- Какова политика в отношении неправильно адресованной почты или отправлений по спискам рассылки или в адрес дискуссионных групп (непристойности, приставания и т.п.)?
- Какова политика по вопросам электронных коммуникаций (подделка почты и т.п.)?

Каждая организация должна разработать политику защиты права сотрудников на тайну. Рекомендуется, чтобы эта политика охватывала все возможные среды, а не только электронную почту.

Предлагается пять критериев оценки подобной политики:

- Согласуется ли политика с существующим законодательством и с обязанностями по отношению к третьим сторонам?
- Не ущемляются ли без нужды интересы работников, работодателей или третьих сторон?

- Реалистична ли политика и вероятно ли ее проведение в жизнь?
- Затрагивает ли политика все виды передачи и хранения информации, используемые в организации?
- Объявлена ли политика заранее и получила ли она одобрение всех заинтересованных сторон?

1.2.3.6. Каковы права и обязанности администраторов безопасности по отношению к другим пользователям?

Должен соблюдаться баланс между правом пользователей на тайну и обязанностью администратора безопасности собирать достаточно информации для разрешения проблем и расследования случаев нарушения режима безопасности. Политика должна определять границы, в пределах которых администратор безопасности вправе исследовать пользовательские файлы с целью разрешения проблем и для иных нужд, и каковы права пользователей. Можно также сформулировать положение относительно обязанности администраторов соблюдать конфиденциальность информации, полученной при оговоренных выше обстоятельствах. Политика должна содержать ответы на несколько вопросов:

- Может ли администратор отслеживать или читать пользовательские файлы при каких-либо обстоятельствах?
- Какие обязательства администратор при этом берет на себя?
- Имеют ли право администраторы исследовать сетевой трафик?

1.2.3.7. Как работать с конфиденциальной информацией?

Прежде чем предоставлять пользователям доступ к вашим сервисам, следует определить, каков уровень защиты данных на вашей системе. Тем самым вы сможете определить уровень конфиденциальности информации, которую пользователи могут у вас размещать. Наверное, вы не хотите, чтобы пользователи хранили секретные сведения на компьютерах, которые вы не собираетесь как следует защищать. Следует сообщить пользователям, какие сервисы (при наличии таковых) пригодны для хранения конфиденциальной информации. Должны рассматриваться различные способы хранения данных (на диске, ленте, файловом сервере и т.д.). Этот аспект политики должен быть согласован с правами системных администраторов по отношению к обычным пользователям.

1.2.4. Что делать, когда политику безопасности нарушают

Очевидно, что любая официальная политика, вне зависимости от ее отношения к информационной безопасности, время от времени нарушается. Нарушение может явиться следствием пользовательской небрежности, случайной ошибки, отсутствия должной информации о текущей политике или ее непонимания. Возможно также, что некое лицо или группа лиц сознательно совершают действия, прямо противоречащие утвержденной политике безопасности.

Необходимо заранее определить характер действий, предпринимаемых в случае обнаружения нарушений политики, чтобы эти действия были быстрыми и правильными. Следует организовать расследование, чтобы понять, как и почему нарушение стало возможным. После этого нужно внести коррективы в систему защиты. Тип и серьезность коррективов зависят от типа случившегося нарушения.

1.2.4.1. Выработка ответа на нарушение политики

Политику безопасности могут нарушать самые разные лица. Некоторые из них являются своими, местными пользователями, другие нападают извне. Полезно определить сами понятия «свои» и «чужие», исходя из административных, правовых или политических положений. Эти положения очерчивают характер санкций, которые можно применить к нарушителю – от письменного выговора до привлечения к суду. Таким образом, последовательность ответных действий зависит не только от типа нарушения, но и от вида нарушителя; она должна быть продумана задолго до первого инцидента, хотя это и непросто.

Следует помнить, что правильно организованное обучение – лучшая защита. Вы обязаны поставить дело так, чтобы не только внутренние, но и внешние легальные пользователи знали положения вашей политики безопасности. Если вы будете располагать свидетельством подобного знания, это поможет вам в будущих правовых акциях, когда таковые понадобятся.

Проблемы с нелегальными пользователями в общем те же. Нужно получить ответы на вопросы о том, какие типы пользователей нарушают политику, как и зачем они это делают. В зависимости от резуль-

татов расследования вы можете просто заткнуть дыру в защите и удовлетвориться полученным уроком или предпочтете более крутые меры.

1.2.4.2. Что делать, когда местные пользователи нарушают политику безопасности сторонней организации

Каждое предприятие должно заранее определить набор административных санкций, применяемых к местным пользователям, нарушающим политику безопасности сторонней организации. Кроме того, необходимо позаботиться о защите от ответных действий сторонней организации. При выработке политики безопасности следует учесть все юридические положения, применимые к подобным ситуациям.

1.2.4.3. Спецификация контактов с внешними организациями и определение ответственных

Политика безопасности предприятия должна содержать процедуры для взаимодействия с внешними организациями, в число которых входят правоохранительные органы, другие организации, команды «быстрого реагирования», средства массовой информации. В процедурах должно быть определено, кто имеет право на такие контакты и как именно они совершаются. Среди прочих нужно дать ответы на следующие вопросы:

- Кто и по каким вопросам может общаться с прессой?
- Когда следует обращаться в правоохранительные органы?
- Если соединение выполняется из сторонней организации, имеет ли право системный администратор обратиться в эту организацию?
- Какого рода сведения об инцидентах могут выходить за пределы организации?

Детальная информация по контактам должна быть постоянно доступна вместе с ясно определенными процедурами отработки этих контактов.

1.2.4.4. Каковы обязанности по отношению к соседям и другим пользователям Интернет?

Рабочая группа по политике безопасности (Security Policy Working Group, SPWG) сообщества Интернет опубликовала документ под названием «Основы политики для безопасной работы в Интернет». В нем Интернет трактуется как совместное предприятие, в котором пользователи должны помогать друг другу в поддержании режима безопасности. Это положение следует учитывать при разработке политики предприятия. Главный вопрос состоит в том, какой информацией можно делиться с соседями, а какой нет. Ответ зависит как от типа организации (военная, учебная, коммерческая и т.д.), так и от характера возможных угроз.

1.2.4.5. Процедурные вопросы реагирования на нарушения

Помимо политических положений необходимо продумать и написать процедуры, исполняемые в случае обнаружения нарушений режима безопасности. Такие процедуры должны быть заготовлены заранее и отрепетированы для всех видов нарушений.

1.2.5. Пресекать или следить?

Когда на организацию совершается нападение, грозящее нарушением информационной безопасности, стратегия ответных действий может строиться под влиянием двух противоположных подходов.

Если руководство опасается уязвимости предприятия, оно может предпочесть стратегию «защититься и продолжить». Главной целью подобного подхода является защита информационных ресурсов и максимально быстрое восстановление нормальной работы пользователей. Действиям нарушителя оказывается максимальное противодействие, дальнейший доступ предотвращается, после чего немедленно начинается процесс оценки нанесенных повреждений и восстановления. Возможно, при этом придется выключить компьютерную систему, закрыть доступ в сеть или предпринять иные жесткие меры. Оборотная сторона медали состоит в том, что пока злоумышленник не выявлен, он может вновь напасть на эту же или другую организацию прежним или новым способом.

Другой подход, «выследить и осудить», опирается на иные философию и систему целей. Основная цель состоит в том, чтобы позволить злоумышленнику продолжать свои действия, пока организация не сможет установить его личность. Такой подход предпочитают правоохранительные органы. К сожале-

нию, эти органы не смогут освободить организацию от ответственности, если пользователи обратятся в суд с иском по поводу ущерба, нанесенного их программам и данным.

Судебное преследование – не единственный возможный исход установления личности нарушителя. Если виновным оказался штатный сотрудник или студент, организация может предпочесть дисциплинарные меры. В политике безопасности должны быть перечислены допустимые варианты наказания и критерии выбора одного или нескольких из них в зависимости от личности виновного.

Руководство организации должно заранее тщательно взвесить различные возможности при выборе стратегии ответных действий. В принципе стратегия может зависеть от конкретных обстоятельств нападения. Возможен и выбор единой стратегии на все случаи жизни. Нужно принять во внимание все за и против и проинформировать пользователей о принятом решении, чтобы они в любом случае осознавали степень своей уязвимости.

Следующий контрольный перечень помогает сделать выбор между стратегиями «защититься и продолжить» и «выследить и осудить».

При каких обстоятельствах предпочесть стратегию «защититься и продолжить»:
- Активы организации недостаточно защищены.
- Продолжающееся вторжение сопряжено с большим финансовым риском.
- Нет возможности или намерения осудить злоумышленника.
- Неизвестен круг пользователей.
- Пользователи неопытны, а их работа уязвима.
- Пользователи могут привлечь организацию к суду за нанесенный ущерб.

При каких обстоятельствах предпочесть стратегию «выследить и осудить»:
- Активы и системы хорошо защищены.
- Имеются хорошие резервные копии.
- Угроза активам организации меньше потенциального ущерба от будущих повторных вторжений.
- Имеет место согласованная атака, повторяющаяся с большой частотой и настойчивостью.
- Организация притягивает злоумышленников и, следовательно, подвергается частым атакам.
- Организация готова идти на риск, позволяя продолжить вторжение.
- Действия злоумышленника можно контролировать.
- Доступны развитые средства отслеживания, так что преследование нарушителя имеет шансы на успех.
- Обслуживающий персонал обладает достаточной квалификацией для успешного выслеживания.
- Руководство организации желает осудить злоумышленника.
- Системный администратор знает, какого рода информация обеспечит успешное преследование.
- Имеется тесный контакт с правоохранительными органами.
- В организации есть человек, хорошо знающий соответствующие законы.
- Организация готова к искам собственных пользователей по поводу программ и данных, скомпрометированных во время выслеживания злоумышленника.

1.2.6. Толкование политики безопасности

Важно определить, кто будет интерпретировать политику безопасности. Это может быть отдельное лицо или подразделение. Вне зависимости от того, насколько хорошо она написана, политика безопасности время от времени нуждается в разъяснении, а заодно и в пересмотре.

1.2.7. Гласность политики безопасности

Письменный документ с изложением политики должен быть доступен не только руководителям и сотрудникам, ответственным за информационную безопасность, он должен быть доступен всем сотрудникам организации. Более того, обеспечение доступа к документу еще не гарантия его действенности.

После того как положения политики безопасности записаны и одобрены, необходимо начать активный процесс, гарантирующий, что политика воспринята и обсуждена. Почтовую рассылку нельзя признать достаточной мерой. Прежде чем политика вступит в силу, следует отвести время для дискуссий, чтобы

все заинтересованные пользователи могли высказать свое мнение и указать на недостатки политики. В идеале политика должна соблюдать баланс между безопасностью и производительностью труда, удобством работы.

Целесообразно провести собрания, чтобы выслушать пожелания пользователей и заодно убедиться в правильном понимании ими предложенной политики. (Творцы политики порой бывают несколько косноязычны.) В собраниях должны участвовать все: от высшего руководства до младших специалистов. Безопасность – забота общая.

Помимо усилий по оглашению политики на начальном этапе, необходимо постоянно напоминать о ней. Опытные пользователи нуждаются в периодических напоминаниях, новичкам ее нужно разъяснять, вводя в курс дела. Прежде чем допускать сотрудника к работе, разумно получить его подпись под свидетельством о том, что он прочитал и понял политику безопасности. В ситуациях, чреватых судебным разбирательством после нарушения политики, бумага с подписью может оказаться весьма кстати.

1.3. Организация системы безопасности

Управлять информационной безопасностью невозможно без соответствующих структур. Для инициирования и контроля за реализацией информационной безопасности внутри организации должна быть создана определенная структура управления. Она должна включать как штатные, так и внештатные органы управления.

1.3.1. Инфраструктура информационной безопасности

Для согласования политики информационной безопасности, распределения функций, координирования мер безопасности в организации следует проводить совещания руководящих лиц. В случае необходимости, нужно обеспечить возможность получения консультаций специалистов и сделать эту информацию доступной для всех. Для отслеживания основных тенденций в области стандартизации, критериев оценки, а также для определения наиболее подходящих пунктов транспортного соединения в случае инцидентов, затрагивающих проблемы безопасности, должны быть установлены контакты с внешними специалистами по обеспечению безопасности. Следует всячески поощрять многопрофильные подходы к обеспечению информационной безопасности, например, совместную работу аудиторов, пользователей и администраторов в этом направлении.

1.3.2. Совещание руководящих лиц по информационной безопасности

Ответственность за обеспечение информационной безопасности несут все руководящие сотрудники. Следует предусмотреть необходимость проведения совещаний высших руководящих лиц для обеспечения четкого руководства и поддержки инициатив по проведению мероприятий безопасности. В случае отсутствия достаточного количества вопросов для проведения регулярных совещаний по безопасности рекомендуется включать эти вопросы в повестку дня других регулярных совещаний.

Обычно на таких совещаниях рассматриваются следующие вопросы:

- обзор и согласование политики информационной безопасности и распределение ответственности;
- мониторинг основных рисков, которым подвергаются информационные ресурсы;
- анализ инцидентов, затрагивающих проблемы безопасности;
- одобрение основных инициатив и планов по повышению уровня информационной безопасности.

Рекомендуется, чтобы один из руководителей нес основную ответственность за координацию политики информационной безопасности.

1.3.3. Координация информационной безопасности

В крупной организации следует координировать меры информационной безопасности на многопрофильных совещаниях.

На таком совещании в присутствии представителей всех подразделений следует координировать реализацию мер информационной безопасности. Типичными вопросами такого совещания могут быть:

- согласование специфических функций и ответственности за информационную безопасность в пределах организации;
- согласование определенных методологий и процедур обеспечения информационной безопасности, например, оценки рисков, системы классификации мер безопасности;
- согласование и поддержка инициатив в отношении информационной безопасности в пределах организации, например, программы по распространению знаний об информационной безопасности;
- обеспечение того, чтобы безопасность стала частью процесса информационного планирования;
- координация реализации специфических мер информационной безопасности для новых систем или услуг;
- обеспечение наглядности поддержки мер информационной безопасности в организации.

1.3.4. Распределение ответственности за информационную безопасность

Ответственность за обеспечение защиты отдельных информационных ресурсов, а также за проведение специфических мер безопасности должна быть четко определена.

Политика информационной безопасности должна обеспечивать общее руководство по распределению функций и ответственности за состояние безопасности в организации. В случае необходимости это должно быть дополнено более детальной местной (на уровне отдельных подразделений) интерпретацией, отражающей специфику местонахождения, а также специфику систем или услуг, которая должна четко определять распределение ответственности в отношении индивидуальных ресурсов (как материальных, так и информационных), а также безопасность информационных процессов, например, планирование бесперебойной деятельности.

Ответственность за безопасность информационной системы должен нести владелец конкретной системы. Владельцы информационных систем могут делегировать свои полномочия в области безопасности (полномочия предпринимать те или иные действия) отдельным пользователям или провайдерам услуг. Однако, в конечном счете, именно они остаются ответственными за обеспечение безопасности системы.

Во избежание путаницы в отношении индивидуальной ответственности важно, чтобы те сферы, за которые каждый руководитель несет ответственность, были бы четко определены, а именно:
- Различные ресурсы и процессы безопасности, связанные с каждой отдельной системой, должны быть определены предельно ясно.
- Назначение ответственных за каждый вид ресурсов или процесс должно быть согласовано, и круг ответственности определен документально.
- Полномочия должны быть четко определены и документированы.

1.3.5. Процедура санкционирования в отношении средств информационной технологии

Все вопросы, связанные с новой информационной техникой, должны быть согласованы с руководителями, а процедура согласования четко разработана. Лицам согласующим соответствующие изменения, следует убедиться в том, что инсталляция программного обеспечения и оборудования производится в производственных целях и будет обеспечивать адекватный уровень защиты безопасности, а также не будет отрицательно влиять на безопасность существующей инфраструктуры.

Следует предусмотреть два уровня санкционирования:
- **Производственное согласование.** Установка каждой единицы программного обеспечения и оборудования должна производиться с разрешения соответствующего руководителя со стороны пользователя, который обосновывает их назначение и использование. Соответствующее разрешение должно быть также получено от руководителя, ответственного за обеспечение информационной безопасности на месте, для соблюдения соответствия всем направлениям политики безопасности и ее требованиям.
- **Техническое согласование.** При необходимости следует проверить, что для всех устройств, подключенных к сетям коммуникации, или находящихся в ведении определенного провайдера услуг, имеется разрешение на установку со стороны руководства.

1.3.6. Консультация специалиста по информационной безопасности

Каждая организация, крупная или небольшая, может выиграть при привлечении консультанта по безопасности. В идеале консультантом должен быть опытный специалист по информационной безопасности, работающий в данной организации. Малые организации, к сожалению, не могут держать в штате такого специалиста-консультанта. В этом случае рекомендуется создание единого централизованного пункта, к услугам которого следует прибегать в случае необходимости принятия обоснованных решений в области безопасности, а также в случае необходимости получения помощи в максимальном развитии знаний и опыта внутри организации.

Консультанты по информационной безопасности или консультационные пункты должны иметь в своем распоряжении все необходимое, для того чтобы дать правильный совет по всем аспектам информационной безопасности.

Качество их оценки угроз безопасности и советов по контрмерам будет предопределять эффективность программы обеспечения информационной безопасности в организации. Для максимальной эффективности консультант или консультационный пункт должны иметь прямую связь с соответствующими руководителями организации. Они должны привлекаться на как можно более ранней стадии, сразу после инцидента, затрагивающего проблемы безопасности, для обеспечения квалифицированного руководства и привлечения соответствующих ресурсов для расследования. Несмотря на то, что большая часть расследований в плане внутренней безопасности будет проводиться под контролем руководящих лиц, специалист по информационной безопасности может быть приглашен для консультации, руководства или проведения расследования.

1.3.7. Сотрудничество между организациями

Специалистам по информационной безопасности, работающим в организации, следует, по своему усмотрению, наладить контакты с внешними специалистами по безопасности (в данной отрасли или на данной территории). Такое сотрудничество дает возможность использования коллективного опыта в оценке угроз безопасности и способствует распространению полезного опыта в области безопасности, помогая тем самым преодолеть трудности, возникающие во взаимоотношениях между организациями.

Важным представляется и установление соответствующих контактов с правоохранительными органами, провайдерами услуг информационной технологии, а также с организациями, занимающимися предоставлением телекоммуникационных услуг. Это даст возможность быстро войти в контакт с нужными лицами и получить консультацию в случае инцидента, затрагивающего проблемы безопасности.

Обмен информацией по вопросам безопасности должен быть ограничен для обеспечения защиты конфиденциальной информации компании от несанкционированного доступа.

1.3.8. Независимая ревизия состояния информационной безопасности

Документ, определяющий политику информационной безопасности, устанавливает ответственность должностных лиц и направления обеспечения информационной безопасности. Существующая практика обеспечения информационной безопасности должна подвергаться независимой ревизии для получения уверенности в том, что организационные меры действительно соответствуют политике безопасности, и ее проведение является эффективным.

Примечание. Возможным исполнителем такой проверки может быть внутренний аудитор, независимый руководитель высшего звена либо третья сторона, специализирующаяся в осуществлении такого рода исследованиях и экспертизе. Кандидаты на проведение такой работы должны иметь соответствующие навыки и опыт.

1.4. Ответственность субъектов информационной безопасности

Все пользователи КИС несут ответственность за обеспечение их безопасности. Однако форма и объем ответственности зависят от роли конкретного сотрудника и степени его причастности к КИС. Целесообразно рассматривать три широкие категории штатного персонала, а также их функции и ответственность в отношении обеспечения безопасности КИС. Общая (т.е. минимальная) ответственность этих категорий штатного персонала оговорена ниже:

Рядовые сотрудники – все, кто занимаются использованием, эксплуатацией, разработкой или внедрением компьютерных систем. Они ответственны за:

- знание своих обязанностей по обеспечению безопасности КИС и принятие соответствующих действий;
- проявление активной заинтересованности в поддержании безопасности КИС – выявление новых видов потенциальных угроз и информирование о них руководителей подразделений;
- знание своих правовых обязанностей и принятие соответствующих действий;
- соблюдение требований, обязательных в масштабе всей организации стандартов;
- соблюдение требований локальных стандартов и инструкций.

Руководители подразделений – сотрудники, уполномоченные администрацией осуществлять ежедневное руководство работой и/или развитием производственных функций и поддерживающих их компьютерных систем. Они ответственны за:

- оценку потенциальных угроз для тех направлений, которыми они руководят;
- разработку соответствующих локальных стандартов и инструкций по обеспечению безопасности КИС и согласование их с администрацией;
- обеспечение выполнения находящимся под их руководством персоналом соответствующих стандартов и инструкций;
- обеспечение надлежащего обучения для администраторов сетей;
- стремление обеспечить достаточное финансирование для нужд безопасности КИС;
- обеспечение регулярного обновления требований безопасности, информационного программного обеспечения и планов действий в экстренных случаях.

Администрация – руководители наиболее высокого ранга. Они ответственны за:

- общую безопасность находящихся в их ведении систем (как владельцы этих систем), включая принятие решений по выдаче разрешений на подключение к своей сети других сетей;
- обеспечение достаточного финансирования для нужд безопасности КИС;
- назначение АДМИНИСТРАТОРОВ БЕЗОПАСНОСТИ КИС для каждого производственного подразделения;
- определение круга основных обязанностей для координаторов по безопасности КИС и обеспечение их обучения в достаточном объеме.

