Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования

Владимирский государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА
ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
КНИГА 10

Д.А. ПОЛЯНСКИЙ

ОЦЕНКА ЗАЩИЩЕННОСТИ

Учебное пособие

Владимир 2005

УДК 519.6 (075)
ББК 22.186
П54

Редактор серии кандидат технических наук М.Ю. Монахов

Рецензенты:

Кандидат технических наук, доцент
начальник кафедры специальной техники
и информационных технологий
Владимирского юридического института
А.С. Клементьев

Кандидат физико-математических наук, доцент
Владимирского государственного университета
А.В. Александров

Печатается по решению редакционно-издательского совета
Владимирского государственного университета

Полянский, Д. А.

П54 Оценка защищенности : учеб. пособие / Д. А. Полянский ; Владим. гос. ун-т. – Владимир : Изд-во Владим. гос. ун-та, 2005. – 80 с. (Комплексная защита объектов информатизации. Кн. 10 / под. ред. М. Ю. Монахова).

ISBN 5-89368-613-6

Это десятая книга из серии «Комплексная защита объектов информатизации». В ней представлен систематизированный материал по методам качественной и количественной оценки защищенности объектов информатизации.

Учебное пособие предназначено для студентов специальности 090104 (075400) «Комплексная защита объектов информатизации» дневной формы обучения. Может быть полезно широкому кругу читателей, самостоятельно осваивающих вопросы защиты информации.

Табл. 4. Ил. 6. Библиогр.: 24 назв.

УДК 519.6 (075)
ББК 22.186

ISBN 5-89368-613-6

ОГЛАВЛЕНИЕ

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

АБ – архитектура безопасности
АС – автоматизированная система
ЗИ – защита информации
ИБ – информационная безопасность
ИП – информационный поток
ИС – информационная система
ИТ – информационные технологии
КСИБ – комплексная система информационной безопасности
МО – монитор обращений
НСД – несанкционированный доступ
ОИ – объект информатизации
ОС – операционная система
ПЗ – профиль защиты
ПО – программное обеспечение
РТКС – распределенная телекоммуникационная система
СВТ – средства вычислительной техники
СЗИ – система защиты информации
СИБ – система информационной безопасности

ВВЕДЕНИЕ

Учебное пособие является десятой книгой из серии «Комплексная защита объектов информатизации», подготовленной кафедрой «Информатика и защита информации» Владимирского государственного университета.

Пособие предназначено в первую очередь для студентов специальности «Комплексная защита объектов информатизации».

В настоящее время ИБ предприятия – один из ведущих факторов его эффективного развития. Информация имеет реальный стоимостный вес, который четко определяется прибылью, получаемой при ее использовании, или ущербом, который может быть нанесен предприятию в случае использования ее другими лицами. Постоянно растет доля расходов организаций на обеспечение целостности информации и защиты ее от возможных внешних угроз. Однако предприятия не хотят выбрасывать деньги на ветер; они хотят покупать только то, что действительно необходимо для построения надежной СЗИ и при этом с минимальными расходами.

В связи с этим остро встает вопрос оценки эффективности средств защиты и оценки защищенности всей информационной системы в целом. Произведя такую оценку, можно выбрать наиболее эффективную систему защиты как с функциональной, так и с экономической точки зрения в каждом конкретном случае.

Как и любая другая оценка, оценка защищенности информационного ресурса может основываться как на количественных, так и на качественных показателях. Очевиден тот факт, что защита информации должна носить комплексный характер. В настоящем учебном пособии проведен анализ различных методик качественных и количественных оценок защищенности с целью их интеграции и получения комплексной достоверной оценки защищенности СИБ. Это такие методики, которые бы учитывали как технические аспекты рассматриваемой системы (архитектуру, состав, взаимодействие компонентов, их свойства), так и экономические и организационные моменты (эффективность использования ресурсов, возможности оптимизации, человеческий фактор).

Данное учебное пособие состоит из шести глав. В нем рассматриваются следующие вопросы.

1. Сущность понятия "коммерческая тайна предприятия" и необходимость ее защиты. Анализ угроз безопасности ОИ и неформальная модель нарушителя (глава 1).