Кроме рассмотренных категорий целесообразно выделить еще две категории:

Администраторы безопасности КИС – сотрудники, назначенные администрацией для обеспечения безопасности определенных ресурсов и распространения знаний по безопасности КИС в отдельных подразделениях. Они ответственны за:

- реализацию правил обеспечения безопасности информационных ресурсов подразделения или функционального комплекса;
- обеспечение администрирования установленных для них средств безопасности;
- обеспечение полной осведомленности среди сотрудников подразделений о важности поддержания безопасности КИС;
- обеспечение информирования всех сотрудников своих подразделений о существовании руководств по безопасности;
- помощь руководителям подразделений в выявлении потенциальных рисков и составлении инструкций для своих подразделений.

Администраторы сетей / системные администраторы – сотрудники, назначенные руководителями подразделений для сопровождения и эксплуатации локальных сетей (LAN) или локальных систем. Они несут определенную ответственность за вверенные им системы, которая заключается в:

- администрировании и идентификации пользователей;
- снятие резервных копий с различных систем и их данных.

1.5. Классификация ресурсов и контроль за ними

Обеспечение соответствующей защиты ресурсов организации невозможно без их идентификации. Все основные информационные ресурсы должны быть четко определены, взяты на соответствующий учет с назначением ответственного лица.

1.5.1. Отчетность по ресурсам

Отчетность за использование ресурсов помогает обеспечить адекватность мер безопасности. По основным ресурсам должны определяться их владельцы с возложением на них ответственности за поддержание соответствующих мер безопасности. Реализация этих мер может быть делегирована другим лицам, но ответственность по отчетности остается на назначенных владельцах ресурсов.

1.5.2. Инвентаризация ресурсов

Инвентаризация ресурсов помогает обеспечить эффективность мер безопасности и может способствовать достижению других целей, например, обеспечению здоровья и личной безопасности, страхованию и управлению активами. Инвентаризация должна проводиться в отношении основных ресурсов каждой информационной системы. Каждый компонент ресурсов должен быть четко определен в соответствии с классификацией по его принадлежности и применяемым к нему мерам безопасности. Примерами ресурсов, ассоциирующихся с информационными системами, могут быть:

- **информационные ресурсы:** базы и файлы данных, системная документация, руководства для пользователей, учебные материалы, операционные процедуры и процедуры поддержки, схемы обеспечения непрерывного функционирования, схемы нейтрализации неисправности;
- **программные ресурсы:** прикладное программное обеспечение, системное программное обеспечение, средства разработки приложений и утилиты;
- **физические ресурсы:** компьютеры и коммуникационное оборудование, магнитные носители информации (ленты и диски), другое техническое оборудование (источники питания, кондиционеры), мебель, помещения;
- **услуги:** вычислительные и коммуникационные услуги, другие технические (отопление, освещение, энергоснабжение, кондиционирование воздуха).

1.5.3. Классификация информации

Классификация информации должна использоваться для определения необходимости принятия мер безопасности, их объема и приоритетности.

Информация имеет различную степень уязвимости и важности. Отдельные компоненты информации могут нуждаться в дополнительной защите или в особом обращении. Для определения соответствующих уровней обеспечения безопасности и информирования пользователей о необходимости особого обращения с информацией должна использоваться система классификации мер безопасности.

1.5.4. Принципы классификации

При классификации мер безопасности и определении соответствующих мероприятий по защите информации следует принимать во внимание необходимость предоставления информации, а также последствия несанкционированного доступа или разрушения информации. В частности, следует обратить внимание на следующие факторы:

- **конфиденциальность:** производственная необходимость предоставления или ограничения доступа к информации с соблюдением конфиденциальности и контроля, требуемых в отношении ограниченного доступа к информации;
- **целостность:** производственная необходимость проверки изменений информации и контроль, необходимый для защиты правильности и полноты информации;
- **доступность:** производственная необходимость иметь доступ к информации и соблюдение принятых видов контроля для ее получения.

Ответственность за определение классификационной принадлежности единицы информации, например, документа, записи данных, файла данных или дискеты, а также за периодичный пересмотр классификации должна лежать на лице, подготовившем данные, или на владельце данных.

Следует уделить особое внимание интерпретации классификационных меток на документах, поступающих от других организаций, которые могут быть различными в отношении одной и той же информации либо похожими.

1.5.5. Маркирование информации

Информация ограниченного доступа и выходные данные систем, обрабатывающих подобную информацию, должны быть снабжены соответствующими метками. Однако зачастую информация перестает быть уязвимой по истечении некоторого периода времени, например, когда она становится достоянием широкой публики. Этот факт следует принимать во внимание, поскольку обеспечение излишней секретности приводит к неоправданным дополнительным расходам.

Выходные данные, поступающие от информационных систем, содержащих информацию ограниченного доступа, должны иметь соответствующую метку. Маркировка должна отражать степень секретности наиболее уязвимых сведений в выходных данных. Это относится к распечатанным отчетам, экранным дисплеям, магнитным носителям (лентам, дискетам, кассетам), электронным сообщениям и электронной передаче файлов.

Примечание. Физические метки являются наиболее подходящими для маркировки. Тем не менее в некоторых случаях, например, при электронной передаче, функция маркирования выполняется иными средствами, такими, как процедуры, контракты или почтовые уведомления.

1.6. Обеспечение безопасности персоналом

Снизить риски, возникающие вследствие ошибок, кражи, мошенничества или неправильного обращения с техникой, возможно только при должной организации работ с персоналом.

1.6.1. Обеспечение безопасности при составлении должностных инструкций и проверка благонадежности

Обеспечение мер безопасности должно начинаться уже на стадии приема на работу; они должны предусматриваться должностными инструкциями и контрактными условиями. Выполнение мер безопасности должно отслеживаться в период работы сотрудника.

Руководители должны обеспечить, чтобы должностные инструкции включали все необходимые обязанности по соблюдению мер безопасности. Принимаемые на работу лица должны пройти соответствующую проверку на благонадежность, особенно для уязвимых видов деятельности. Все служащие и сторонние пользователи должны подписать обязательство о соблюдении конфиденциальности (о неразглашении тайны, нераспространении информации ограниченного пользования).

1.6.2. Отражение мер безопасности в должностных инструкциях

В должностные инструкции должна быть включена ответственность за соблюдение мер безопасности в соответствии с проводимой в организации политикой информационной безопасности. Сюда входят общие обязанности по реализации или соблюдению политики безопасности, а также особые обязанности по защите конкретных ресурсов или по выполнению конкретных процедур и процессов обеспечения безопасности.

1.6.3. Проверка на благонадежность при приеме на работу

Принимаемые на работу должны подвергаться проверке, если работа связана с доступом к средствам обработки уязвимой информации. При этом необходимо:

- представление, по крайней мере, двух положительных характеристик, одна служебная и одна личная;
- проверка автобиографических данных на полноту и достоверность;
- подтверждение образовательной и профессиональной квалификации;
- проверка идентичности личности, например, паспортных данных;
- проверка кредитоспособности при приеме на ответственные должности, например, проверка финансового положения.

1.6.4. Договор о соблюдении конфиденциальности

Пользователи информационными средствами организации должны подписать соответствующее обязательство в отношении конфиденциальности (о неразглашении). Служащие обычно подписывают такое обязательство как часть основных условий приема на работу.

Персонал отделений и сторонние пользователи, не связанные существующим контрактом, содержащим обязательства по соблюдению конфиденциальности, должны обязательно подписать такой договор, прежде чем получить доступ к информационным средствам организации.

Договора о соблюдении конфиденциальности должны пересматриваться в случае изменений условий приема на работу или контрактных условий, особенно когда служащие собираются увольняться или по окончании срока действия контракта.

1.7. Обучение пользователей

Чтобы обеспечить информированность пользователей о существующих угрозах для информационной безопасности и связанных с ними проблемах, а также предоставить им все необходимое для реализации выработанной организацией политики обеспечения безопасности в процессе работы, необходимо планировать и регулярно осуществлять мероприятия по обучению.

Пользователи должны быть обучены процедурам безопасности и правильному использованию информационных средств.

Пользователи должны получить официальное письменное разрешение на доступ с указанием прав и ограничений.

1.7.1. Теоретическое и практическое обучение информационной безопасности

До получения разрешения на доступ к информационным услугам пользователи должны пройти соответствующее обучение в отношении политики и процедур обеспечения безопасности, включая требования безопасности и контроля, а также обучение по правильному использованию информационных средств, например, по процедурам подключения к системе, использованию пакетов прикладных программ.

Примечание. Данные меры необходимы для обеспечения правильного выполнения процедур безопасности и минимизации возможных рисков для конфиденциальности, целостности и доступности данных или услуг, которые могут возникнуть из-за ошибки пользователя.

Такая политика должна применяться в отношении служащих организации и сторонних пользователей.

1.8. Реагирование на инциденты

Информация об инциденте должны быть доведена до руководства как можно быстрее. Это необходимо для того, чтобы сократить ущерб от инцидентов, касающихся проблем безопасности, и сбоев в работе, а также отслеживать такие инциденты и делать соответствующие выводы на будущее.

1.8.1. Доведение информации об инцидентах, касающихся проблем безопасности

Должна быть разработана официальная процедура доведения такой информации совместно с процедурой реагирования на инциденты с указанием действий, которые следует предпринять при получении сообщения об инциденте. Все служащие организации и подрядчики должны владеть процедурой сообщения об инцидентах и обязаны докладывать о таких инцидентах как можно быстрее в соответствующую службу.

Все служащие организации и подрядчики должны быть ознакомлены с процедурами доклада о различного вида инцидентах (нарушение защиты, угроза, уязвимые места защиты или сбои), которые могут повлиять на безопасность ресурсов организации. Они обязаны сообщать о любых обнаруженных или вызывающих подозрение инцидентах как можно быстрее в соответствующую службу. Организация должна создать формальную дисциплинарную процедуру в отношении служащих, чьи действия привели к нарушению безопасности.

1.8.2. Сообщение об уязвимости защиты

Пользователи информационными услугами обязаны фиксировать и сообщать обо всех замеченных или предполагаемых уязвимых местах средств защиты в отношении систем или услуг. Пользователи должны сообщать об этом либо непосредственному руководителю, либо своему поставщику услуги как можно быстрее. Пользователи должны знать, что ни при каких обстоятельствах они не должны предпринимать самостоятельные попытки проверить слабые места, вызывающие подозрение.

Примечание. Это делается в целях их же защиты, поскольку их действия по проверке слабых мест могут быть интерпретированы как потенциальное злоупотребление.

1.8.3. Сообщение о сбоях программного обеспечения

Пользователи услуг информационной техники должны фиксировать все программы, которые, по их мнению, работают некорректно, т.е. не соответствуют спецификациям, а также сообщать об этом в местную службу поддержки или же непосредственно провайдеру услуг.

Следует разработать процедуры немедленных действий лиц, которые предполагают, что сбой обусловлен умышленным искажением части программы, например, наличием компьютерного вируса. При этом особое внимание должно быть уделено следующим аспектам:

- Записать симптомы и любые сообщения, появляющиеся на экране.
- Прекратить использование компьютера, при возможности изолировать его. Немедленно поставить в известность службу технической поддержки. Если оборудование подлежит осмотру, оно должно быть отключено от локальной сети организации до того, как на него вновь будет подано питание. Дискеты не должны передаваться на другие машины.
- Немедленно сообщить о происшествии в соответствующую службу.

Пользователи не должны ни при каких обстоятельствах не пытаться изъять подозрительные программы. Восстановление должно производиться опытным персоналом, имеющим соответствующую подготовку.

1.8.4. Процедуры дисциплинарного воздействия

Должны существовать официальные процедуры дисциплинарного воздействия в отношении сотрудников, нарушивших правила и процедуры политики безопасности в организации. Наличие таких процедур будет сдерживать служащих, которых могут склонить к нарушению процедур обеспечения безопасности. Кроме того, они должны обеспечивать корректное и справедливое обращение со служащими, подозреваемыми в совершении серьезных или неоднократных нарушений требований безопасности. Процедуры дисциплинарного воздействия должны разрабатываться под руководством специалиста по кадрам (юриста) и согласовываться с руководством организации.

2. Основные положения теории защиты информации

"Если, рассуждая о природе богов и происхождении вселенной, мы не достигнем желанной нашему уму цели, то в этом нет ничего удивительного, поскольку следует помнить, что и я, говорящий, и вы судьи – всего лишь люди; так что если наши соображения будут правдоподобны, не следует стремиться ни к чему больше».

Платон

"Я сделал как мог, и пусть, кто может – сделает лучше».

Древние римляне

2.1. Введение

Теория защиты информации определяется как система основных идей, относящихся к защите информации в современных системах ее обработки, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

В приведенном определении уже содержатся общие сведения о задачах теории защиты, в более же развернутом виде теория защиты должна:

1) предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты;

2) полно и адекватно отображать структуру и содержание взаимосвязей с родственными и смежными областями знаний;

3) аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации;

4) ориентировать в направлении наиболее эффективного решения основных задач защиты и предоставлять необходимые для этого научно-методологические и инструментальные средства;

5) формировать научно обоснованные перспективные направления развития теории и практики защиты информации.

Сформулированным выше целевым назначением теории защиты предопределяется ее состав и общее содержание. Составными частями ее, очевидно, должны быть:

1) полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;

2) систематизированные результаты ретроспективного анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты, полно и адекватно отображающие наиболее устойчивые тенденции в этом развитии;

3) научно обоснованная постановка задачи защиты информации в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в защите информации и объективные предпосылки удовлетворения;

4) общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;

5) методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;

6) методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;

7) научно обоснованные предложения по организации и обеспечению работ по защите информации;

8) научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

Приведенный перечень составных частей даже при таком очень общем представлении их содержания предметно свидетельствует о большом объеме и многоаспектности теории защиты, что, естественно, порождает значительные трудности ее формирования. Эти трудности усугубляются еще тем, что проблема защиты информации относится к числу сравнительно новых, причем по мере развития исследований, разработок и практической их реализации появляются новые аспекты, защита информации представляется все более комплексной и все более масштабной проблемой. Существенное влияние оказывает также неординарность проблемы защиты, наиболее значимым фактором которой является повышенное влияние на процессы защиты случайных трудно предсказуемых событий. Всем изложенным предопределяется настоятельная необходимость выбора и обоснования методологических принципов формирования самой теории защиты.

2.2. Возникновение и история развития проблемы защиты информации

Проблема защиты информации, вообще говоря, имеет многовековую историю. Ведь даже наскальные рисунки (не говоря уже о древних рукописях) есть не что иное, как попытка сохранить информацию о реалиях объективного мира. Применение же специальных мер в целях сохранения информации в тайне практиковалось еще в древние времена: достоверно, например, известно, что выдающийся политический деятель и полководец Древнего Рима Цезарь использовал для этих целей криптографическое преобразование текстов сообщений (вошедшее в историю под названием шифра Цезаря), хотя по современным представлениям весьма примитивное.

Но поскольку здесь рассматриваются вопросы защиты информации в автоматизированных системах ее обработки, то и ретроспективный анализ их происхождения и развития будем производить на глубину реального существования этих систем. В ведущих, с точки зрения информатизации, странах (прежде всего США) рассматриваемая проблема находится в центре внимания специалистов и интенсивно разрабатывается уже более 30 лет. Достаточно красноречивым свидетельством этого внимания может служить тот факт, что число публикаций по различным аспектам защиты информации только в открытой печати исчисляется многими тысячами, причем среди них многие десятки – это публикации монографического характера. Издаются специальные журналы, регулярно проводятся конференции, соответствующие дисциплины включены в учебные планы всех вузов, готовящих специалистов по вычислительной технике и ее использованию.

Прежде всего, специалисты единодушны в оценке чрезвычайной важности проблемы защиты, причем в подтверждение приводятся многочисленные конкретные факты злоумышленных действий над информацией, находящейся в КИС. Последствия таких действий нередко были достаточно тяжелы.

Под воздействием указанных выше фактов и в связи с расширяющейся открытостью, в последние годы резко возрос интерес к проблеме защиты информации в КИС, а соответствующие работы ведутся широким фронтом и с растущей интенсификацией. Свидетельством сказанному служат следующие факты:

1. Непрерывно растет число публикаций в открытой печати, среди которых имеются достаточно серьезные монографии.
2. Регулярно проводятся специальные конференции и семинары.
3. Издаются специализированные журналы.
4. Организована регулярная подготовка, повышение и оценка уровня квалификации (сертификация) профессиональных специалистов по защите информации.

Основой научно-методологического базиса, создающего объективные предпосылки для решения всей совокупности задач защиты информации на регулярной основе является так называемый системно-концептуальный подход, характерные особенности которого состоят в следующем:

1. Полный учет особенностей существующих и перспективных концепций построения, организации и обеспечения функционирования КИС.
2. Системный учет всей совокупности потенциально возможных дестабилизирующих факторов, влияющих на защищенность информации.
3. Наиболее полный учет имеющихся и перспективных возможностей (способов, методов, средств) защиты информации.
4. Разработка унифицированных подходов к формированию перечня, способов, методов и средств решения задач защиты.

Рассмотрим теперь развитие методологических подходов к организации и обеспечению защиты информации.

Естественно, что за истекшее после возникновения проблемы время существенно изменилось как представление о ее сущности, так и методологические подходы к решению. Указанные изменения происходили постепенно и непрерывно, поэтому всякая периодизация этого процесса в значительной мере будет носить искусственный характер. Тем не менее относительно подходов к защите информации весь период активных работ по рассматриваемой проблеме довольно четко делится на три этапа, которые условно можно назвать начальным, развитым и комплексным.

Начальный этап защиты характеризовался тем, что под защитой информации (защитой информации содержащей сведения составляющие тайну) понималось предупреждение несанкционированного ее получения лицами или процессами (задачами), не имеющими на это полномочий, и для этого использовались формальные (т.е. функционирующие без участия человека) средства. Наиболее распространенными механизмами защиты были проверки по паролю прав на доступ к КИС (цель – предупредить доступ незарегистрированных пользователей) и разграничение доступа к массивам (базам) данных (цель – предупредить доступ зарегистрированных пользователей к данным, находящимся за пределами их полномочий).

Проверка прав на доступ по паролю заключалась в том, что каждому зарегистрированному пользователю предоставлялся персональный пароль (некоторый набор символов из вполне определенного алфавита), все пароли хранились в защищенной области ЗУ, доступ пользователя к КИС разрешался только тогда, когда предъявленный им пароль совпадал с хранящимся в ЗУ. Основное достоинство данного механизма в его простоте, основной недостаток – низкая надежность: короткие пароли можно разгадать простым перебором возможных комбинаций, длинные – трудно запоминать; кроме того, искусный злоумышленник при определенных усилиях проникал в ту область ЗУ, в которой хранились эталонные пароли. В целях повышения надежности проверки прав разработаны следующие меры: увеличение длины алфавита, из которого формировались пароли; использование нескольких паролей; шифрование эталонных паролей и др.

Разграничение доступа к массивам (базам) данных осуществлялось несколькими способами: разделением массивов (баз) на зоны по степени секретности с предоставлением каждому пользователю соответствующего уровня доступа; по выдаваемым пользователям мандатам, в которых указывались идентификаторы тех элементов массивов (баз) данных, к которым им разрешался доступ; по специально составленной матрице полномочий, по строкам которой размещались идентификаторы пользователей, по столбцам – идентификаторы элементов массивов (баз) данных, а на пересечении строк и столбцов – условное обозначение прав соответствующего пользователя относительно соответствующего элемента данных (доступ запрещен, разрешено читать, записывать, то и другое и т.п.). Механизмы разграничения доступа оказались достаточно эффективными и настолько необходимыми, что в той или иной модификации используются до настоящего времени, и будут использоваться и в будущем.

Рассмотренные механизмы защиты реализовывались с помощью специальных программ, которые выполняли свои функции под управлением операционной системы защищаемой ЭВМ. Но для обеспечения эффективного их функционирования необходимы специальные организационные мероприятия: генерирование и распределение паролей, внесение эталонных паролей в ЗУ ЭВМ, формирование и ведение реквизитов разграничения доступа, общая организация защиты и др.

Общая оценка механизмов начального этапа защиты сводится к тому, что они обеспечили определенный уровень защиты, однако проблему в целом не решили, поскольку опытные злоумышленники находили способы и пути их преодоления.

Наиболее серьезной попыткой решения проблем защиты информации на принципиальных подходах первого этапа была программа разработки так называемой системы безопасности ресурса (СВР), выполнявшаяся по заданию одного из военных ведомств США. В соответствии с заданием СВР должна была представлять собою операционную систему для используемых ЭВМ, содержащую такие механизмы, которые обеспечивали бы высоконадежную защиту обрабатываемой информации от несанкционированного доступа в злоумышленных целях.
Основными механизмами защиты стали рассмотренное выше опознавание пользователей и разграничение доступа. В качестве обеспечивающих предусматривались механизмы контроля защиты и регистрации фактов несанкционированных действий.

Для того времени СВР была наиболее мошной системой защиты. Для ее проверки была создана специальная комиссия, которая испытывала ее в течение нескольких дней путем попыток несанкционированного проникновения к защищенной информации. Результаты проверки для СВР были неутешитель-

ны: значительное число попыток несанкционированного проникновения оказалось успешным, причем ряд этих проникновений не был обнаружен механизмами контроля и зафиксирован механизмами регистрации. В итоге заказывающее ведомство отказалось от практического применения СВР в своей работе.

Второй этап назван этапом развитой защиты, причем эта развитость определяется тремя характеристиками:

1. Постепенное осознание необходимости комплексирования целей защиты. Первым итогом на этом пути стало совместное решение задач обеспечения целостности информации и предупреждения несанкционированного ее получения.
2. Расширение арсенала используемых средств защиты, причем как по их количеству, так и по разнообразию. Повсеместное распространение получило комплексное применение технических, программных и организационных средств. Широко стала практиковаться защита информации путем криптографического ее преобразования. В целях регулирования правил защиты в ведущих странах установленным порядком стали приниматься специальные законодательные акты.
3. Все применяемые средства зашиты в КИС все более целенаправленно стали объединяться в функциональные самостоятельные системы (подсистемы) защиты.

Для иллюстрации размаха работ на втором этапе скажем, что только для решения задачи опознавания пользователей разрабатывались методы и средства, основанные на следующих признаках:

1. Традиционные пароли, но по усложненным процедурам.
2. Голос человека, поскольку он – индивидуальная характеристика.
3. Отпечатки пальцев, индивидуальность которых общеизвестна.
4. Геометрия руки, причем доказано, что по длине четырех пальцев руки человека можно опознать его с высокой степенью надежности.
5. Рисунок сетчатки глаза, который тоже является индивидуальной характеристикой человека.
6. Личная подпись человека, причем идентифицируемыми характеристиками служит графика написания букв, динамика подписи и давление пишущего инструмента.
7. Фотография человека.

В последнее время для рассматриваемых целей широко используются персональные карточки, содержащие идентифицирующую информацию, необходимую и достаточную для надежного опознавания человека.

Таким образом, второй этап может быть охарактеризован весьма интенсивными поисками, разработкой и реализацией способов, методов и средств защиты.

Третий этап назван этапом комплексной защиты, он приходит на смену второму, поэтому это этап будущего. Характерная его особенность заключается в попытках аналитико-синтетической обработки данных всего имеющегося опыта теоретических исследований и практического решения задач защиты и формирования на этой основе научно-методологического базиса защиты информации. Иными словами, основная задача третьего этапа – перевод всего дела защиты информации на строгую научную основу.

К настоящему времени в плане решения названной задачи уже разработаны основы целостной теории защиты информации, формирование этих основ может быть принято за начало третьего этапа в развитии методологии защиты.

Основные выводы, вытекающие из основ теории защиты, сводятся к следующему:

1. Защита информации в современных КИС должна быть комплексной как по целям защиты, так и по используемым способам, методам и средствам.
2. В целях создания условий для широкомасштабной оптимизации защиты должен быть разработан и обоснован набор стратегических подходов, полный в смысле учета всех потенциально возможных требований и условий защиты.
3. В целях создания объективных предпосылок для рациональной реализации любого стратегического подхода на регулярной основе должен быть разработан развитой и унифицированный методико-инструментальный базис, обеспечивающий высокоэффективное решение любого набора задач защиты.
4. Все перечисленные выше цели могут быть достигнуты лишь при том условии, что проблемы защиты информации будут решаться в органической взаимосвязи с проблемами информатизации основных сфер жизнедеятельности общества.

2.3. Методы исследования проблем защиты информации

Методологический базис составляют совокупности методов и моделей, необходимых и достаточных для исследований проблемы защиты и решения практических задач соответствующего назначения.

На формирование названных методов большое влияние оказывает тот факт, что процессы защиты информации подвержены сильному влиянию случайных факторов и особенно тех из них, которые связаны с злоумышленными действиями людей – нарушителей защищенности. Те же методы, стройная структура которых сформирована в классической теории систем, разрабатывались применительно к потребностям создания, организации и обеспечения функционирования технических, т.е. в основе своей формальных систем. Адекватность этих методов для удовлетворения указанных потребностей доказана практикой многих десятилетий. Но попытки применения методов классической теории систем к системам того типа, к которому относятся и системы защиты информации, с такой же убедительностью доказали их недостаточность для решения аналогичных задач в данных системах. В силу сказанного в качестве актуальной возникла задача расширения комплекса методов классической теории систем за счет включения в него таких методов, которые позволяют адекватно моделировать процессы, существенно зависящие от воздействия трудно предсказуемых факторов. К настоящему времени названная задача в какой-то мере решена, причем наиболее подходящими для указанных целей оказались методы нечетких множеств, лингвистических переменных (нестрогой математики), неформального оценивания, неформального поиска оптимальных решений.

Ниже в самом общем виде излагается существо названных методов. При этом имеется в виду, что для более детального их изучения читатели будут обращаться к специальным публикациям.

2.3.1. Основные положения теории нечетких множеств

Под **множеством** понимается любое объединение некоторых различных между собой объектов (элементов – угроз, уязвимостей, ресурсов), которые при решении соответствующей задачи должны (или могут) рассматриваться как единое целое. В теории множеств разработаны средства описания элементов множества, отношений между элементами и различных операций над элементами. Теория множеств уже стала классической, по ней имеются учебники и пособия различного уровня, поэтому излагать здесь ее основы нет необходимости.

Средства классической теории множеств могут найти эффективное применение при моделировании систем защиты информации. Однако в этой теории рассматриваются лишь детерминированные множества, по крайней мере, в плане принадлежности множеству заявленных его элементов. Иными словами, предполагается, что каждый элемент, указанный в перечне или в условиях формирования элементов, несомненно, принадлежит множеству, в то время как в системах защиты информации большую роль играют случайные факторы. Например, случайным является принадлежность многих каналов несанкционированного получения информации (КНПИ) к множеству КНПИ, потенциально возможных в том или ином компоненте КИС, принадлежность многих средств защиты к множеству средств, с помощью которых может быть эффективно перекрыт тот или иной КНПИ и т.п. Указанные элементы принадлежат соответствующим множествам лишь с некоторой вероятностью. Для описания таких систем в последние годы интенсивно развивается так называемая теория нечетких множеств. Имеются попытки использования методов данной теории для построения моделей систем защиты информации.

2.3.2. Основные положения нестрогой математики

Нестрогой математикой, или математикой здравого смысла (называемой еще теорией лингвистических переменных) будем называть совокупность приемов построения и использования моделей больших систем, основывающихся на неформальных суждениях и умозаключениях человека, формируемых им исходя из жизненного опыта и здравого смысла. Интерес к такой математике проявляется в последние годы в связи с все возрастающей актуальностью задач анализа и синтеза организационных систем, а также управления процессами их функционирования. Как известно, многие системы организационного типа характеризуются высоким уровнем неопределенности, в силу чего не удается построить адекватные им модели с помощью средств традиционных методов моделирования. Необходим аппарат с таким диапазоном представления и оперирования, который был бы адекватен уровню неопределенности моделируемых систем. Характерными примерами таких систем являются системы, основные цели функционирования которых определяются потребностями людей. Нестрогая математика и представляется как основа методологии моделирования таких систем. К сожалению, в имеющихся публикациях отсутствует системное изложение данной методологии.

Поскольку основной объект нашего изучения – системы защиты информации – относится к системам с весьма высоким уровнем неопределенности (нарушение статуса защищенности информации, как правило, обусловливается целями и действиями людей), то представляется целесообразным включить методологию нестрогой математики в арсенал средств, предназначаемых для использования при ре-

шении проблем защиты. Этим и обусловлено выделение данного вопроса в самостоятельный раздел методологических основ защиты информации.

Исходным базисом нестрогой математики служит совокупность трех посылок:

1) в качестве меры характеристик изучаемых систем вместо числовых переменных или в дополнение к ним используются лингвистические переменные. Если, например, нас интересует такая характеристика, как вероятность доступа нарушителя к защищаемой информации, то в лингвистическом измерении значениями этой характеристики могут быть: «крайне незначительная», «существенная», «достаточно высокая», «весьма высокая» и т.п.;

2) простые отношения между переменными в лингвистическом измерении описываются с помощью нечетких высказываний, которые имеют следующую структуру: «из А следует В», где А и В – переменные в лингвистическом измерении. Примером такого отношения может быть: «Если в системе охранной сигнализации вероятность отказов датчиков значительная, то для предупреждения проникновения на контролируемую территорию посторонних лиц интенсивность организационного контроля над этой территорией должна быть повышенной». Переменными здесь являются «вероятность отказов датчиков» и «интенсивность организационного контроля», а лингвистическими значениями – «значительная» и «повышенная» соответственно;

3) сложные отношения между переменными в лингвистическом измерении описываются нечеткими алгоритмами. В качестве примера рассмотрим нечеткий алгоритм сложного отношения между переменными: «надежность компонентов системы защиты информации» и «интенсивность контроля хранилища носителей защищаемой информации».

Совершенно очевидно, что интенсивность контроля хранилищ носителей должна быть тем больше, чем выше степень угрозы хищения носителей, находящихся в хранилище. Степень угрозы хищения в свою очередь зависит от надежности: защиты территории, на которой расположены хранилища (НТ); защиты помещений, в которых находятся хранилища (НП); замков на дверях хранилищ (НЗ); библиотекарей хранилищ (НБ). Если для интенсивности контроля хранилищ носителей и для каждого из названных четырех параметров, влияющих на эту интенсивность, принять три возможных значения (малая (М), средняя (С), большая (Б)), то нечеткий алгоритм решения рассматриваемой задачи может быть представлен так, как показано на рис. 2.1.

Нетрудно видеть, что аппарат нестрогой математики может быть рекомендован для использования в таких ситуациях, в которых строгое описание систем и процессов их функционирования или невозможно или нецелесообразно в силу самого характера решаемой задачи. Так, в настоящее время нет необходимых данных для строгого определения значений параметров, определяющих степень уязвимости информации в КИС, эффективность систем защиты информации и т.п.

Вполне реальными являются также такие условия, когда строго количественные алгоритмы оценки ситуации и принятия решений являются нецелесообразными и даже вредными. Например, вряд ли целесообразно (по крайней мере, в настоящее время) пытаться строить строгий алгоритм для обеспечения выработки общей стратегии защиты информации. Построение такого алгоритма сопряжено с трудностями, преодоление которых неизбежно требует таких допущений, что адекватность этих алгоритмов становится весьма сомнительной. В то же время на основе чисто интуитивных рассуждений квалифицированных и опытных специалистов можно построить нечеткие (в указанном выше смысле) алгоритмы, которые, с одной стороны, будут достаточно простыми и адекватными реальным процессам, а с другой – создавать хорошие предпосылки для эффективного решения важных задач.

Нецелесообразность построения строгих алгоритмов может иметь место, например, в следующих ситуациях: реализация строгого алгоритма является трудоемкой, а время на его реализацию крайне ограничено; множество возможных ситуаций слишком велико, а возможности для их рассмотрения ограничены; поступающая информация такого качества, что результаты реализации строгого алгоритма являются сомнительными и т.п. В таких ситуациях, очевидно, целесообразным будет построение некоторых обобщенных алгоритмов, которые создадут предпосылки для наиболее рационального принятия решений в потенциально возможных ситуациях.

Именно такие подходы будут здесь использованы при обосновании рациональной технологии управления защитой информации, организации работ по защите информации и др.

Необходимо, однако, обратить внимание на следующее обстоятельство. При изложении вопросов практического использования методов нестрогой математики каждый раз акцентировалось внимание на том, что эти методы лишь создают предпосылки, необходимые для эффективного решения соот-

ветствующей задачи, но не гарантируют эффективного решения. Такая гарантия может быть обеспечена лишь рациональными действиями людей, использующих нечеткие алгоритмы. Отсюда следует, что организация функционирования систем с высоким уровнем неопределенности должна включать в себя (и притом в качестве важнейшего атрибута) подготовку людей (персонала) к решению соответствующих задач с использованием методов нестрогой математики.

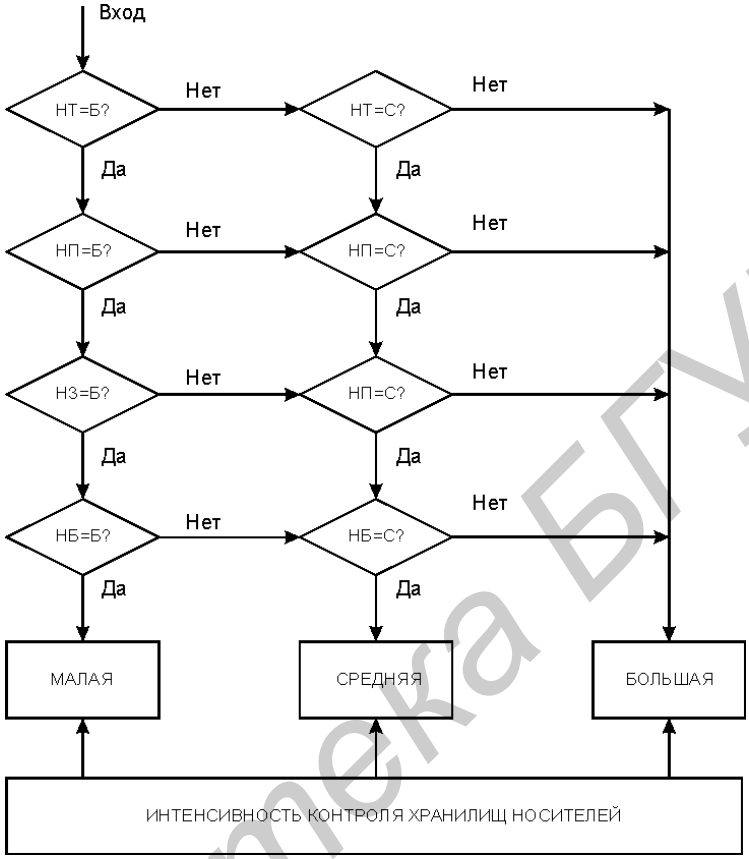

Рис. 2.1. Структура нечеткого алгоритма определения интенсивности контроля хранилищ носителей

И, наконец, о соотношении методологии нестрогой математики и методологии теории нечетких множеств. При внимательном рассмотрении обеих названных методологий нетрудно усмотреть достаточно глубокую их аналогию. Объективным основанием для этого является то обстоятельство, что в основе обеих методологий лежит представление о неопределенности, размытости границ принадлежности элементов (представлений, суждений) определенному множеству. Однако существуют и принципиальные различия рассматриваемых методологий. В теории нечетких множеств, во-первых, предусматривается количественная оценка меры принадлежности рассматриваемых элементов тому или иному множеству, а во-вторых, предполагается разработка строгого алгоритма решения соответствующей задачи. В нестрогой математике нечеткость рассуждений последовательно проводится вплоть до алгоритма решения соответствующей задачи.

2.3.3. Неформальные методы оценивания

В процессе моделирования больших систем неизбежно приходится оценивать значения различных параметров этих систем. Значения некоторых параметров удается непосредственно измерить (например, геометрические характеристики доступных предметов, отрезки времени и т.п.) или вычислить по известным аналитическим зависимостям (например, вероятность сложного события по вероятностям составляющих его событий, площади геометрических фигур по известным их размерам и т.п.). Если имеются данные о функционировании моделируемой системы или ее аналога за достаточно продолжительное время, то значения некоторых параметров можно определить путем статистической обработки их значений, зафиксированных в процессе наблюдения. Общеизвестные методы математической статистики позволяют не только определить текущее значение параметра, но и оценить досто-

верность такого определения в зависимости от продолжительности (числа) наблюдений и их совпадения (разброса), установить необходимое число наблюдений для определения значения параметра с заданной точностью.

Иногда значения интересующих параметров удается определить по аналогии со значениями других, схожих с определяемыми, значения которых известны.

Однако нередки случаи, когда значения параметров моделируемых систем не удается получить названными выше методами. Такая ситуация бывает особенно характерной для систем с высоким уровнем неопределенности и не имеющих достаточной предыстории функционирования. Именно такими являются рассматриваемые здесь системы защиты информации. Например, в настоящее время нет данных, необходимых для определения таких параметров, как вероятности проявления дестабилизирующих факторов в различных КИС и различных условиях их функционирования, вероятности успешного использования злоумышленником проявившихся дестабилизирующих факторов, показатели эффективности функционирования различных средств защиты и многих других. В таких случаях неизбежно приходится пользоваться неформальными методами оценивания, основанными на оценках людей – специалистов в соответствующей сфере.

Из неформальных методов оценивания наиболее известными являются методы экспертных оценок. Экспертными оценками называются такие методы поиска решений сложных, не поддающихся формализации задач, которые основаны на суждениях (оценках, высказываниях) специально выбираемых (назначаемых) экспертов. Эти методы достаточно просты по своей сущности, они нашли широкое отражение в специальной литературе. Последовательность и содержание решения задач методами экспертных оценок в самом общем виде могут быть представлены следующим образом: разработка постановки задачи; обоснование перечня и содержания тех параметров задачи, для определения значений которых целесообразно использовать экспертные оценки; обоснование форм и способов экспертных оценок; разработка реквизитов (бланков, инструкций и т.п.), необходимых для проведения экспертных оценок; подбор и подготовка (обучение, инструктаж) экспертов, привлекаемых для решения задачи; организация и обеспечение работы экспертов; контроль и первичная обработка экспертных оценок; базовая обработка экспертных оценок.

По способам привлечения экспертов к решению задач различают: простые суждения, интервьюирование и анкетирование. При использовании метода простых суждений эксперт устно или письменно высказывается по поставленному вопросу, при интервьюировании каждый эксперт устно или письменно отвечает (в диалоговом режиме) на серию вопросов, которые ставит организатор экспертизы, при анкетировании каждый эксперт отвечает письменно на вопросы, содержащиеся в заблаговременно составляемых одной или нескольких анкетах.

Принципиально важным для методов экспертных оценок является получение такой выборки оценок экспертов, на которой статистически устойчиво проявилось бы их общее мнение по решаемой проблеме. Отсюда одно из основных требований и одна из основных трудностей состоят в подборе такого количества компетентных экспертов, которого достаточно для получения статистически устойчивых решений. Однако при этом возникает серьезный вопрос о соизмерении компетентности различных экспертов по решаемой проблеме. Для решения этого вопроса в подавляющем большинстве существующих методик экспертных оценок вводится так называемый коэффициент компетентности, представляющий собою число в интервале от 0 до 1, причем оценке каждого эксперта присваивается вес, равный этому коэффициенту. Значение коэффициента компетентности определяется либо самим экспертом (самооценка) либо коллегами по экспертизе (взаимная оценка). В некоторых случаях используются одновременно обе оценки.

Технология использования методов экспертных оценок представляет собой последовательность следующих операций:

1) Формирование достаточно представительной группы компетентных экспертов.

2) Выбор способа организации работы с экспертами.

3) Выбор метода формирования экспертами суждений (оценок) по решаемым вопросам и проведение экспертизы.

4) Выбор метода обработки оценок группы экспертов.

Ниже кратко излагаются возможные подходы к решению перечисленных задач.

1. Формирование группы экспертов. В решении данной задачи существенно значимыми представляются два вопроса: персональный подбор экспертов и формирование представительной их группы.

При персональном подборе экспертов рекомендуется руководствоваться следующей совокупностью критериев:

- *компетентность* – наличие знаний и опыта по решаемой проблеме;

- *креативность* – способность решать творческие задачи;
- *антиконформизм* – неподверженность влиянию авторитетов;
- *конструктивность мышления* – способность давать практически значимые решения;
- *коллективизм* – способность работать в коллективе в соответствии с общепризнанными этическими нормами поведения;
- *самокритичность* – способность критично относиться к собственной компетенции и своим суждениям;
- *наличие времени* для работы в экспертных группах;
- *заинтересованность* – наличие желания в решении рассматриваемой проблемы.

Численность группы должна быть достаточно представительной для того, чтобы на основе совокупной обработки их суждений можно было определить статистически устойчивую оценку. Считается, что группа должна иметь численность не менее 20 человек.

2. *Выбор способа работы с экспертами.* Наиболее эффективными способами работами с экспертами считаются интервьюирование и анкетирование. Первый способ заключается в том, что руководитель экспертизы последовательно берет интервью (в общепринятой интерпретации этого понятия) у экспертов, второй – в том, что каждый эксперт самостоятельно заполняет заблаговременно разработанную анкету. К достоинствам первого способа относится возможность уточнять по ходу интервью оценки эксперта, используя для этого подходы метода психоинтеллектуальной генерации), второго – возможность экспертам не только глубоко сосредоточиться на решаемой проблеме, но и дополнительного изучения проблемы. Названные способы могут комбинироваться: например, проводится предварительное интервьюирование экспертов, затем эксперты заполняют анкеты, после чего осуществляется заключительное интервьюирование в целях изучения мотивов экспертов относительно их оценок и возможного уточнения этих оценок.

3. *Выбор метода формирования экспертами оценок.* Данная задача относится к наиболее важным в общей процедуре экспертных оценок. Она заключается в решении двух подзадач: выбора формы выражения оценки и выбора способа ее формирования.

Форма выражения оценки может быть неявной и явной. Неявное выражение состоит в том, что эксперт ранжирует оцениваемые элементы (объекты, явления) по степени их важности (линейное ранжирование) или делит на группы с возможным ранжированием в группах (групповое ранжирование). При явном выражении эксперты дают элементам лингвистические или количественные оценки. При этом количественная оценка может выражаться коэффициентом (весом) на непрерывной шкале (чаще всего от 0 до 1) или баллом из предложенного множества (пять, десять и т.п.).

По способу формирования оценки могут быть непосредственными (эксперт определяет значение каждого оцениваемого элемента на заданной шкале) и сравнительными, формируемыми на основе сравнения пар оцениваемых элементов и означающими ту степень предпочтения (значимости), которая, по мнению эксперта, имеет место в условиях решаемой задачи.

4. *Выбор метода обработки результатов экспертизы.* В табл. 2.1 приведены примеры возможных конечных результатов для всех их разновидностей, образуемых рассмотренной выше классификационной структурой.

а) Оценки экспертов осуществляются в форме ранжирования. Пусть $r_{ij}\,(i=1,2,...,n;\ j=1,2,...,m)$ есть ранг, присвоенный *i*-му элементу *j*-м экспертом. Обработка результатов заключается в построении обобщенной ранжировки. Для этого вводится конечномерное дискретное пространство ранжировок и метрика этого пространства. Ранжировка каждого эксперта представляется точкой в данном пространстве, а обобщенная – такой точкой в нем, которая наилучшим образом согласуется с точками, являющимися ранжировками экспертов. Однако определение обобщенной ранжировки представляется чрезвычайно сложной процедурой, что существенно ограничивает возможности практической реализации. Поэтому излагать здесь эту процедуру не будем, заинтересованным рекомендуем обратиться к специальным публикациям.

Более простым является метод ранжирования по величинам сумм рангов, присвоенных каждому элементу всеми экспертами. В этих целях для матрицы $\|r_{ij}\|$ вычисляются величины

$$r_i = \sum_{j=1}^{m} r_{ij} \qquad (2.1)$$

$$i = 1,2,...,n$$

и элементы упорядочиваются по возрастанию величин r_i

Таблица 2.1

Классификация и возможные результаты разновидностей экспертных оценок

<table>
<tr><td colspan="3" rowspan="2">Форма выражения оценки</td><td colspan="2">Способ формирования оценки</td></tr>
<tr><td>Непосредственный</td><td>Сравнительный</td></tr>
<tr><td rowspan="2">Неявная</td><td colspan="2">Линейное ранжирование</td><td>Не имеет места</td><td>Последовательность элементов в соответствии с их рангами</td></tr>
<tr><td colspan="2">Групповое ранжирование</td><td>Не имеет места</td><td>Несколько последовательностей с расположением их по рангам</td></tr>
<tr><td rowspan="3">Явная</td><td rowspan="2">Количественная</td><td>На непрерывной шкале</td><td colspan="2" rowspan="2">1. Групповые оценки объектов, параметров, явлений
2. Веса оцениваемых элементов</td></tr>
<tr><td>Балльная</td></tr>
<tr><td colspan="2">Лингвистическая</td><td colspan="2">1. Согласованная лингвистическая оценка
2. Количественная оценка</td></tr>
</table>

б) Оценки экспертов осуществляются в количественном выражении по непрерывной шкале. Пусть $x_{ij}\,(i=1,2,...,n;\ j=1,2,...,m)$ есть оценка *i*-го элемента *j*-м экспертом. Тогда в самом простом случае групповая оценка определяется как среднее арифметическое оценок экспертов, т.е.

$$x_i = \left(\sum_{j=1}^{m} x_{ij}\right) / m\,. \tag{2.2}$$

Для более точного определения x_i вводится понятие весов оценок экспертов как некоторой меры близости их к групповой оценке. В этом случае групповая оценка вычисляется по рекуррентной процедуре, имеющей вид:

$$x_i^t = \sum_{i=1}^{m} x_{ij} \cdot K_j^{t-1} \tag{2.3}$$

$$j = 1,2,...,n; t = 1,2...$$

$$K_j^t = \frac{\sum_{i=1}^{n} x_{ij} \cdot x_j^t}{\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij} \cdot x_i^t}, \tag{2.4}$$

$$i = 1,2,...,n;\ j = 1,2,...,m$$

$$K_0 = \frac{1}{m} \cdot$$

Доказано, что сходимость этой процедуры обеспечивается практически во всех случаях.

Заметим, однако, что приведенная рекуррентная процедура справедлива лишь для случая нормированных оценок группы взаимооцениваемых элементов. В случае же ненормированных оценок или независимого оценивания отдельных элементов групповая оценка может быть вычислена по такой (тоже рекуррентной) процедуре:

$$x_i^t = \left(\sum_{i=1}^{m} x_{ij} \right) \cdot K_j^{t-1} \quad . \tag{2.5}$$

$$K_j^t = 1 - \frac{\left| x_{ij} \cdot x_i^t \right|^2}{\sum_{j=1}^{m} \left| x_{ij} \cdot x_i^t \right|^2}, \tag{2.6}$$

$$K_0 = \frac{1}{m}.$$

в) Оценки экспертов осуществляются в количественном выражении по способу парных сравнений. Пусть $\frac{W_i}{W_{i'}} i = 1,2,...,n; j = 1,2,...,m$ есть степень предпочтения i-го элемента над элементом i', оцененная j-*м* экспертом. Степени предпочтения всех элементов относительно всех других образуют квадратную матрицу $\left\| \frac{W_i}{W_{i'}} \right\|_j$. Такую матрицу формирует каждый эксперт. Обработка каждой матрицы осуществляется в такой последовательности:

1-й шаг – вычисляются значения собственных векторов строк матрицы:

$$a_{ij} = \sqrt[n]{\prod_{i=1}^{n} \left(\frac{W_i}{W_{i'}} \right)_j}. \tag{2.7}$$

$$i = 1,2,...,n; j = 1,2,...,m.$$

2-й шаг – вычисляются нормированные значения собственных векторов:

$$\overline{x_{ij}} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}}, \tag{2.8}$$

$$i = 1,2,...,n; j = 1,2,...,m \ .$$

Вектор $\overline{x_{ij}}$ называется вектором приоритетов j-го эксперта.

3-й шаг – вычисляются значения локальных приоритетов каждого эксперта:

$$y_{ij} = \left(\frac{W_i}{W_1} \right)_j \cdot x_{1j} + \left(\frac{W_i}{W_2} \right)_j \cdot x_{2j} + ... + \left(\frac{W_i}{W_n} \right)_j \cdot x_{nj}, \tag{2.9}$$

$$i = 1,2,...,n; j = 1,2,...,m.$$

4-й шаг – на основе величин y_{ij} по процедуре, изложенной в пункте «б», определяются значения групповых оценок $y_i (i = 1,2,...,n)$.

г) Оценки экспертов осуществляются в балльном выражении. Пусть b_{ij} есть балл, присвоенный i-му элементу j-м экспертом. Тогда коэффициент относительной важности i-го элемента определяется по следующей зависимости:

$$B_i = \frac{\sum_{j=1}^{m} b_{ij}}{\sum_{i=1}^{n} \sum_{j=1}^{m} b_{ij}}. \tag{2.10}$$

Нетрудно видеть, что в данном случае может быть построена рекуррентная процедура аналогично тому, как это представлено выше в п. «б».

д) Оценки экспертов осуществляются в лингвистическом выражении. Как показано в табл. 2.1, в данном случае могут быть получены две групповые оценки: лингвистические значения оцениваемых элементов и/или количественная оценка.

Лингвистические оценки могут быть получены процедурой «голосования», т.е. выбором того значения, которое дано большинством экспертов. Для элементов повышенной значимости может быть использовано правило квалифицированного большинства ("за» – не менее 75% оценок экспертов).

Количественная групповая оценка по совокупности оценок лингвистических может быть определена следующим образом. Пусть, например, каждому эксперту предлагается дать лингвистическую оценку требуемого уровня защиты информации на конкретном объекте одним из следующих значений: 1) не нужна; 2) невысокая, 3) средняя, 4) высокая, 5) очень высокая. Кроме этого, каждый эксперт приводит тот диапазон на шкале 0–1, в котором, по его мнению, находится его оценка. Тогда в качестве количественной его оценки может быть принята середина указанного интервала, а затем оценки всех экспертов могут быть обработаны по методике, рассмотренной в п. «б».

Такая лингвистико-количественная экспертиза особенно целесообразна в тех случаях, когда оценке подвергается сложное многофакторное событие с высоким уровнем неопределенности.

2.3.4. Неформальные методы поиска оптимальных решений

Решение проблем защиты информации связано с поиском оптимальных решений, т.е. таких вариантов действий, которые при заданных затратах ресурсов обеспечивают максимальную эффективность процессов или достижение заданной эффективности процессов при минимальных затратах ресурсов.

Процедуры поиска оптимальных решений являются наиболее сложными процедурами, осуществляемыми при создании, организации и обеспечении функционирования больших систем, поэтому разработке методологии поиска оптимальных решений в различных ситуациях уделяется повышенное внимание. К настоящему времени разработан достаточно представительный арсенал методов поиска оптимальных решений в самых различных ситуациях. Практическая реализация подавляющего большинства методов сопряжена с осуществлением значительного объема сложных расчетов, поэтому регулярное и интенсивное их развитие началось лишь после появления ЭВМ. Вполне естественно поэтому, что развивались главным образом те методы, которые могли быть реализованы конечными алгоритмами. Данному условию отвечают далеко не все методы, а те, которые ему отвечают, позволяют решать далеко не все оптимизационные задачи, с которыми приходится встречаться на практике. Особенно трудными для реализации являются те задачи, в постановке которых имеются неопределенности. А именно такие задачи возникают при решении проблем защиты информации в КИС. В связи с этим особый интерес представляют развиваемые в последние годы неформальные методы поиска оптимальных решений. При этом обозначилось два направления использования неформальных методов в решении оптимизационных задач:

- сведение сложной неформальной задачи к формальной постановке в целях использования уже реализованных формальных методов;
- неформальный поиск оптимального решения, т.е. непосредственная реализация процедуры поиска.

Классификационная структура методов приведена на рис. 2.2.

Сведение неформальной задачи к формальной постановке заключается в формировании строго выраженных условий задачи, т.е. подлежащих поиску Переменных, ограничений, которым должны удовлетворять переменные, и целевой функции, подлежащей максимизации или минимизации в процессе поиска оптимального решения. Для этих целей, как показано на рисунке, могут использоваться методы теории нечетких множеств, эвристическое программирование и эволюционное моделирование.

Методы теории нечетких множеств позволяют получать аналитические выражения для количественных оценок нечетких условий принадлежности элементов к тому или иному множеству и тем самым сводить постановки неопределенных задач к строго определенным. При наличии же строгих постановок для решения задачи могут быть использованы соответствующие конечные методы, которые, как известно, гарантируют поиск оптимальных решений.

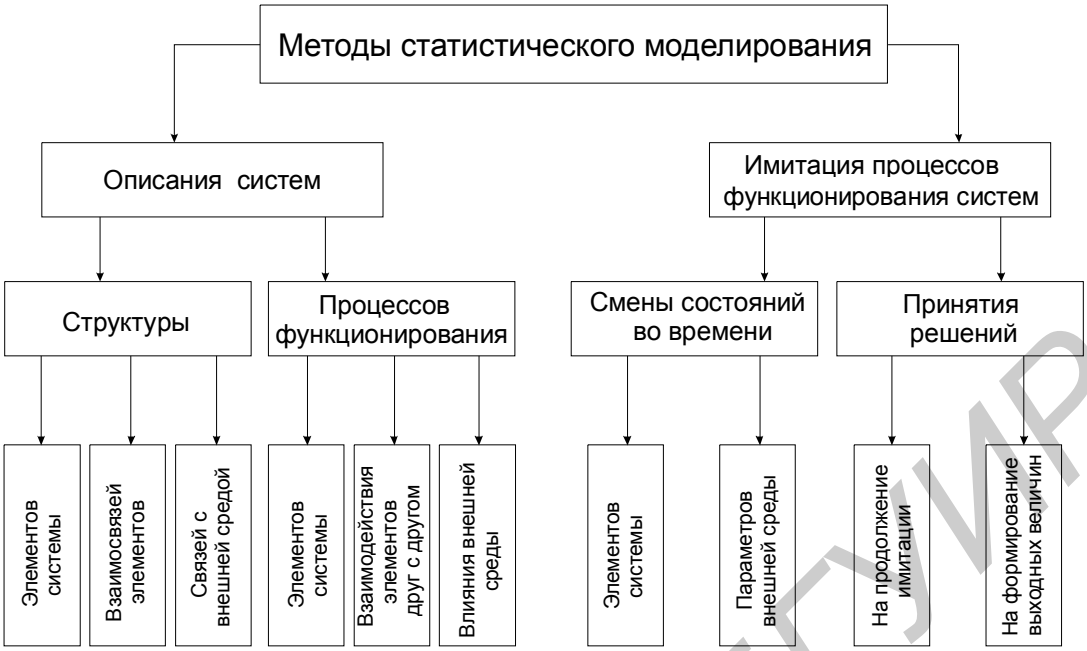

Рис. 2.2. Классификационная структура методов поиска оптимальных решений

Эвристическим программированием названы такие методы поиска оптимальных решений, основу которых составляют формализованные (т.е. представленные в виде конечного алгоритма) эвристики. Под эвристикой (эвристическим правилом, эвристическим методом) принято понимать правило, стратегию или просто ловкий прием, найденные человеком на основе своего опыта, имеющихся знаний и интуиции, и позволяющие наиболее эффективно решать некоторый класс слабоструктурированных задач. Найденные таким образом эвристики подвергаются формализации с целью представления их в виде конечного алгоритма, который можно реализовать на ЭВМ.

Таким образом, схема разработки методов эвристического программирования в обобщенном виде может быть представлена следующей последовательностью процедур: изучение содержания соответствующего класса слабоструктурированных задач; изучение приемов решения задач данного класса человеком; выявление закономерностей в решении человеком задач рассматриваемого класса; формализация выявленных закономерностей, приемов и правил и построение на этой основе модели решения задач данного класса; алгоритмическая реализация построенной модели.

Принципиальным моментом является то, что методы эвристического программирования вовсе не гарантируют получения строго оптимальных решений. Более того, не исключаются даже случаи, когда полученное на основе эвристической модели решение будет далеко от оптимального. Единственное, что гарантируют эти методы – это, во-первых, что решение непременно будет найдено, и, во-вторых, что найденное решение будет лучшим среди решений, получаемых без использования эвристик.

Регулярная теория построения эвристических моделей до настоящего времени в полной мере не разработана. Наиболее правдоподобной представляется следующая интерпретация принципиальных отличий эвристического поиска от поиска по конечным формальным методам. В процессе решения задачи строго формальными методами поле поиска (область допустимых решений) остается неизменным. Сам процесс решения заключается в прямом, направленном или случайном переборе возможных решений. Для эвристических же методов характерно, с одной стороны, сужение поля поиска (области допустимых решений) за счет исключения из рассмотрения подобластей заведомо непригодных решений, а с другой – расширение поля поиска за счет генерирования новых подобластей. Из конкретных методологий, реализующих данное представление об эвристиках, наибольшее распространение получили так называемые лабиринтные и концептуальные эвристики.

Согласно лабиринтной модели задача перед решением представляется в виде лабиринта возможных путей поиска решения, ведущих от начальной площадки, характеризующей условия задачи, к конечной, характеризующей условия завершения решения задачи. Предполагается, что благодаря своим

природным механизмам мышления человек способен очень быстро произвести отсекание всех неперспективных вариантов движения по лабиринту и оставить то поле возможных вариантов, которое с большой вероятностью содержит путь, ведущий к конечной площадке.

Основным механизмом поиска решения в концептуальных эвристиках считается генерирование множества таких путей решения задачи, среди которых с большой вероятностью содержится и результативный путь. Концептуальная теория рассматривает механизм получения решения в следующем виде. При анализе исходной ситуации и соотнесении ее с результирующей человек не просто собирает информацию, необходимую для решения задачи, а строит (даже не осознавая этого) структурированную модель проблемной ситуации, вычленяя в исходной информации важные элементы и формируя на их основе обобщенные элементы и отношения между ними. Такие обобщенные элементы и отношения названы концептами, откуда получила название и сама рассматриваемая теория. Концепты играют основную роль в осмысливании исходной ситуации, создании ее модели и мысленной работе с моделью. Согласно концептуальной теории набор концептов универсален, и ему соответствуют имеющиеся у человека механизмы вычисления, трансформации и формирования отношений. В результате мысленного эксперимента со структурированной моделью ситуации человек получает возможность породить тот небольшой участок лабиринта, в котором уже нетрудно найти необходимое решение.

Эволюционное моделирование представляет собою расширенную модификацию статистического моделирования, причем расширение заключается в том, что в процессе моделирования статистически совершенствуется (прогрессивно эволюционирует) сам алгоритм, в соответствии с которым имитируются процессы функционирования моделируемых систем. Иными словами, как бы моделируются процессы естественной эволюции. Общая схема процесса эволюционного моделирования представлена на рис. 2.3.

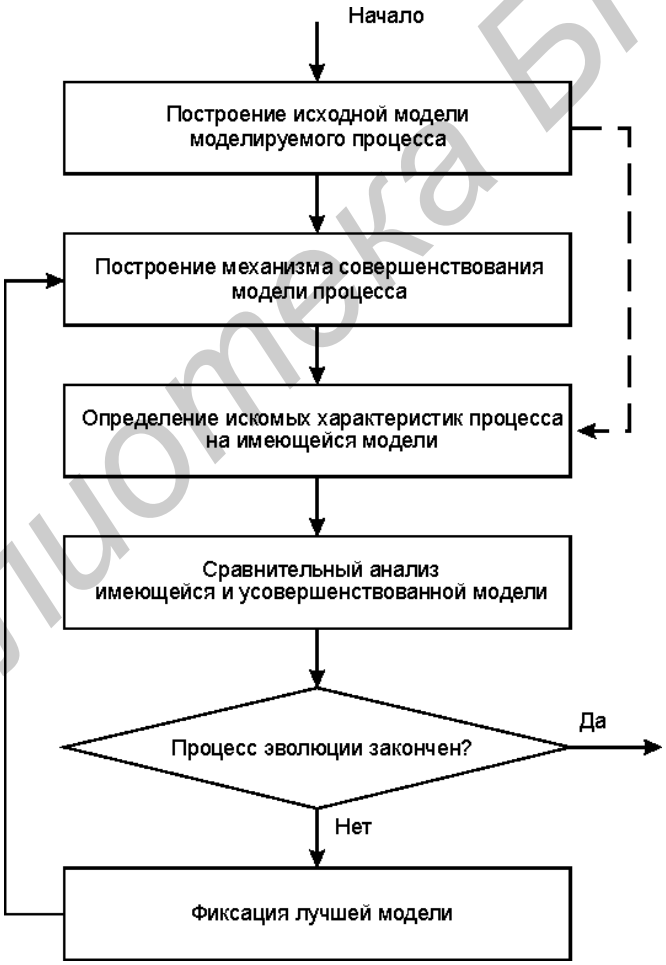

Рис. 2.3. Общая схема эволюционного моделирования

Из неформальных методов непосредственного поиска оптимальных решений, как показано на рис. 2.2., к настоящему времени разработаны и могут быть рекомендованы для практического применения методы простых экспертных оценок, неформально-эвристического программирования и методы, осно-

ванные на управлении продуктивным мышлением человека непосредственно в процессе решения задачи.

Методы простых экспертных оценок были рассмотрены выше. Использование их естественным образом распространяется и на задачи поиска оптимальных решений, если только процесс поиска может быть ограничен простой оценкой.

Под неформально-эвристическим понимается такая разновидность эвристического программирования, когда человек принимает непосредственное участие не только в процессах составления моделей для поиска решений, но также в их обучении (т.е. подготовке к решению задач в конкретных условиях) и в процессах непосредственного решения конкретных задач. Одной из разновидностей неформально-эвристического программирования являются так называемые неформальные аналоги, т.е. поиск решения человеком на основе тех прецедентов решения аналогичных задач, которые имели место в предшествующей личной практике или практике других специалистов.

Последнюю группу выделенных на рис. 2.2 неформально-эвристических методов непосредственного поиска оптимальных решений составляют методы, основанные на управлении продуктивным мышлением человека непосредственно в процессе самого поиска.

К настоящему времени наибольшее развитие получили две разновидности методологии управления интеллектуальной деятельностью: метод так называемого мозгового штурма и метод психоинтеллектуальной генерации.

"Мозговой штурм» представляет собой метод получения новых идей, решений в процессе коллективного творчества группы экспертов, проводимого по определенным правилам. Метод «мозгового штурма» называют также «мозговой атакой», методом коллективной генерации идей и методом группового рассмотрения с отнесенной оценкой.

Принципиальной особенностью метода является абсолютное исключение в ходе самого сеанса критики и вообще какой-либо оценки высказываемых идей. Сама сущность метода состоит в разделении во времени решения двух задач: генерирования новых идей и анализа (оценки) этих идей, для чего даже создаются две разные группы экспертов: генераторов идей и аналитиков.

Процесс поиска решения по методу психоинтеллектуальной генерации осуществляется в виде целенаправленно управляемой беседы-дискуссии двух непременных участников – ведущего и решающего. Ведущий ставит решающему вопросы (проблемы), по которым последний высказывает свои суждения. Вокруг этих суждений и завязывается дискуссия, направляемая ведущим на возможно более полное и глубокое рассмотрение проблемы. В помощь ведущему могут выделяться оппонент и эксперты. Задача оппонента заключается в поиске слабых мест в суждениях решающего и формировании возражений и критических замечаний с тем, чтобы как можно энергичнее побудить его к дискуссии (преднамеренное вовлечение в дискуссию). Эксперты помогают ведущему оценивать высказываемые суждения и намечать последовательность и содержание дальнейшего обсуждения проблемы. Среди всех высказываний решающего отыскиваются наилучшие решения обсуждаемой проблемы.

2.4. Угрозы безопасности автоматизированной системы обработки информации

К настоящему времени известно большое количество разноплановых угроз различного происхождения, таящих в себе различную опасность для информации. Системная их классификация приведена в табл.2.2.

Ниже приводится краткий комментарий к приведенным в табл.2.2 параметрам классификации, их значениям и содержанию.

1. Виды угроз. Данный параметр является основополагающим, определяющим целевую направленность защиты информации.

2. Происхождение угроз. В табл. 2.2 выделено два значения данного параметра: случайное и преднамеренное. При этом под случайным понимается такое происхождение угроз, которое обусловливается спонтанными и не зависящими от воли людей обстоятельствами, возникающими в системе обработки данных в процессе ее функционирования. Наиболее известными событиями данного плана яв-

ляются отказы, сбои, ошибки, стихийные бедствия и побочные влияния. Сущность перечисленных событий определяется следующим образом:

а) отказ – нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций;

б) сбой – временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

в) ошибка – неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

г) побочное влияние – негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обусловливается злоумышленными действиями людей, осуществляемыми в целях реализации одного или нескольких видов угроз.

3. Предпосылки появления угроз. В табл. 2.2 названы две разновидности предпосылок: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведывательных органов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, злоумышленные действия недобросовестных сотрудников системы). Перечисленные разновидности предпосылок интерпретируются следующим образом:

а) количественная недостаточность – физическая нехватка одного или несколько элементов системы обработки данных, вызывающая нарушения технологического процесса обработки или/и перегрузку имеющихся элементов;

б) качественная недостаточность – несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

в) деятельность разведывательных органов иностранных государств – специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами. К основным видам разведки относятся агентурная (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых доброжелателей) и техническая, включающая радиоразведку (перехват радиосредствами информации, циркулирующей в радиоканалах систем связи), радиотехническую (регистрацию спецсредствами сигналов, излучаемых техническими системами) и космическую (использование космических кораблей и искусственных спутников для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации другими доступными способами;

г) промышленный шпионаж – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или похищения, а также по созданию для себя благоприятных условий в целях получения максимальных выгод;

д) злоумышленные действия уголовных элементов – хищение информации или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

е) злоумышленные действия недобросовестных сотрудников – хищение (копирование) или уничтожение информационных массивов или/и программ по эгоистическим или корыстным мотивам.

4. Источники угроз. Под источником угроз понимается непосредственный исполнитель угрозы в плане негативного воздействия ее на информацию. Перечень и содержание источников приведены в табл.2.2 и в дополнительных комментариях не нуждаются.

Таблица 2.2

Системная классификация угроз информации

Параметры классификации	Значения параметров	Содержание значения критерия
1. Виды	1.1.Физической целостности.	Уничтожение (искажение).
	1.2. Логической структуры.	Искажение структуры.
	1.3. Содержания.	Несанкционированная модификация.
	1.4. Конфиденциальности.	Несанкционированное получение; утечка информации
	1.5. Права собственности.	Присвоение чужого права.
2. Природа происхождения	2.1. Случайная.	Отказы, сбои, ошибки.
		Стихийные бедствия.
		Побочные влияния.
	2.2. Преднамеренная.	Злоумышленные действия людей.
3.Предпосылки появления	3.1. Объективные.	Количественная недостаточность элементов системы.
		Качественная недостаточность элементов системы.
	3.2. Субъективные.	Разведывательные органы иностранных государств.
		Промышленный шпионаж.
		Уголовные элементы.
		Недобросовестные сотрудники.
4. Источники угроз	4.1. Люди.	Посторонние лица, пользователи, персонал.
	4.2. Технические устройства.	Регистрации, передачи, хранения, переработки, выдачи.
	4.3.Модели, алгоритмы, программы.	Общего назначения, прикладные, вспомогательные.
	4,4.Технологические схемы обработки.	Ручные, интерактивные, внутримашинные, сетевые.
	4.5. Внешняя среда.	Состояние атмосферы, побочные шумы, побочные сигналы

2.5. Причины, виды и каналы утечки информации

Основными причинами утечки информации являются:

- несоблюдение персоналом норм, требований, правил эксплуатации КИС;
- ошибки в проектировании КИС и систем защиты КИС;
- ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае лицом, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922-96 рассматриваются три вида утечки формации:

- разглашение;
- несанкционированный доступ к информации;
- получение защищаемой информации разведками (как отечественными, так и иностранными).

Под *разглашением* информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Под *несанкционированным доступом* понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Получение защищаемой *информации разведками* может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

Канал утечки информации – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может располагаться в пределах контролируемой зоны, охватывающей КИС, или вне ее.
Применительно к КИС выделяют следующие каналы утечки:

1. Электромагнитный канал. Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в аппаратных компонентах КИС. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки). Электромагнитный канал в свою очередь делится на следующие каналы:

- радиоканал (высокочастотное излучение);
- низкочастотный канал;
- сетевой канал (наводки на сеть электропитания);
- канал заземления (наводки на провода заземления);
- линейный канал (наводки на линии связи между компьютерными системами).

2. Акустический (виброакустический) канал. Связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации КИС.

3. Визуальный канал. Связан с возможностью визуального наблюдения злоумышленником за работой устройств отображения информации КИС без проникновения в помещения, где расположены компоненты системы. В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т.п.

4. Информационный канал. Связан с доступом (непосредственным и телекоммуникационным) к элементам КИС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также с подключением к линиям связи. Информационный канал может быть разделен на следующие каналы:

- канал коммутируемых линий связи,
- канал выделенных линий связи,

- канал локальной сети,
- канал машинных носителей информации,
- канал терминальных и периферийных устройств.

2.6. Модели разграничения доступа к информации

Для проведения желаемой политики безопасности в системе должны присутствовать соответствующие механизмы. В большинстве случаев эти механизмы содержат некоторые автоматизированные компоненты, зачастую являющиеся частью базового программного обеспечения (операционной системы) с соответствующим множеством процедур пользователя и администратора.

В то время как политика безопасности представляет собой множество правил для конкретной системы, модель безопасности – абстрактное описание поведения целого класса систем, без рассмотрения конкретных деталей их реализации. Модель безопасности является инструментом разработки политики безопасности.

Политика безопасности компьютерной системы может быть выражена формальным и неформальным образом. Для неформального описания политики безопасности широкое распространение получило описание правил доступа субъектов к объектам в виде таблиц, наглядно представляющих правила доступа. Обычно под этим подразумевается, что субъекты, объекты и типы доступа в данной системе определены, а множество субъектов и объектов конечно и определено. Основным преимуществом такого способа представления политики безопасности является доступность для понимания малоквалифицированным пользователем.

2.6.1. Модели безопасности

Модель дискреционного доступа. В рамках модели контролируется доступ субъектов к объектам. Для каждой пары субъект-объект устанавливается тип операции доступа (READ, WRITE и т.п.). Контроль доступа осуществляется посредством механизмов, которые предусматривают возможность санкционированного изменения правил разграничения доступа.

Модель дискретного доступа. В рамках модели рассматриваются механизмы распространения доступа субъектов к объектам.

Модель мандатного управления доступом (Белла-Лападула). Формально записана в терминах теории отношений. Описывает механизм доступа к ресурсам системы, при этом для управления доступом используется матрица контроля доступа. В рамках модели рассматриваются простейшие операции Read\Write, на которые накладываются ограничения. Множество субъектов и объектов упорядочены в соответствии с их уровнем полномочий и уровнем безопасности. Состояния системы изменяются по правилам трансформации состояний. Во множестве субъектов могут присутствовать доверенные субъекты, которые не подчиняются ограничениям на операции чтение-запись.

Модели распределённых систем (синхронная и асинхронная). В рамках моделей субъекты выполняют операции с объектами на нескольких устройствах обработки. Рассматриваются операции доступа субъектов к объектам, которые могут быть удалёнными, что может вызвать противоречия в модели. В рамках асинхронной модели в один момент времени несколько субъектов могут получить доступ к нескольким объектам. Переход системы из одного состояния в другое в один момент времени может осуществляться под воздействием более чем одного субъекта.

Модель безопасности военной системы передачи данных (MMS) – формально записана в терминах теории множеств. Субъекты могут выполнять специальные операции над объектами сложной структуры. В модели присутствует администратор безопасности для управления доступом к данным и устройствам к глобальной сети передачи данных. При этом для управления доступом используются матрицы контроля доступа. В рамках модели используются операции READ, WRITE, CREATE,DELETE, операции над объектами специфической структуры, а также могут появляться операции направленные на специфическую обработку информации. Состояние системы изменяется с помощью функции трансформации.

Модель трансформации прав доступа. Формально записана в терминах теории множеств. В рамках модели субъекту в данный момент времени предоставляется только одно право доступа. Для управ-

ления доступом применяются функции трансформации прав доступа. Механизм изменения состояния системы основывается на применении функции трансформации состояний системы.

Схематическая модель – формально записана в терминах теории множеств и теории предикатов. Для управления доступом используется матрица доступа со строгой типизацией ресурсов. Для изменения прав доступа применяется аппарат копирования меток доступа.

Иерархическая модель – формально записана в терминах теории предикатов. Описывает управление доступом для параллельных вычислений, при этом управление доступом основывается на вычислении предикатов.

Модель безопасных спецификаций – формально описана в аксиоматике Хоара. Определяет количество информации, необходимое для раскрытия системы защиты в целом. Управление доступом на основании классификации пользователей. Понятие механизма изменения состояний не применяется.

Модель информационных потоков – формально записана в терминах теории множеств. В модели присутствуют объекты и атрибуты, что позволяет определить информационные потоки. Управление доступом осуществляется на основе атрибутов объектов. Изменения состояния является изменением соотношения между объектами и атрибутами.

Вероятностные модели – в модели присутствуют субъекты, объекты и их вероятностные характеристики. Рассматриваются операции доступа субъектов к объектам READ и WRITE. Операции доступа также имеют вероятностные характеристики.

Модель элементарной защиты. Предмет защиты помещён в замкнутую и однородную защищённую оболочку, называемую преградой. Информация со временем стареет и цена её уменьшается. За условие достаточности защиты принимается превышение затрат времени на преодоление нарушителем преграды над временем жизни информации. Вводится вероятность не преодоления преграды нарушителем ($P_{СЗИ}$), вероятность обхода преграды нарушителем ($P_{ОБХ}$), вероятность преодоления защиты нарушителем за время меньшее времени жизни информации ($P_{НР}$). Для введенной модели нарушителя показано, что $P_{сзи} = \min [(1-P_{НР})(1-P_{ОБХ})]$, что является иллюстрацией принципа слабейшего звена. Развитие модели учитывает вероятность отказа системы и вероятность обнаружения блокировки действий нарушителя.

Модель системы безопасности с полным перекрытием. Отмечается, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему. Модель описывается в терминах теории графов. Степень обеспечения безопасности системы можно измерить, используя лингвистические переменные. В базовой системе рассматривается набор защищаемых объектов, набор угроз, набор средств безопасности, набор уязвимых мест, а также набор барьеров.

Модель гарантированно защищённой системы обработки информации. В рамках модели функционирование системы описывается последовательностью доступов субъектов к объектам. Множество субъектов является подмножеством множества объектов. Из множества объектов выделено множество общих ресурсов системы, доступ к которым не может привести к утечке информации. Все остальные объекты системы являются порождёнными пользователями, каждый пользователь принадлежит множеству порождённых им объектов. При условиях, что в системе существует механизм, который для каждого объекта устанавливает породившего его пользователя, что субъекты имеют доступ только к общим ресурсам системы и к объектам, порождённым ими и при отсутствии обходных путей политики безопасности модель гарантирует невозможность утечки информации и выполнение политики безопасности.

Субъектно-объектная модель. В рамках модели все вопросы безопасности описываются доступами субъектов к объектам. Выделены множество объектов и множество субъектов. Субъекты порождаются только активными компонентами (субъектами) из объектов. С каждым субъектом связан (ассоциирован) некоторый объект или объекты, т.е. состояние объекта влияет на состояние субъекта. В модели присутствует специализированный субъект – монитор безопасности субъектов, который контролирует порождение субъектов. Показана необходимость создания и поддержки изолированной программной среды.

2.6.2. Модель пятимерного пространства безопасности Хардстона

Модель использует пятимерное пространство безопасности для моделирования процессов установления полномочий и организации доступа на их основании.

Модель имеет 5 наборов:

A – набор установленных полномочий;

U – набор установленных пользователей;

E – набор установленных операций;

R – набор установленных ресурсов;

S – набор установленных состояний.

Доступ рассматривается как ряд запросов, осуществляющих пользование и для осуществления операций E над ресурсами R , в то время когда система находится в состоянии R.

Запрос на доступ – это кортеж:

q = {u, e, R, s}.

Величины U и S задаются системой, таким образом запрос на доступ есть подпространство четырехмерной проекции пространства безопасности. Запросы получают право на доступ в том случае когда они полностью заключены в соответствующее под пространство. Процесс организации доступа можно описать следующим алгоритмом.

Для запроса q = {U, R, A} – набора U' вполне определенных групп пользователей, набора R' вполне определенных ресурсов и набора A' – правильно установленных полномочий процесс организации доступа состоит из следующих процедур:

1. Вызвать все вспомогательные программы, необходимые для предварительного принятия решений.
2. Определить из U те группы пользователей, которые принадлежат группе U. Затем выбрать из P спецификации полномочий, которые соответствует выделенной группе пользователей. Этот набор полномочий F(U) определяет полномочия пользователя U.
3. Определить из P набор F(E) полномочий, которые устанавливают E как основную операцию. Этот набор называется привилегией операции E.
4. Определить из P набор F(R) (привилегия единичного ресурса R) полномочий, которые определяют поднабор ресурсов из R', имеющего общие элементы с запрашиваемой единицей ресурса R. Полномочия, которые являются общими для 3-х привилегий в шагах 2, 3, 4 образуют D(q) – домен полномочий для запроса q:

   D(q) = F(U)^F(E)*F(R).

5. Удостовериться, что запрашиваемый ресурс R полностью включается в D(q), т.е. любой элемент из R должен содержаться в некоторой единице ресурса, которая определена в домене полномочий D(q).
6. Осуществить разбиение набора D(q) на эквивалентные классы так, чтобы 2 полномочия попадали в эквивалентный класс тогда и только тогда, когда они специфицируют одну единицу ресурса. Для любого такого класса логическая операция ИЛИ или И выполняется с условием доступа элементов любого класса. Новый набор полномочий:

   А. Один на единицу ресурса, указанную в D(q) есть F(u, q)

   Б. Фактическая привилегия пользователя и по отношению к запросу q.
7. Вычислить EAC, условие фактического доступа соответствующую запросу q, осуществляя логическое И (ИЛИ) над условиями доступа членов F(u, q). Операция И (ИЛИ) выполнение над которой перекрывает единицу запрашиваемого ресурса.
8. Оценить EAC и принять решение о доступе:

   А. Разрешить доступ к R, если R перекрывается.

   Б. Отказать в доступе в противном случае.
9. Произвести запись необходимых событий.
10. Вызвать все программы необходимые для организации доступа после принятия решений.
11. Выполнить все программы, вытекающие для любого случая из условия 8.

12. Если решение о доступе было положительным, завершить физическую обработку.

Достоинства модели: простота реализации. Пример – матрица доступа.

Недостаток модели: ее статичность, т.е. модель не учитывает динамику изменений состояний ВС, не накладывает ограничений.

2.6.3. Модель Белла-Лападула

В предыдущих моделях существовала проблема «Троянских коней».

Троянская программа – любая программа, от которой ожидают выполнение желаемых действий, а она выполняет и нежелательные действия. В модели Белла-Лападула такой проблемы не существует.

Классическая модель Белла-Лападула (БЛ) построена для анализа систем защиты, реализующих мандатное (полномочное) разграничение доступа. Возможность ее использования в качестве формальной модели таких систем непосредственно отмечена в критерии TCSEC «Оранжевая книга». Модель БЛ была предложена в 1975 г.

Пусть определены конечные множества: S – множество субъектов системы (например, пользователи системы и программы); O – множество объектов системы (например, все системные файлы); *R={read, write, append*, *execute}* – множество видов доступа субъектов из S к объектам из O, где *read* – доступ на чтение, *write* – на запись, *append* – на запись в конец объекта, *execute* – на выполнение.

Обозначим:

$B = \{b \subseteq S \times O \times R\}$ – множество текущих доступов в системе;

M – матрица разрешенных доступов, где $M_{SO} \in R$ – разрешенный доступ субъекта s к объекту o;

L – множество уровней секретности, например $L = \{U, C, S, TS\}$, где *U<C<S<TS*;

$(f_s, f_o, f_c) \in F = L^S \times L^O \times L^S$ – тройка функций (f_s, f_o, f_c), определяющих:

$f_s = S \to L$ – уровень допуска объекта;

$f_O = O \to L$ – уровень секретности объекта;

$f_s = S \to L$ – текущий уровень допуска субъекта, при этом $\forall s \in S f_C(s) \le f_S(s)$;

H – текущий уровень иерархии объектов (далее не рассматривается);

$V = B \times M \times F \times H$ – множество состояний системы;

Q – множество запросов системе;

D – множество решений системы $D = \{yes, no, error\}$;

$W \subseteq Q \times D \times V \times V$ – множество действий системы, где четверка $(q, d, v_1, v_2) \in W$ означает, что система по запросу q с ответом d перешла из состояния v_1 в состояние v_2;

N_0 – множество значений времени $N_0 = (0, 1, 2, ...)$;

X – множество функций $x : N_0 \to Q$, задающих все возможные последовательности запросов к системе;

Y – множество функций $y : N_0 \to D$, задающих все возможные последовательности ответов системы по запросам;

Z – множество функций $z : N_0 \to V$, задающих все возможные последовательности состояний системы.

Далее в модели БЛ дается ряд свойств, определений и теорем, позволяющих проверить систему – разрабатываемую или существующую – на предмет безопасности. Классическая модель БЛ предлагает общий подход к построению систем, реализующих мандатную (полномочную) политику безопасности. В модели БЛ определяется, какими свойствами должны обладать состояние и действия системы, чтобы она была безопасной согласно данному в модели определению. В то же время в модели не указывается конкретно, что должна делать система по запросам на доступ субъектов к объектам при переходе из состояния в состояние, как конкретно должны при этом изменяться значения элементов модели.

2.6.4. Средства разграничения доступа

Представленные здесь средства реализуют модели избирательного (дискреционного) доступа

"Dallas Lock»

В комплексе «Dallas Lock» неявно используется атрибуты

R(d) = {Y, N},

где

Y – право полного доступа субъекта к объекту;

N – отсутствие права.

В соответствии с этим любому субъекту ставится в соответствие либо список запрещенных объектов, либо список разрешенных объектов.

"Secret Net»

В системе «Secret Net» набор применяемых атрибутов шире:

R(s) = {R, W, X},

где

R – разрешение на чтение;

W – разрешение на модификацию;

X – разрешение на запуск задачи.

"Аккорд»

В СЗИ НДС «Аккорд» набор общих прав доступа:

R(a) = {R, W, C, D, N, V, O, M, E, G, X},

где

R – разрешение на открытие файлов только для чтения;

W – разрешение на открытие файлов только для записи;

C – разрешение на создание файлов на диске;

D – разрешение на удаление файлов;

N – разрешение на переименование файлов;

V – видимость файлов;

O – эмуляция разрешения на запись информации в файл;

M – разрешение на создание каталогов на диске;

E – разрешение на удаление каталогов на диске;

G – разрешения перехода в каталог;

X – разрешение на запуск программ.

3. Управление защитой информации

3.1. Введение

В данном пособии под управлением будем понимать процесс целенаправленного воздействия на объект, осуществляемый для организации его функционирования по заданным правилам.

Основная (опосредованная) цель управления защитой информации – обеспечение реализации потенциальных возможностей информационной системы.

Непосредственная цель управления защитой информации – выработка и реализация своевременных и обоснованных решений, наилучших (оптимальных) с точки зрения реализации потенциальных возможностей системы защиты КИС в конкретных условиях.

Основные свойства и показатели эффективности процессов управления защитой информации:

Устойчивость управления – определяется способностью управлять с заданной эффективностью при активном вмешательстве нарушителя.

Непрерывность управления – возможность постоянно воздействовать на процесс защиты информации.

Скрытность управления защитой информации – определяется способностью воспрепятствовать в выявлении организации управления.

Оперативность управления определяется способностью своевременно и адекватно реагировать на действия злоумышленников и реализовывать управленческие решения к заданному сроку.

Обоснованность управления характеризуется всесторонним учетом условий решения поставленной задачи, применением различных моделей, расчетных и информационных задач, экспертных систем, опыта и любых других факторов, повышающих достоверность исходной информации и принимаемых решений.

Управление системой защиты и осуществление контроля за функционированием КИС – все это составляющие одной задачи – реализации политики безопасности.

Управление защитой информации представляет собой широкомасштабный и многогранный процесс начинающийся с формулирования положений политики безопасности организации и кончая регулярной оценкой защищенности КИС. Далее в настоящем разделе рассмотрены только некоторые составляющие процесса управления защитой информации в КИС.

3.2. Аудит

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Различают внешний и внутренний аудит. Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации. Рекомендуется проводить внешний аудит регулярно. Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании утвержденного плана и в соответствии с правилами изложенными, например в «Положении о внутреннем аудите», подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Аудит безопасности информационных систем является одной из составляющих ИТ аудита. Целями проведения аудита безопасности являются:

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

3.2.1. Определение и задачи аудита

Под термином «аудит» КИС понимается системный процесс получения и оценки объективных данных о текущем состоянии КИС, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенному критерию и предоставляющий результаты заказчику.

В настоящее время актуальность аудита резко возросла, это связано с увеличением зависимости организаций от информации и КИС. Рынок насыщен аппаратно-программным обеспечением, многие организации в силу ряда причин (наиболее нейтральная из которых – это моральное старение оборудования и программного обеспечения) видят неадекватность ранее вложенных средств в информационные системы и ищут пути решения этой проблемы. Их может быть два: с одной стороны – это полная замена КИС, что влечет за собой большие капиталовложения, с другой – модернизация КИС. Последний вариант решения этой проблемы – менее дорогостоящий, но открывающий новые проблемы, например, что оставить из имеющихся аппаратно-программных средств, как обеспечить совместимость старых и новых элементов КИС.

Более существенная причина проведения аудита состоит в том, что при модернизации и внедрении новых технологий их потенциал полностью не реализуется. Аудит КИС позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание КИС.

Кроме того, возросла уязвимость КИС за счет повышения сложности их элементов, увеличения объемов программного обеспечения, появления новых технологий передачи и хранения данных.

Спектр угроз расширился. Это обусловлено следующими причинами:
- передача информации по сетям общего пользования;
- «информационные войны» конкурирующих организаций;
- высокая текучесть кадров с низким уровнем порядочности.

По данным некоторых западных аналитических агентств **до 95%** попыток несанкционированного доступа к конфиденциальной информации происходит по инициативе бывших сотрудников организации.

Аудит ИБ в информационной системе это процесс сбора сведений, позволяющих установить:
- обеспечивается ли безопасность ресурсов организации (включая данные);
- обеспечиваются ли необходимые параметры целостности и доступности данных;
- достигаются ли цели организации в части эффективности информационных технологий.

Проведение аудита позволит оценить текущую безопасность функционирования КИС, оценить риски, прогнозировать и управлять их влиянием на бизнес процессы организации, корректно и обоснованно подойти к вопросу обеспечения безопасности информационных активов организации, основные из которых:
- идеи;
- знания;
- проекты;
- результаты внутренних обследований.

В настоящее время многие системные интеграторы на телекоммуникационном рынке декларируют поставку полного, законченного решения. К сожалению, в лучшем случае все сводится к проектированию и поставке оборудования и программного обеспечения. Построение информационной инфраструктуры «остается за кадром» и к решению не прилагается. Оговоримся, что в данном случае под информационной инфраструктурой понимается отлаженная система, выполняющая функции обслуживания, контроля, учета, анализа, документирования всех процессов, происходящих в информационной системе.

Все чаще и чаще у клиентов возникают к системным интеграторам, проектным организациям, поставщикам оборудования вопросы следующего содержания:
- Что дальше? (Наличие стратегического плана развития организации, место и роль КИС в этом плане, прогнозирование проблемных ситуаций).
- Соответствует ли наша КИС целям и задачам бизнеса? Не превратился ли бизнес в придаток информационной системы?
- Как оптимизировать инвестиции в КИС?
- Что происходит внутри этого «черного ящика» – КИС организации?

- Сбои в работе КИС, как выявить и локализовать проблемы?
- Как решаются вопросы безопасности и контроля доступа?
- Подрядные организации провели поставку, монтаж, пусконаладку. Как оценить их работу? Есть ли недостатки, если есть, то какие?
- Когда необходимо провести модернизацию оборудования и ПО? Как обосновать необходимость модернизации?
- Как установить единую систему управления и мониторинга КИС? Какие выгоды она предоставит?
- Руководитель организации, руководитель IT подразделения должны иметь возможность получать достоверную информацию о текущем состоянии КИС в кратчайшие сроки. Возможно ли это?
- Почему все время производится закупка дополнительного оборудования?
- Сотрудники IT подразделения постоянно чему-либо учатся, есть ли в этом необходимость?
- Какие действия предпринимать в случае возникновения внештатной ситуации?
- Какие возникают риски при размещении конфиденциальной информации в КИС организации? Как минимизировать эти риски?
- Как снизить стоимость владения КИС?
- Как оптимально использовать сложившуюся КИС при развитии бизнеса?

На эти и другие подобные вопросы нельзя мгновенно дать однозначный ответ. Только рассматривая все проблемы в целом, взаимосвязи между ними, учитывая нюансы и недостатки, можно получить достоверную, обоснованную информацию. Для этого в консалтинговых компаниях во всем мире существует определенная специфическая услуга – аудит компьютерной информационной системы (КИС).

Подход к проведению аудита КИС, как отдельной самостоятельной услуги, с течением времени упорядочился и стандартизировался. Крупные и средние аудиторские компании образовали ассоциации – союзы профессионалов в области аудита КИС, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ. Как правило, это закрытые стандарты, тщательно охраняемое ноу-хау.

Однако существует ассоциация – The Information Systems Audit and Control Association & Foundation (ISACA), занимающаяся открытой стандартизацией аудита КИС.

3.2.2. ISACA

Она основана в 1969 году и по состоянию на 2002 год объединяла более 23000 членов из более чем 100 стран. Ассоциация ISACA координирует деятельность более чем 26000 аудиторов информационных систем (CISA – Certified Information System Auditor и CISM – Certified Information Security Manager), имеет свою систему стандартов в этой области, ведет исследовательские работы, занимается подготовкой кадров, проводит конференции.

Основная декларируемая цель ассоциации – это исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем.

В помощь профессиональным аудиторам, руководителям IT подразделений, администраторам и заинтересованным пользователям ассоциацией ISACA и привлеченными специалистами из ведущих мировых консалтинговых компаний был разработан стандарт CoBiT (Control Objectives for Information and Related Technology).

3.2.3. CoBiT

CoBiT – открытый стандарт, первое издание которого в 1996 году было продано в 98 странах по всему миру и облегчило работу профессиональных аудиторов в сфере информационных технологий. Стандарт связывает информационные технологии и действия аудиторов, объединяет и согласовывает многие другие стандарты в единый ресурс, позволяющий авторитетно, на современном уровне получить представление и управлять целями и задачами, решаемыми КИС. CoBiT учитывает все особенности информационных систем любого масштаба и сложности.

Главное правило, положенное в основу CoBiT, следующее: ресурсы КИС должны управляться набором естественно сгруппированных процессов для обеспечения организации необходимой и надежной информацией (рис. 3.1).

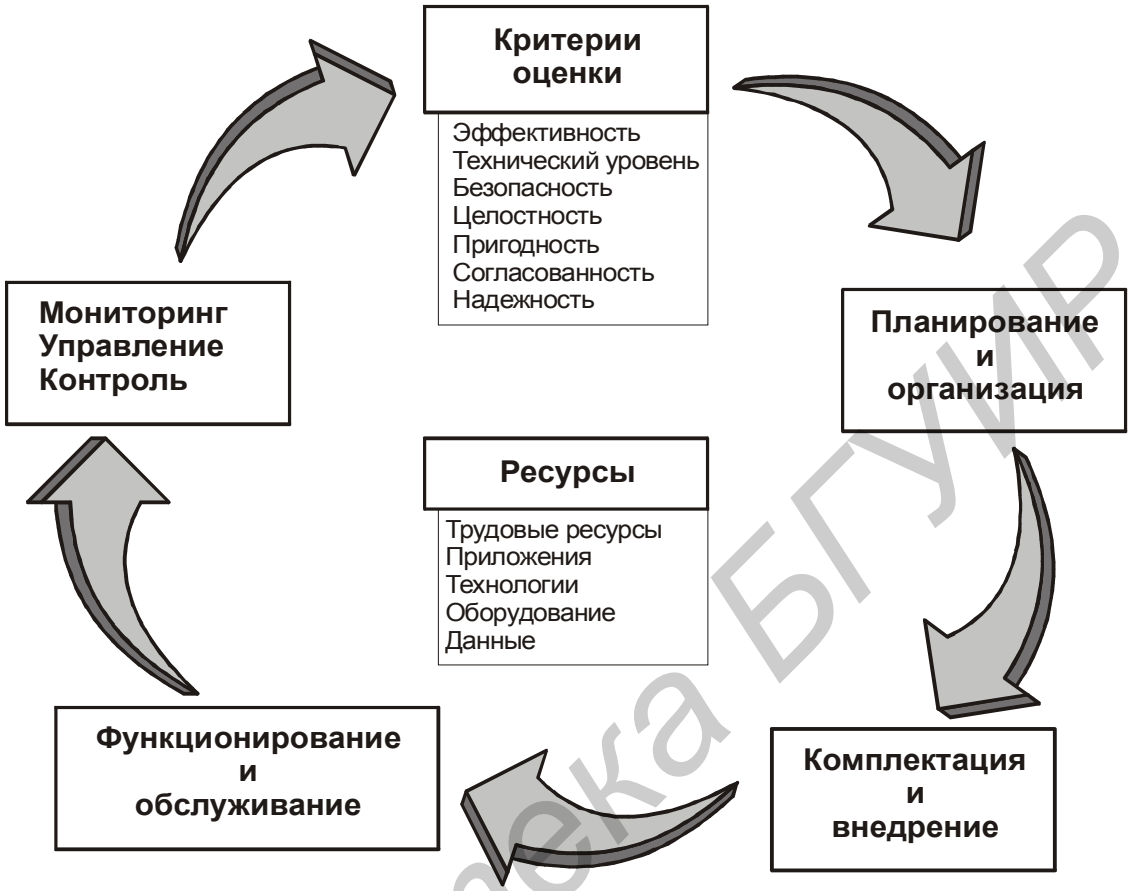

Рис. 3.1. Структура стандарта CoBIT

Теперь немного разъяснений по поводу того, какие ресурсы и критерии их оценки используются в стандарте CoBiT:

Трудовые ресурсы— под трудовыми ресурсами понимаются не только сотрудники организации, но также руководство организации и контрактный персонал. Рассматриваются навыки штата, понимание задач и производительность работы.

Приложения – прикладное программное обеспечение, используемое в работе организации.

Технологии – операционные системы, базы данных, системы управления и т.д.

Оборудование – все аппаратные средства КИС организации, с учетом их обслуживания.

Данные – данные в самом широком смысле – внешние и внутренние, структурированные и неструктурированные, графические, звуковые, мультимедиа и т.д.

Все эти ресурсы оцениваются CoBiT на каждом из этапов построения или аудита КИС по следующим критериям:

Эффективность – критерий, определяющий уместность и соответствие информации задачам бизнеса.

Технический уровень – критерий соответствия стандартам и инструкциям.

Безопасность – защита информации.

Целостность – точность и законченность информации.

Пригодность – доступность информации требуемым бизнес-процессам в настоящем и будущем. А также защита необходимых и сопутствующих ресурсов.

Согласованность – исполнение законов, инструкций и договоренностей, влияющих на бизнес-процесс, то есть внешние требования к бизнесу.

Надежность – соответствие информации, предоставляемой руководству организации, осуществление соответствующего управления финансированием и согласованность должностных обязанностей.

CoBiT базируется на стандартах аудита ISA и ISACF, но включает и другие международные стандарты, в том числе принимает во внимание утвержденные ранее стандарты и нормативные документы:

- технические стандарты;
- кодексы;
- критерии КИС и описание процессов;
- профессиональные стандарты;
- требования и рекомендации;
- требования к банковским услугам, системам электронной торговли и производству.

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

Несмотря на размер разработчики старались, чтобы стандарт был прагматичным и отвечал потребностям бизнеса, при этом сохраняя независимость от конкретных производителей, технологий и платформ.

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

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

Отличительные черты CoBiT:

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

Рассмотрим преимущества CoBiT перед многочисленными западными разработками. Прежде всего, это его достаточность – наряду с возможностью относительно легкой адаптации к особенностям КИС. И, конечно же, то, что стандарт легко масштабируется и наращивается. CoBiT позволяет использовать любые разработки производителей аппаратно-программного обеспечения и анализировать полученные данные не изменяя общие подходы и собственную структуру.

3.2.4. Практика проведения аудита КИС

Представленная на рис. 3.2. блок-схема отражает, хотя и не в деталях, ключевые точки проведения аудита КИС. Рассмотрим их подробнее.

На этапе подготовки и подписания исходно-разрешительной документации определяются границы проведения аудита. Границы аудита определяются критическими точками КИС (элементами КИС), в которых наиболее часто возникают проблемные ситуации.

На основании результатов предварительного аудита всей КИС (в первом приближении) проводится углубленный аудит выявленных проблем.

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

Далее проводится сбор информации о текущем состоянии КИС с применением стандарта CoBiT, объекты контроля которого получают информацию обо всех нюансах функционирования КИС как в двоич-

ной форме (Да/Нет), так и форме развернутых отчетов. Детальность информации определяется на этапе разработки исходно-разрешительной документации. Существует определенный оптимум между затратами (временными, стоимостными и т.д.) на получение информации и ее важностью и актуальностью.

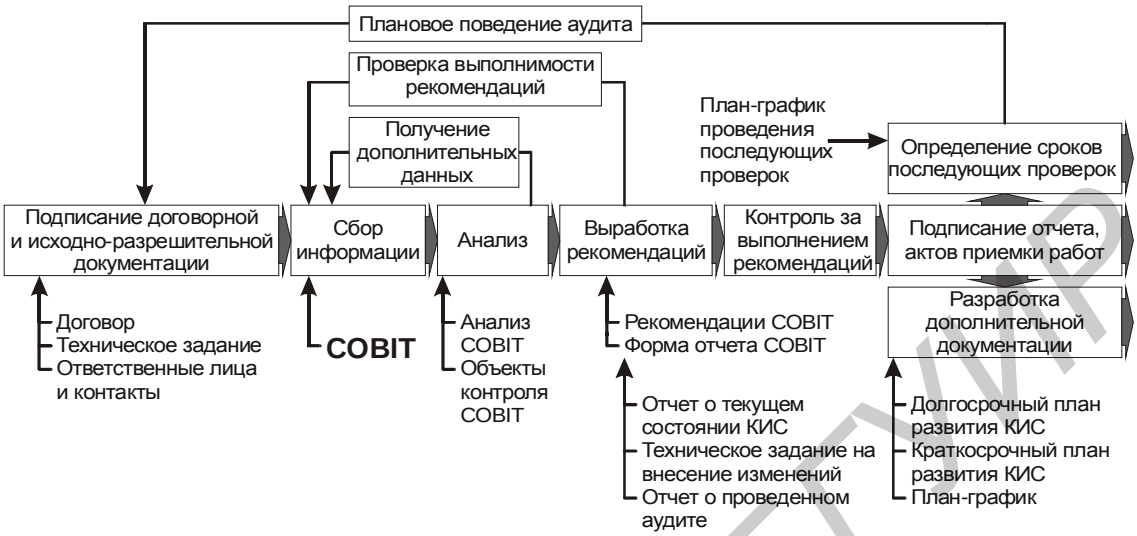

Рис. 3.2. Общая последовательность проведения аудита КИС

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

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

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

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

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

3.2.5. Результаты проведения аудита КИС

Результаты аудита КИС организации можно разделить на три основные группы:

- Организационные – планирование, управление, документооборот функционирования КИС.
- Технические – сбои, неисправности, оптимизация работы элементов КИС, непрерывное обслуживание, создание инфраструктуры и т.д.
- Методологические – подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Проведенный аудит позволит обоснованно создать следующие документы:

- Долгосрочный план развития КИС.
- Политика безопасности КИС организации.
- Методология работы и доводки КИС организации.

- План восстановления КИС в чрезвычайной ситуации.

3.3. Управление паролями

Доступ сотрудников к данным или иным источникам в системе обычно контролируется комбинацией идентификаторов пользователей системы и паролей. Для того чтобы такой подход был эффективным, необходимо поддерживать целостность пароля в течение всего периода его действия. Если идентификатор пользователя не предназначен для использования более, чем одним лицом (нежелательная ситуация, которая снимает ответственность), пароль должен быть известен только владельцу идентификатора пользователя, к которому он относится.

Система или сеть будет подвергаться опасности, если пароль и, следовательно, идентификатор пользователя компрометируются. Серьезность такой опасности зависит от:

- функций, доступных данному идентификатору пользователя – чем привилегированнее идентификатор, тем больше угроза;
- степени уязвимости данных, к которым может быть получен доступ.

Возможность использования компьютера или терминала может быть ограничена паролем включения питания, который не позволяет пользоваться компьютером, пока не будет введен правильный пароль. Screen savers (первоначально предназначавшиеся для предохранения экранов от пережога во время неактивного использования) обычно имеют парольные средства для предотвращения несанкционированного доступа к машине в отсутствие оператора. Эти средства могут быть полезными для предотвращения случайного несанкционированного доступа, но зачастую их можно обойти, имея достаточные технические знания.

Пароли наиболее часто компрометируются из-за отсутствия должной осторожности. Они также могут компрометироваться посредством некоторой формы изощренной атаки с использованием программного обеспечения для сборки паролей.

3.3.1. Потенциальные угрозы

Потеря конфиденциальности вследствие:

- несанкционированного доступа к данным из-за потери защиты пароля.

Потеря целостности вследствие:

- несанкционированного изменения системы и/или ее данных из-за потери защиты пароля.

Потеря доступности вследствие:

- незапоминания пароля;
- неправильного или несанкционированного изменения пароля.

3.3.2. Пути снижения рисков

- избегать использования общих идентификаторов пользователей вместе с общими паролями;
- выбирать пароли длиной не менее шести знаков;
- соблюдать следующие правила в отношении паролей:
- никому не раскрывать свой пароль;
- убедиться, что никто не наблюдает за вами во время ввода пароля;
- не записывать пароль там, где его может кто-либо может обнаружить;
- выбирать свои собственные пароли;
- изменять устанавливаемые по умолчанию пароли при использовании нового идентификатора пользователя в первый раз;
- перед заменой пароля проверить установки клавиш, таких как *Caps Lock* и *Shift Lock,* для того чтобы обеспечить правильность знаков;
- использовать простые (т.е. легко запоминаемые) пароли, такие как слова с произвольными орфографическими ошибками;
- включить в состав пароля не менее одного знака, который не является буквой;
- использовать некоторую форму триггера памяти для облегчения вызова пароля;
- периодически менять свой пароль, предпочтительно не реже одного раза в месяц;
- заменить пароль, если есть подозрения в его компрометации.

Не выбирать пароль, который:

- вероятно может быть найден в словаре (особенно слова, ассоциирующиеся с безопасностью, такие как «система», «секрет», «пароль» и т.п.);
- является обычным именем;
- имеет ассоциацию с предыдущим паролем (например, имеет в своем составе наименование или обозначение месяца, если пароль меняется ежемесячно);
- имеет явную ассоциацию с его владельцем (например, номер автомобиля, имя ребенка, название дома, инициалы и т.п.);
- состоит из одной повторяющейся буквы;

Запрещается:

- использовать пароль в скрипте входа в систему или макросе;
- пересылать пароли по электронной почте;
- устанавливать идентификатор пользователя без пароля или с паролем, состоящим из символов пробела;

Администраторы сетей и системные администраторы должны:

- идентифицировать и менять устанавливаемые по умолчанию пароли, когда система запускается в эксплуатацию;
- менять или удалять соответствующие идентификаторы пользователей и/или пароли при перемещении персонала;
- блокировать соответствующие идентификаторы пользователей в случае отсутствия сотрудника в течение длительного времени;
- обеспечить подходящую конфигурацию программного обеспечения управления паролями;

При выборе системного программного обеспечения отдавать предпочтение тем, чей механизм контроля паролей:

- позволяет использовать в паролях как буквы, так и числа;
- требует подтверждения новых паролей (например двойного ввода), чтобы избежать риска неправильного набора;
- вынуждает менять пароль спустя определенное время;
- не позволяет повторного использования паролей (для одного и того же идентификатора пользователя);
- отключает идентификатор пользователя, если пароль неправильно вводится несколько раз (обычно три раза) подряд;
- не выводит на дисплей пароли при их вводе;
- требует, чтобы пароли имели не менее шести знаков;
- хранит пароли в зашифрованном виде;
- защищает таблицу или файл паролей системы от несанкционированного доступа;
- предоставляет средство сброса паролей в случае, когда их забывают, и обеспечивает наблюдение за этим процессом;

Там, где проблемы безопасности особенно важны, рассмотреть возможность:

- использования устройства для генерации нового пароля при каждой необходимости доступа в систему или сеть;
- совместного использования пароля с интеллектуальной карточкой;
- ограничения доступа к идентификаторам пользователей обычными часами работы соответствующих сотрудников.

3.3.3. Обязательные правила

Пароли должны включать в себя не менее шести знаков; их необходимо держать в секрете (посредством таких мер, как регулярная замена, исключение общих слов и т.п.). Никому не сообщайте свой пароль без явного разрешения руководителя подразделения.

По окончании времени использования информационной системы или при оставлении своего терминала или ПК без присмотра соблюдайте формальные процедуры выхода из работы.

3.4. Управление идентификаторами привилегированных пользователей

Компьютерные системы, от PC LAN до мейнфреймов, обычно различают пользователей посредством User-ID (идентификаторов пользователей). Данный раздел посвящен особым «идентификаторам привилегированных пользователей», дающих привилегированным пользователям право как устанавливать систему, так и впоследствии сопровождать ее. Например, такой ID используется для предоставления или аннулирования доступа в систему или к ее данным, прогонять резервные копии и осуществлять восстановление. Идентификатор привилегированного пользователя по своей природе должен предоставлять возможность доступа последнего ко всем программам и данным в системе, несмотря на их принадлежность и обычные ограничения в области безопасности.

Как следствие, этот очень нужный ID несет риск безопасности в своем праве, если его использование тщательно не контролируется и не отслеживается. Компьютер не может сказать, кто в самом деле пользуется в настоящий момент идентификатором – любой, кто говорит, что он привилегированный пользователь, и знает нужный пароль, и есть привилегированный пользователь. Несанкционированный доступ под идентификатором привилегированного пользователя может быть использован для модификации любых журналов мониторинга, таким образом уничтожая любые улики.

Дополнительная угроза заключается в том, что в аварийной ситуации может понадобиться использование идентификатора привилегированного пользователя для корректировки некоторых ошибок глубоко в системе. Такое использование может осуществить кто-либо другой, а не сам системный администратор, тем самым расширяются возможности несанкционированного использования прав привилегированного пользователя.

3.4.1. Потенциальные угрозы

Потеря конфиденциальности вследствие:

- несанкционированного использования идентификатора привилегированного пользователя для получения доступа к уязвимым данным;
- несанкционированного использования идентификатора привилегированного пользователя для изменения или снятия ограничений в отношении защиты и безопасности.

Потеря целостности вследствие:

- санкционированного, но некомпетентного использования идентификатора привилегированного пользователя для внесения изменений в программное обеспечение и/или данные;
- несанкционированного использования идентификатора привилегированного пользователя для внесения изменений в программное обеспечение и/или данные.

Потеря доступности вследствие:

- несанкционированного или некомпетентного использования идентификатора привилегированного пользователя, что привело к порче или удалению ключевого программного обеспечения и данных.

3.4.2. Пути снижения рисков

- соблюдать особые меры предосторожности в отношении защиты идентификаторов привилегированных пользователей (см. параграф – управление паролями);
- обязательно отключиться от идентификатора привилегированного пользователя по завершении выполнения задания, требующего его использования, а также при оставлении терминала или ПК без присмотра;
- предоставлять доступ к идентификаторам привилегированных пользователей только специально подготовленным сотрудникам и только для определенного набора заданий;
- регистрировать и отслеживать случаи фактического использования идентификаторов привилегированных пользователей и попытки их использования;
- использовать все имеющиеся в системе средства, такие как контрольные журналы, для регистрации действий с применением идентификаторов привилегированных пользователей;
- поддерживать тщательный контроль, преимущественно на уровне руководства, за всеми паролями привилегированных пользователей, предназначенными для использования в аварийной ситуации. Немедленно заменить их после использования;

- использовать идентификаторы привилегированных пользователей для выполнения только тех задач, которые специально требуют их применения (т.е. не использовать их, если задание может быть выполнено с применением идентификаторов обычных пользователей и обычных процедур);
- присваивать идентификаторам привилегированных пользователей непритязательные имена (без указания на привилегии);
- там, где возможно (например, с операционной системой UNIX), идентификаторы привилегированных пользователей самого высокого уровня должны быть доступны только при первоначальном подключении к идентификатору обычного пользователя, тем самым обеспечивая некоторую степень ответственности. Для некоторых заданий, требующих высокого уровня привилегий, может оказаться возможным ограничить их до «консольного» терминала, который может быть защищен физически.

3.4.3. Обязательные правила

Обязательные правила, в основном, касаются использования паролей и аналогичны изложенным в пункте 3.3.3.

3.5. Планирование мероприятий по обеспечению логической безопасности

Логическая безопасность – это нефизические(как правило, программные) средства контроля доступа в систему. Используются для защиты уязвимой информации и программных средств.

Большинство компьютерных систем, используемых в организации, имеют механизм обеспечения безопасности, который может использоваться для создания соответствующей структуры контроля с целью защиты системы. Для ПК стандартная операционная система которых не обеспечивает такого механизма, имеются пакеты, которые могут выполнять эту функцию.

Хорошо спланированные мероприятия по обеспечению логической безопасности наряду с физической безопасностью повышают защиту компьютерных систем и содержащихся в них данных от несанкционированного доступа и/или вмешательства.

3.5.1. Потенциальные угрозы

Потеря конфиденциальности вследствие:
- несанкционированного доступа к уязвимой информации.

Потеря целостности вследствие:
- несанкционированного или неконтролируемого внесения изменений в программное обеспечение и/или данные, содержащиеся в системе;
- отсутствия разграничения в отношении кто и что может изменять в системе.

Потеря доступности вследствие:
- искажения или удаления (случайного или намеренного) программного обеспечения и/или данных в системе не имеющими прав пользователями.

3.5.2. Пути снижения рисков

- Планировать логическую безопасность системы в целом, принимая во внимание степень уязвимости подлежащей защите системы и данных и объем защиты, которая может быть обеспечена физическими средствами.
- Разделить обязанности для минимизации риска злоупотреблений в системе, будь то по небрежности или преднамеренно. В частности, рассмотреть возможность разделения следующих функций:
  - ввод данных;
  - управление сетью;
  - администрирование системы;
  - развитие и сопровождение системы;

  - управление изменениями;
  - администрирование безопасности.
- Предоставить каждому уполномоченному пользователю системы уникальный идентификатор пользователя и пароль, с тем чтобы они могли быть идентифицированы, и им могли быть даны соответствующие права доступа.
- Защитить систему от доступа паролями или аналогичными средствами.
- Предпринять меры (т.е. использовать формальные процедуры, автоматический выход из системы) для обеспечения отключения пользователей от системы по окончании работы или при оставлении своего терминала или ПК без присмотра (за консультацией обращаться к специалистам соответствующих служб).
- Обеспечить защиту всех системных и прикладных программ с тем, чтобы они могли обновляться только теми, кто имеет на это право.
- Внедрить процедуры проверки для обнаружения изменений в программных файлах (контрольное суммирование).
- Обеспечить защиту всех уязвимых данных с тем, чтобы они могли быть доступны только тем, кто имеет на это разрешение.
- Держать очень уязвимую информацию (особенно это касается информации, которую не должны видеть лица, имеющие доступ к привилегированным идентификаторам пользователя) на съемных носителях, таких как дискеты. Такие данные должны быть обеспечены защитой и храниться отдельно от системы (см. параграф «Планирование мероприятий по обеспечению физической безопасности»).
- Шифровать уязвимые данные во время хранения и/или передаче по линиям связи.

3.5.3. Обязательные правила

Все системы (включая переносные и «домашние» компьютеры), в которых используются уязвимые данные, должны настраиваться и эксплуатироваться таким образом, чтобы доступ к таким данным могли иметь только имеющие соответствующие полномочия сотрудники (за консультацией обращайтесь к администратору безопасности).

3.6. Планирование мероприятий по обеспечению физической безопасности

Физическая безопасность – это физические (не программные – охрана, замки, двери, решетки и. т.п.) средства контроля доступа к ресурсам системы.

Любое физическое имущество должно предохраняться от потери, повреждения или кражи, компьютерное оборудование не составляет исключения. Однако физическая защита компьютерного оборудования представляет собой первую оборонительную линию для любой компьютерной системы, которую оно поддерживает. В некоторых системах, например, операционных системах UNIX, физический доступ к серверу позволяет обойти все меры защиты системы. Физическая безопасность обеспечивает защиту компьютерной системы в целом, т.е. программное обеспечение и данные, а также аппаратные средства.

Следовательно, меры, принимаемые для сохранения физической безопасности компьютерного оборудования, должны отражать не только стоимость замены оборудования, но и возможный ущерб от потери системы, программного обеспечения и данных. В некоторых случаях организация могла бы оказаться в затруднительном положении, если бы содержащее уязвимые данные и/или системы оборудование было вынесено из организации.

В общем, риск случайного повреждения может быть снижен, если руководствоваться общим здравым смыслом (и соблюдать инструкции по технике безопасности). Однако, для защиты систем от воздействия окружающей среды, неосторожности, намеренного вмешательства и кражи необходимы другие меры. С уменьшением размеров аппаратных средств увеличивается возможность их кражи, особенно это касается таких компонентов как диски и ПК. Существует риск кражи и таких компонентов, как платы памяти и процессорные чипы, которые малы, легко снимаются и довольно дорого стоят.

3.6.1. Потенциальные угрозы

Потеря конфиденциальности вследствие:
- несанкционированного доступа к уязвимой информации в результате утери или кражи компьютерного оборудования.

Потеря доступности вследствие:
- утери, повреждения или кражи компьютерного оборудования;
- пропадания питания или бросков напряжения.

3.6.2. Пути снижения рисков
- обеспечить защиту оставляемых без присмотра аппаратных средств, которые поддерживают дорогостоящие, критичные и/или уязвимые компьютерные системы – устанавливать их в закрываемом на ключ шкафу, в отдельной закрываемой на ключ комнате, или установить замки на клавиатурах;
- надежно хранить все портативные носители данных (дискеты, ленты) в соответствии с их уязвимостью, критичностью или ценностью хранящихся на них данных – держать в сейфе, если они не используются в данный момент. Заметим, что стандартные, даже огнестойкие, сейфы не обеспечивают надлежащей защиты магнитных носителей;
- обеспечить защиту источников питания критичных систем.

3.7. Слежение за состоянием безопасности

Основанием для защиты информационной системы с использованием мер безопасности является повышение уверенности в конфиденциальности, целостности и доступности, как самой системы, так и ее данных.

Однако установление необходимых мер безопасности само по себе не является гарантией того, что они будут продолжать свою работу так, как от них ожидается, в течение всего срока функционирования системы. Например, безопасность может быть скомпрометирована по невнимательности в процессе внесения обычных изменений в систему; плохое администрирование системы может допустить возникновение ошибок, которые постепенно подрывают целостность системы; изменения могут быть сделаны с деструктивным намерением. Если не существует процедур слежения за состоянием безопасности, то вполне вероятно, что случаи компрометации останутся незамеченными до тех пор, пока не произойдет функциональный сбой, раскрытие конфиденциальной информации или финансовые потери.

Поэтому важно, чтобы менеджеры систем и администраторы сетей имели средства выявления слабых мест в безопасности систем и обнаружения фактических брешей в безопасности при их появлении. Однако наличие таких возможностей требует накладных расходов. Затраты при этом должны соразмеряться с потенциальными рисками. Хорошо обдуманная и спроектированная функция слежения за состоянием безопасности КИС должна помочь добиться правильного соотношения между затратами и риском.

3.7.1. Потенциальные угрозы

Потеря конфиденциальности, доступности и целостности вследствие:
- остающихся незамеченными случаев нарушения безопасности (например, несанкционированного доступа к привилегированным или иным идентификаторам пользователя, программному обеспечению, уязвимым данным);
- санкционированных изменений в системе, приводящих к неожиданной и незамеченной потере эффективности действующих мер обеспечения безопасности;
- несанкционированных изменений, снижающих степень безопасности, но остающихся незамеченными (например, приводящих к неадекватному или неправильному контролю доступа к уязвимым данным в течение долгого периода времени).

3.7.2. Пути снижения рисков

Проектировать такую систему или процедуру слежения за состоянием безопасности, которая бы:

- учитывала все аспекты безопасности системы;
- отслеживала те области, где бреши в безопасности будут наиболее уязвимыми;
- отслеживала те области, где изменения (будь то технологические, организационные или структурные) могут снизить эффективность существующих в настоящий момент мер безопасности;
- уделяла основное внимание областям риска и отчетности (например, сообщениям об исключительных ситуациях);
- отслеживала свою собственную эффективность (т.е. регистрировала свои собственные удачи и сбои).

Распределить персональную ответственность за слежение за состоянием безопасности и определить конкретное время для этого.

Документировать процедуры и сферы ответственности.

Установить наблюдение за работой системы слежения и регулярно пересматривать процедуры при накоплении опыта.

3.8. Планирование мероприятий на случай выхода системы из строя

Компьютерная система включает в себя целый ряд компонентов (обычно это данные, программное обеспечение, аппаратные средства и сеть), и все они должны работать на систему, чтобы сделать ее полностью доступной. Надежность системы определяется надежностью ее самого слабого звена; ни одна система не может считаться гарантированной от сбоя. Например, данные могут быть потеряны случайно или умышленно; аппаратные и программные средства могут выйти из строя; внешние факторы, такие, как сбой питания или пожар, могут вывести систему из строя временно или навсегда.

Потеря любой системы будет иметь неблагоприятные последствия. Ключевыми вопросами здесь являются: насколько серьезны эти последствия и как скоро они сказываются на производственном процессе. Планирование мероприятий на случай выхода системы из строя ставит своей целью контроль, ограничение и, по возможности, избежание подобных последствий. Любые принимаемые меры предосторожности должны, конечно, соответствовать рискам, например, было бы простой тратой денег обеспечение дорогостоящего восстановления системы в течение часа, если она могла бы бездействовать в продолжение дня без нанесения серьезного ущерба. Важно также, чтобы планирование обеспечивало согласованность средств защиты разных компонентов и их эффективность при совместном внедрении в систему в целом.

Вообще говоря, сбой является результатом:

1) проблемы в самой системе;

2) проблемы, являющейся внешней по отношению к системе, но локализованной (например, сбой питания или пожар в компьютерном зале);

3) проблемы, являющейся внешней по отношению к системе, но имеющей намного более широкие последствия, даже за пределами самого организации (например, крупный пожар или общественные беспорядки).

Отдельные подразделения несут ответственность за свои системы и, следовательно, за свои собственные процедуры резервирования и восстановления. Вместе с тем планирование в отношении сбоя по пункту 3 должно проводиться в более широком контексте, поскольку восстановление одной системы может происходить за счет восстановления другой.

Способность к восстановлению системы и ее данных зависит от наличия резервной копии, с которой можно начинать восстановление. Резервные копии обычно хранятся на переносных носителях (например, дискетах, лентах), которые сами добавляют угрозу для безопасности (см. соответствующие разделы руководства), особенно если эти резервные копии содержат легко дешифруемую информацию, такую как документы пословной обработки. Следовательно, при планировании необходимо учитывать риски для безопасности, исходящие от самого механизма резервирования и восстановления.

Последняя из рассматриваемых проблем касается некоторых крупных компьютерных конфигураций (обычно поддерживающих многочисленные приложения), где безопасность поддерживается **отдельной системой обеспечения безопасности.** Особая осторожность здесь потребуется для обеспечения поддержания безопасности приложений в случае выхода из строя самой системы безопасности.

3.8.1. Потенциальные угрозы

Потеря конфиденциальности вследствие:
- неадекватной защиты данных, хранящихся на резервных носителях (например лентах, дискетах);
- выхода из строя не самого приложения, а защищающей его отдельной системы безопасности.

Потеря целостности и/или доступности вследствие:
- случайной или умышленной потери или разрушения данных;
- потери или разрушения системного или прикладного программного обеспечения;
- сбоя оборудования, на котором работает система, или магнитных носителей (например дисков, дискет), на которых хранятся данные;
- выхода из строя сети или каналов связи;
- внешних факторов (например, пожара, пропадания питания, бомбового удара).

3.8.2. Пути снижения рисков

Убедиться, что безопасность системы и ее данных поддерживается даже в случае сбоя какой-либо защищающей ее отдельной системы безопасности.

Разработать и внедрить процедуры восстановления (например, от «дисков с зеркальным отображением» до полного «горячего резерва»), которые могут определить:
- как долго может продолжаться производственный процесс без системы или ее данных и во что это обойдется;
- какие существуют альтернативы (например, канцелярская система) и как долго они могут работать;
- различные типы сбоев и их продолжительность;
- при составлении проектов планов восстановления, привлекать пользователей системы и обеспечить получение их одобрения;
- определить тип необходимых резервных копий, когда и как часто их необходимо делать, как быстро они могут понадобиться, где они должны храниться (т.е. на местах и/или в отдельных помещениях), и как долго их необходимо хранить – за технической консультацией обращайтесь к специалистам соответствующих служб;
- обеспечить, чтобы резервные копии (особенно на переносных носителях) не представляли большего риска для безопасности, чем сама система, с которой они сняты – за технической консультацией обращайтесь к специалистам соответствующих служб;
- четко распределить обязанности по изготовлению резервных копий и обеспечить понимание этих обязанностей;
- обеспечить совместимость резервных копий данных и систем;
- если система должна быть восстановлена в другом месте, проверить на совместимость систему и восстановительные программные средства;
- регулярно тестировать планы восстановления;
- проверять ранее сделанные резервные копии на читаемость;
- оформлять процедуры резервирования и восстановления в виде документов (и хранить копию в удаленном месте);
- регистрировать местонахождение, состояние и «возраст» всех резервных копий (и хранить копию в удаленном месте);
- регулярно пересматривать все процедуры резервирования и восстановления.

3.9. Использование средств удаленной диагностики

В настоящее время многие поставщики как аппаратных, так и программных средств предлагают «средства удаленной диагностики» для своих продуктов. Эти средства позволяют поставщику входить прямо в систему по телефонной линии с целью диагностики проблем. Такая связь может использоваться поставщиком для предоставления экстренных или обычных новых версий программного обеспечения.

Предоставление поставщику прямого доступа в систему может снизить размер платы за сопровождение и наверняка ускорить оказание услуг. Наблюдается тенденция расширения поставщиками продвижения такой услуги. Доходит даже до того, что это ставится условием заключения контракта на сопровождение.

Хотя налицо некоторые преимущества использования каналов удаленной диагностики, в одинаковой степени существуют и определенные опасности. Если не установлен надлежащий контроль, такие каналы могут представлять основную угрозу конфиденциальности и целостности системы и ее данным, особенно если поставщик знает, как система поддерживает производственную деятельность организации.

3.9.1. Потенциальные угрозы

Потеря конфиденциальности вследствие:
- доступа поставщика к уязвимым данным;
- несанкционированного использования канала дальней связи;
- перехвата сообщений между организацией и поставщиком.

Потеря целостности и/или доступности вследствие:
- неконтролируемого или несанкционированного изменения поставщиком программного обеспечения или данных;
- внешнего вмешательства во время передачи сообщений в санкционированное изменение программного обеспечения;
- заражения компьютерным вирусом.

3.9.2. Пути снижения рисков
- обеспечить, чтобы поставщики полностью сознавали свою ответственность и необходимость сохранения конфиденциальности и безопасности системы и ее данных. Проверять, какие устройства устанавливает поставщик. Они должны быть подтверждены письменным договором или контрактом;
- отключать коммутируемый канал, когда он не используется;
- использовать процедуру обратного дозвона для проверки происхождения запроса на установление связи;
- вести журнал регистрации времени начала связи, совершенных действий и времени прерывания связи;
- контролировать доступ по каналу связи в систему и к уязвимым данным с помощью паролей или аналогичных средств. Рассмотреть возможность временного удаления очень уязвимых данных прежде, чем разрешить установление соединения;
- тестировать все новые версии программных средств, полученные по каналу удаленной диагностики, в том же объеме, что и программные средства, получаемые обычным путем;
- шифровать все сообщения, передаваемые между организацией и поставщиком.

3.9.3. Обязательные правила

Не передавайте уязвимую информацию по сетям общего пользования или по другим сетям, находящимся вне контроля организации, если только она не защищена средствами шифрования или эквивалентными средствами (за консультацией обращайтесь к администратору безопасности).

Не подключайтесь ни к какой внешней услуге или линии связи без получения консультации у специалистов относительно прямых или непрямых последствий такого подключения и относительно особых

правил, касающихся определенных типов линий связи или услуг. Это в особенности касается подключения к сети Internet.

4. Перечень стандартов Республики Беларусь, касающихся информационной безопасности

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Госстандарт СССР.

ГОСТ 31078-2002. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

СТБ ИСО/МЭК 9126-2003. Информационные технологии. Оценка программной продукции. Характеристики качества и руководства по их применению.

СТБ ИСО/МЭК ТО 9294-2003. Информационные технологии. Руководство по управлению документированием программного обеспечения.

СТБ ИСО/МЭК 12119:1994. Информационные технологии. Пакеты программ. Требования к качеству и тестирование

СТБ ИСО/МЭК ТО 12182-2003. Информационные технологии. Классификация программных средств.

СТБ ИСО/МЭК 12207-2003. Информационные технологии. Процессы жизненного цикла программных средств.

СТБ ИСО/МЭК 14764-2003. Информационные технологии. Сопровождение программных средств.

СТБ ГОСТ Р 51241-2003. Средства контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

СТБ 1176.1. Функция хеширования.

СТБ 1176.2. Процедуры выработки и проверки электронной цифровой подписи.

СТБ 1221-2000. Документы электронные. Правила выполнения, обращения и хранения.

СТБ 34.101.1 – 2001. Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель.

СТБ 34.101.2 – 2001. Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности.

СТБ 34.101.3 – 2001. Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Гарантийные требования безопасности.

СТБ П 34.101.4-2002. Информационная технология. Профиль защиты электронной почты предприятия.

СТБ П 34.101.5-2003. Информационные технологии и безопасность. Общая методология испытаний продуктов и систем информационных технологий на соответствие уровням гарантий.

СТБ П 34.101.6-2003. Информационные технологии и безопасность. Задание по обеспечению безопасности. Разработка, обоснование, оценка.

СТБ П 34.101.7-2003. Информационные технологии и безопасность. Профиль защиты. Разработка, обоснование, оценка.

СТБ П 34.101.8-2003. Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования

РД РБ07040.1001-2002. Автоматизированная система межбанковских расчетов. Общие требования по обеспечению непрерывной работы и восстановления работоспособности участников в АС МБР.

РД РБ 07040.1101-2000. АС МБР. Архивы электронных документов. Общие требования.

РД РБ 07040.1601-2000. АС МБР. Форматы электронных сообщений. Ч. 1. Электронные сообщения системы расчетов по крупным и срочным платежам на валовой основе в режиме реального времени.

РД РБ 07040.1602-2002. Автоматизированная система межбанковских расчетов. Форматы электронных сообщений. Часть 2. Электронные сообщения клиринговой системы расчетов.

РД РБ 07040.1605-2000. АС МБР. Правила формирования электронных документов. Ч. 1. Электронные документы и сообщения системы расчетов по крупным и срочным платежам на валовой основе в режиме реального времени.

РД РБ 07040.1606-2000. АС МБР. Правила формирования электронных документов. Ч. 2. Электронные сообщения и документы клиринговой системы расчетов.

5. Перечень правовых актов Республики Беларусь, касающихся информационной безопасности

Уголовный кодекс.

Гражданский кодекс.

Уголовно-процессуальный кодекс.

Банковский кодекс.

Закон Республики Беларусь «О государственных секретах».

Закон Республики Беларусь «Об информатизации».

Закон Республики Беларусь «Об информационной безопасности» (проект).

Закон Республики Беларусь «О защите информации» (проект).

Закон Республики Беларусь «Об электронном документе».

Закон Республики Беларусь «О национальном архивном фонде и архивах Республики Беларусь».

Закон Республики Беларусь «Об органах государственной безопасности».

Закон Республики Беларусь «О милиции».

Положение о Государственном центре безопасности информации при Президенте Республики Беларусь.

Временное положение о порядке выдачи субъектам хозяйствования специальных разрешений (лицензий) на разработку, производство, реализацию, монтаж, наладку, сервисное обслуживание технических и программных средств защиты информации и контроля ее защищенности, специальных материалов и оборудования для производства этих средств, программно-аппаратных средств защиты от несанкционированного доступа, в том числе с применением средств криптографии, проведение специальных исследований технических средств от утечки информации, работ по выявлению устройств съема информации и контроля ее защищенности.

Положение о коммерческой тайне. Утверждено постановлением Совета Министров Республики Беларусь от 6 ноября 1992 г. № 670.

Глоссарий

Абонент. Лицо (группа лиц или организация), имеющее право на пользование услугами соответствующей системы.

Авторизация. Предоставление определенных полномочий аутентифицированному субъекту на выполнение некоторых действий в системе.

Администратор безопасности. Лицо, уполномоченное специальным образом в системе информационной безопасности управлять всей системой или определенными функциями в системе – сферами влияния. Администратор безопасности системы (подсистемы) отвечает за информационную безопасность системы (подсистемы) в целом и наделяет полномочиями определенных пользователей, устанавливая для них сферы влияния (сферы ответственности).

Администрирование. Процесс управления защитой информации на общесистемном уровне или на уровне сфер влияния, ограниченных предоставленными администраторам полномочиями. Сферы влияния могут пересекаться и включать одна другую. Администрирование на общесистемном уровне поглощает все сферы администрирования.

Архив. Система хранения информации в течение установленного срока.

Аттестация. Комплекс проверок программного (программно-аппаратного) продукта с целью удостоверения соответствия его установленным требованиям в реальных условиях эксплуатации.

Аудит безопасности. Аудит безопасности включает распознавание, запись, хранение и анализ информации, связанной с действиями, влияющими на безопасность. Получаемые в результате записи аудита могут быть проанализированы для определения значимости этих действий для безопасности. Этот класс образован из семейств, которые определяют, помимо всего прочего, требования к отбору событий, подлежащих аудиту, анализу записей аудита, их защите и хранению.

Аудит. Периодический контроль (просмотр) протокольной информации в системе с целью обеспечения ее безопасности или повышения производительности.

Аутентификация пользователя (абонента). Проверка соответствия пользователя предъявляемым им идентификатору и паролю. Установление подлинности пользователя.

Аутентификация сообщения. Добавление к блоку данных контрольного поля для обнаружения любых изменений в данных.

Безопасность информационной системы. Свойство информационной системы противостоять попыткам несанкционированного доступа к ресурсам.

Безопасность компьютерной системы. Свойство компьютерной системы противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям и навязыванию ложной информации, выходу (выводу) из строя, разрушению ресурсов и системы в целом.

Блокировка данных. Защита файла или его части (блока, записи) путем запрещения доступа к ним всех пользователей за исключением одного.

Блокировка. Запрет на выполнение последующих действий.

Верификация. Доказательство правильности работы программы, комплекса, системы.

Вирус. Программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии. Часто содержит логические бомбы или создает различные аудио- и видеоэффекты.

Восстановление. Возврат к исходному (доаварийному) состоянию или к нормальному функционированию.

Готовность системы. Мера способности системы выполнять свои функции при нахождении в рабочем состоянии. Количественно готовность можно оценить с помощью коэффициента готовности.

Группа пользователей. Один или несколько пользователей, объединенные общими требованиями доступа к некоторым ресурсам и выступающие как один субъект доступа к ресурсам системы.

Данные. Информация, представленная в формализованном виде, пригодном для интерпретации, обработки и пересылки ее автоматическими средствами при возможном участии человека.

Дезинформация. Сознательное искажение передаваемых сведений с целью ложного представления у лиц, использующих эти сведения; передача ложной информации.

Дешифрование. Процесс восстановления открытой информации из закрытой. Выполняется с помощью аналитических методов позволяющих определить использованный ключ или понизить стойкость алгоритма шифрования.

Диагностика. Контроль, проверка и прогнозирование состояния объекта. Цель технической диагностики – обнаружение неисправностей и выявление элементов, ненормальное функционирование которых является причиной возникновения неисправностей.

Достоверность. Свойство информации быть правильно воспринятой; вероятность отсутствия ошибок.

Доступ. Взаимодействие между субъектом и объектом, обеспечивающее передачу информации между ними.

Доступность. Свойство объекта (системы, ресурса) быть доступным для использования по назначению авторизованным субъектом во время, определенное регламентом работы.

Живучесть. Свойство системы оставаться работоспособной в условиях внешних воздействий.

Журнал. Набор данных (файл), используемый для сбора и учета статистической информации, различных сообщений и других данных.

Задание по безопасности (ЗБ). Задание по безопасности содержит цели и требования безопасности ИТ для конкретно определенного ОО и определяет функции безопасности и меры обеспечения уверенности в безопасности, предоставляемые этим ОО для выполнения установленных требований. В ЗБ может быть заявлено о соответствии одному или нескольким ПЗ, и оно составляет основу для оценки.

Защита от несанкционированного доступа (НСД). Предотвращение или существенное затруднение несанкционированного доступа к программам и данным путем использования аппаратных, программных и криптографических методов и средств защиты, а также проведения организационных мероприятий. Наиболее распространенным программным методом защиты является парольная система.

Защита. Средства для ограничения доступа или использования всех или части ресурсов системы; юридические, организационные и программно-технические меры предотвращения несанкционированного доступа к объектам системы (аппаратуре, программам и данным).

Идентификатор пользователя. Символическое имя, присваиваемое отдельному пользователю (лицу или группе лиц – субъекту).

Идентификация пользователя. Присвоение пользователю (субъекту доступа) идентификатора.

Идентификация группы. Присвоение группе пользователей, имеющих общие требования к защите некоторых ресурсов, идентификатора.

Идентификация. Присвоение субъектам и объектам доступа идентификаторов.

Ключ. Код, на основе которого производится шифрование.

Ключевая система. Совокупность криптографических ключей и правил обращения с ними при обеспечении криптографической защиты информации.

Компрометация. Утеря конфиденциальной (критичной) информации либо получение ее неавторизованным для этого субъектом (лицом, программой, процессом и т.п.).

Контроль доступа. Предупреждение несанкционированного использования какого-либо ресурса, включая предупреждение использования ресурса несанкционированным способом.

Контрольная сумма. Уникальное число, поставленное в соответствие некоторой информации по определенному алгоритму, позволяющее судить о целостности этой информации.

Конфиденциальность. Свойство информации, состоящее в том, что она не может быть обнаружена и сделана доступной отдельным лицам, программам, процессам без разрешения.

Концепция. Определенный способ понимания, трактовки каких-либо явлений, основная точка зрения, руководящая идея для их освещения, ведущий замысел, конструктивный принцип различных видов деятельности

Криптографическая система. Совокупность технических и/или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

Критичность. Критерий защиты информации, позволяющий классифицировать информацию и установить уровни защиты информации в системе.

Мониторинг. Отображение текущего состояния контролируемых объектов системы с целью своевременного выявления угроз безопасности.

Надежность. Характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени. Показателями надежности являются вероятность безотказной работы, среднее время наработки на отказ, среднее время восстановления.

Нормативный (нормативно-технический) документ. Документ, содержащий требования, правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов, обязательный для исполнения в пределах области распространения.

Объект защиты. Ресурс системы, подлежащий защите.

Объект оценки (ОО). Та часть продукта или системы, которая является предметом оценки. Угрозы, цели и требования безопасности **объекта оценки**, а также краткая спецификация функций безопасности и мер по обеспечению уверенности в безопасности излагаются в **задании по безопасности (ЗБ)**, которое используется оценщиками как основание при оценке.

Оператор. Тип пользователя, выполняющего свои функциональные обязанности путем непосредственного взаимодействия с ЭВМ.

Описание объекта оценки. Устанавливает контекст оценки. Поскольку рассматривается определенная категория **объекта оценки**, могут быть указаны совокупность предположений и условия применения **объекта оценки** этой категории.

Орган сертификации. Орган, уполномоченный установленным образом проводить сертификацию.

Отказ. Ситуация, в которой система или какая-то ее часть оказывается неспособной выполнять возлагаемые на нее функции.

Оценка задания по безопасности. Цель оценки **задания по безопасности** состоит в том, чтобы показать, что **задание по безопасности** является полным, непротиворечивым и технически грамотным, и поэтому оно пригодно в качестве основы для оценки **объекта оценки**.

Оценка профиля защиты. Цель оценки **профиля защиты** состоит в том, чтобы показать, что **профиль защиты** является полным, непротиворечивым и технически грамотным. В дальнейшем применение **профиля защиты** предусмотрено при изложении требований к оцениваемому **объекту оценки**.

Оценка. Основными исходными материалами для оценки являются задание по безопасности, совокупность свидетельств об **объекте оценки** и собственно **объект оценки**. Ожидаемым результатом процесса оценивания является содержащееся в одном или нескольких отчетах, документирующих заключения оценки, подтверждение того, что **объект оценки** удовлетворяет требованиям **задания по безопасности**.

Пароль ресурса. Идентификатор ресурса (строка символов), который является его секретом. Доступ к ресурсу получает тот пользователь, который знает **П. ресурса.**

Пароль. Секретный признак, подтверждающий право доступа; обычно это строка символов.

Парольная защита ресурса. Возможность системы предоставить доступ к ресурсам, защищенным паролями, только тем пользователям, которым известны пароли.

Парольная история. Возможность системы хранить предыдущие пароли и при изменении пароля сравнивать новый пароль с хранимыми, чтобы запретить частое использование одних и тех же паролей.

Подпись электронная. См. **Подпись цифровая**.

Подпись цифровая. Последовательность двоичных цифр, сформированная с использованием информации, принадлежащей только подписывающему лицу, и некоторой контрольной суммы (см.) подписываемых данных, добавляемая к блоку данных (электронному сообщению) или результату их криптографического преобразования, позволяющая получателю данных проверить подлинность источника и целостность данных, что обеспечивает защиту от подлога или подделки.

Подпись. Собственноручно написанная фамилия.

Полномочия. Права субъекта (пользователя, процесса, программы, системы) на осуществление тех или иных действий над защищаемым ресурсом.

Пользователь. Зарегистрированный в системе субъект доступа к ее ресурсам.

Протокол. Набор данных (файл), содержащий информацию о произошедших событиях и действиях субъектов в системе.

Протоколирование. Регистрация действий субъектов и событий, имеющих место в системе (подсистеме).

Профиль защиты (ПЗ). Профиль защиты определяет независимую от реализации совокупность требований и целей безопасности для некоторой категории продуктов или систем, отвечающую одинаковым запросам потребителей в безопасности ИТ. **Профиль защиты** предназначен для неоднократного применения и определения требований, которые признаны полезными и эффективными для достижения установленных целей.

Расшифрование. Операция, обратная шифрованию и связанная с восстановлением исходного текста из зашифрованного.

Реализация объекта оценки. Воплощение **объекта оценки** в соответствии с его спецификацией.

Регистрация. Документирование (фиксация) идентификатора и пароля в установленных для этого ресурсах системы.

Резервирование. Комплекс мер по обеспечению доступности системы в случае сбоев или отказов технических средств.

Резервное копирование. Комплекс мер по созданию резервных копий информации в системе с целью обеспечения гарантированного восстановления ее работоспособности в случае частичного или полного разрушения (потери) информации.

Ресурс. Любой из компонентов системы (лицо, программа, процедура, набор данных, файл, компьютер, сеть и т.д.).

Риск. Риск есть стоимостное выражение вероятности события, ведущего к потерям.

Санкционирование. Предоставление права пользования услугами системы, например, права доступа к данным.

Сбой. Кратковременный, неустойчивый отказ оборудования.

Сертификат защиты (сертификат). Документ, удостоверяющий соответствие средств вычислительной техники или автоматизированной системы набору требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных.

Сертификат соответствия. Документ, выдаваемый в соответствии с правилами сертификации, указывающий, что обеспечивается необходимая уверенность в том, что должным образом идентифицированная продукция, процесс или услуга, соответствует конкретному стандарту или другому нормативному документу.

Сертификация соответствия. Действие третьей стороны, доказывающее, что обеспечивается необходимая уверенность в том, что должным образом идентифицированная продукция, процесс или услуга, соответствуют конкретному стандарту или другому нормативному документу. (Третья сторона – лицо или орган, признанные независимыми от сторон, участвующих в рассматриваемом вопросе).

Сертификация уровня защиты. Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

Сертификация. Официальная аттестация продукта.

Система защиты данных. Комплекс аппаратных, программных и криптографических средств, а также мероприятий, обеспечивающих защиту данных от случайного или преднамеренного разрушения, искажения и использования.

Система разграничения доступа. Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Система сертификации. Система, располагающая собственными правилами процедуры и управления для проведения сертификации соответствия.

Спецификации безопасности объекта оценки. Определяют фактически существующую или предполагаемую реализацию **объекта оценки**.

Список доступа. Перечень пользователей, которым разрешен доступ к ресурсу (объектам), с указанием предоставленных прав доступа.

Среда безопасности. Законы, политики безопасности организаций и т.д., определяющие условия использования **объекта оценки**. Сюда также включены угрозы, относящиеся к среде **объекта оценки**.

Субъект доступа. Пользователь (лицо) или процесс, действия которых регламентируются правилами разграничения доступа.

Субъект защиты. См. **Пользователь**.

Трафик. Поток сообщений в сети передачи данных; рабочая нагрузка линии связи.

Требования безопасности объекта оценки. Преобразование целей безопасности ИТ в совокупность специальных требований к функциям и уверенности в безопасности, относящихся к **объекту оценки** и его среде ИТ.

Угроза. Потенциальная возможность нарушения защиты от несанкционированного доступа.

Управление доступом. Определение, ограничение, и контроль доступа пользователей, программ и процессов (субъектов) к данным, программам и устройствам системы (объектам).

Уязвимость. Свойство системы, которое может привести к нарушению ее защиты при наличии угрозы.

Цели безопасности. Сформулированное намерение противостоять идентифицированным угрозам и/или удовлетворять принятой политике безопасности организации и предположениям.

Целостность наборов данных, сообщений. Свойство набора данных, сообщений, означающее, что они не могут быть изменены или разрушены без санкции на доступ; условия, при которых данные (сообщения) сохраняются для использования по назначению.

Целостность. Состояние данных или компьютерной системы, в которой данные или программы используются установленным образом, обеспечивающим устойчивую работу системы; автоматическое восстановление в случае обнаружения системой потенциальной ошибки; автоматическое использование альтернативных компонент вместо вышедших из строя.

Шифрование канальное. Реальное применение процедур шифрования данных в канале передачи данных коммуникационной системы.

Шифрование с открытым ключом. Криптографический метод, в котором используются раздельные ключи для шифрования (открытый ключ) и расшифрования (секретный ключ).

Шифрование. Преобразование данных для получения шифрованного текста.

Литература
(с краткой аннотацией)

1. Брагг Роберта. Система безопасности Windows 2000.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001.

   Пособие для профессионалов, в котором излагаются основы стратегии безопасности для систем, работающих под управлением Windows 2000. Позволяет читателю понять основные концепции безопасности, освоить методы управления доступом к Windows с помощью инструментов безопасности, настроить систему защиты удаленного доступа, установить или обновить операционную систему с учетом требований безопасности.

2. Гайкович В., Лершин А. Безопасность электронных банковских систем. – М.,1993.

   Компьютерные системы – одна из наиболее уязвимых сторон современных банков и финансовых организаций, притягивающих злоумышленников. Они нуждаются в защите. Как защищать свои системы? От кого? Сколько это будет стоить? Как вести себя в критических ситуациях.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2 кн. Кн. 1. – М.: Энергоатомиздат, 1994.

   В книге с позиций системно-концептуального подхода рассмотрен широкий круг вопросов, относящихся к защите информации, накапливаемой, хранимой и обрабатываемой в современных автоматизированных системах и сетях.

4. Герасименко В.А., Малюк А.А. Основы защиты информации. – М., 1997.

   Рекомендовано Министерством общего и профессионального образования РФ в качестве учебника для вузов.

5. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. Серия «Информатизация России на пороге XXI века». – М.: СИНТЕГ, 1999.

   Впервые в отечественной литературе рассматривается концепция информационной войны. Показан размах, который приобрела эта концепция на Западе, в частности, приводятся взгляды Министерства обороны США на проблему ведения информационной войны. Анализируются средства и методы ведения информационной войны, возможные объекты атаки и средства их защиты.

6. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему / Под науч. ред. Д.П. Зегжды, В.В. Платонова. – СПб.: Мир и семья-95, 1997.

   Это первое отечественное издание, посвященное уникальной технологии создания защищенных систем обработки информации, где рассмотрены проблемы практической реализации моделей безопасности. В книге дается представление о защищенной информационной системе, анализируется существующий опыт разработки подобных систем и причины нарушения их безопасности, что позволяет предложить качественно новые методы и средства их защиты.

7. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2001.

   Рассматриваются технологические основы защиты информационного взаимодействия в компьютерных сетях при их подключении к открытым коммуникациям, методы и средства межсетевого экранирования для зашиты локальных сетей от несанкционированных воздействий со стороны открытых коммуникаций, базовые протоколы и средства построения защищенных виртуальных сетей на различных уровнях эталонной модели сетевого взаимодействия.

8. Зубанов Ф. Windows NT – выбор «профи». 2-е изд., испр. и доп. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1997.

   Основное внимание в книге уделяется вопросам планирования, установки, защиты и администрирования, обеспечивающих безотказную работу вычислительной системы. В частности, рассматриваются доменная структура сетей Microsoft, учетные записи пользователей и групп, управление политикой ведения учетных записей, вопросы отказоустойчивой работы с дисками, кластерные технологии, файловые системы, безопасная работа в глобальных сетях и при подключении к Internet. Кроме того, описываются особенности новой, 4 версии Windows NT.

9. Каплан А., Нильсен М.Ш. Windows 2000 изнутри: Пер. с англ. – М.: ДМК, 2000.

Большую часть книги занимает критический обзор архитектуры Windows 2000 в сравнении с Windows NT 4.0 и другими сетевыми ОС, например UNIX и NetWare, а также Windows 95/98. Подробно описываются достоинства и недостатки нового пользовательского интерфейса, средств администрирования на основе MMC, службы каталогов Active Directory, технологии кластеризации. Много внимания уделяется реализации сетевого протокола TCP/IP, который полностью заменил устаревший NetBIOS, а также файловой системе NTFS 5.

10. Кастер Х. Основы Windows NT и NTFS / Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1996.

Взгляд изнутри на проект, философию, архитектуру и будущее операционной системы Microsoft Windows NT.

11. Компьютерная преступность и информационная безопасность / Под общ. ред. А.П. Леонова. – Мн.: АРИЛ, 2000. – 552 с.

В рамках междисциплинарного подхода к исследованию проблемы информационной безопасности рассмотрены актуальные вопросы обеспечения гарантированной защиты информации в компьютерных системах и сетях.

12. Леонов А.П., Леонов К.А., Фролов Г.В. Безопасность автоматизированных банковских и офисных систем. – Мн.: НКП Беларуси, 1996.

Монография посвящена проблеме комплексной защиты информационной безопасности автоматизированных банковских и офисных систем. Рассматриваются системная методология защиты информационной безопасности, эволюция аппаратно-программных платформ автоматизации банков и офисов, методы и средства комплексной зашиты информации в автоматизированных банковских и офисных системах.

13. Люцарев В.С., Ермаков К.В., Рудный Е.Б., Ермаков И.В. Безопасность компьютерных сетей на основе Windows NT – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1998.

В книге изложен взгляд независимых специалистов на проблемы функционирования и защиты компонентов операционной системы Microsoft Windows NT.

14. Петренко С.А., Петренко А.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с.

В книге содержится комплексное описание всех основных вопросов аудита безопасности корпоративных систем Internet/Intranet в соответствии с требованиями международных стандартов ISO 15408, ISO 17799 (BS7799), BSI и COBIT.

15. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацкевич И.В. – М.: Радио и связь, 2000. – 168 с.

Рассматривается общая концепция защиты информации в операционных системах, аппаратное и программное обеспечение защитных функций ОС.

16. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4: Пер. с англ. В 2 т. Т. 1. – М.: Мир, 1999.

В томе 1 рассмотрены концепция и модель безопасности сети, вопросы системной политики, а также защита от персонала, шифрование, удаленный доступ.

17. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4: Пер. с англ. В 2 т. Т. 2. – М.: Мир, 1999.

В томе 2 подробно рассмотрены вопросы защиты компонентов сети, а также использование брандмауэров, серверов полномочий и пакетной фильтрации. В конце книги описана система безопасности Windows NT5 и приведен обширный толковый словарь терминов по компьютерной безопасности.

18. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издатель Молгачева С.В., 2001.

Книга посвящена рассмотрению широкого круга проблем компьютерной безопасности. Наряду с теоретическим и нормативно-методическим материалом содержит описание практических подходов к реализации систем безопасности.

Св. план 2003, поз. 22

Учебное издание

Иванченко Юрий Иванович,
Деев Алексей Юрьевич,
Заговалко Алексей Владимирович

ИНТЕЛЛЕКТУАЛЬНЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие
для студентов специализации
«Интеллектуальные компьютерные технологии защиты информации»
специальности «Искусственный интеллект»

в 3-х частях

Часть 1
Общие положения защиты информации

Редактор Е.Н. Батурчик
Компьютерная верстка: А.Ю. Деев, А.В. Заговалко

Подписано в печать .12.2003.	Формат 60x84 1/8.	Бумага офсетная.
Печать ризографическая.	Гарнитура Ариал.	Усл. печ. л.
Уч.-изд. л. 6,5.	Тираж 100 экз.	Заказ 226.

Издатель и полиграфическое исполнение
Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Лицензия ЛП № 156 от 30.12.2002.
Лицензия ЛВ № 509 от 03.08.2001.
220013, Минск, П. Бровки, 6.