2. Анализ требований российских, европейских и международных стандартов информационной безопасности как основы первичной качественной ОИ (глава 2).

3. Задачи, принципы и этапы построения, направления работ по созданию КСИБ, отвечающей требованиям стандартов. Формальная модель и механизм функционирования такой КСИБ (глава 3).

4. Качественные методы оценки СИБ: оценка уровня безопасности и оценки рисков (глава 4).

5. Количественные методы оценки СИБ: метод экспертных оценок, метод информационных потоков, графовый метод и метод весовых коэффициентов (глава 5).

6. Комплексный подход к оценке эффективности СИБ: качественные и количественные аспекты оценки эффективности и оценка экономической эффективности (глава 6).

Глава 1. АНАЛИЗ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

1.1. Сущность коммерческой тайны и необходимость ее защиты

Говоря о защите какой-либо информации, следует прежде всего выяснить, к какой категории она относится. Определяют следующую классификацию тайн по шести категориям [9]:

- государственная тайна,
- коммерческая тайна,
- банковская тайна,
- профессиональная тайна,
- служебная тайна,
- персональные данные.

Последние пять составляют конфиденциальную информацию.

Коммерческая тайна предприятия – это не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и др., передача или утечка которых может нанести ущерб интересам предприятия.

В соответствии с Гражданским кодексом Российской Федерации (Ч. 1, ст. 139, п. 1) информация составляет служебную или коммерческую тайну в случае ее действительной или потенциальной коммерческой ценности в силу неизвестности ее третьим лицам, отсутствия к ней свободного доступа на законном основании и принятия обладателем ее мер по охране ее конфиденциальности.

Сведения, составляющие коммерческую тайну и подлежащие охране, должны удовлетворять следующим пяти критериям оценки [12, 16]:

1. их открытое использование связано с ущербом для предприятия;
2. они не являются общеизвестными или общедоступными на законных основаниях;
3. предприятие может осуществить надлежащие меры по сохранению их конфиденциальности по соображениям экономической и иной выгоды;
4. эти сведения нуждаются в защите, так как они не являются государственными секретами и не защищены авторским и патентным правом;
5. сокрытие этих сведений не наносит ущерба обществу.

Действующее законодательство предоставляет право администрации предприятия самостоятельно решать многие вопросы обеспечения его безопасности.

Но современное общество заинтересовано в широкой доступности информации в целях ускорения научно-технического прогресса. В рыночной экономике информация является товаром, и ее получение, хранение, передача и использование должны подчиняться законам товарно-денежных отношений. Построение экономически эффективной КСИБ напрямую зависит от того, насколько точно проведена оценка стоимости защищаемой информации.

Возможные потери от утечки информации приводят к конкретной величине экономического ущерба. Поэтому и затраты на защиту такой информации должны быть экономически ограничены суммой возможных потерь. При излишнем засекречивании коммерческой информации рост расходов на эти цели не адекватен снижению вероятности утечки более ценных сведений. Поэтому нецелесообразно охранять как коммерческую тайну не всю информацию предприятия, связанную с производственным процессом, а только ту ее часть, которая обеспечивает возможность расширять рынок сбыта, улучшать качество продукции, заключать выгодные сделки с партнерами.

В нашей стране в настоящее время отсутствует законодательная защита коммерческой тайны, не практикуется широкое применение мер экономической ответственности при решении этой проблемы, не наработана соответствующая судебная практика. Возможно, именно поэтому в реальной жизни предприятий процветает явное и тайное безвозмездное заимствование интеллектуальной собственности и коммерческой информации конкурентов.

Экономический ущерб наносится предприятию, когда его сотрудники подрабатывают по совместительству в других местах, используя при этом информацию, созданную на основном предприятии, но юридически не закрепленную в его собственности. Но именно этот интеллектуальный продукт часто является наиболее ценным капиталом предприятия.

Точный стоимостный расчет совокупной величины всех возможных потерь достаточно сложен, а иногда и невозможен из-за отсутствия достоверных исходных данных. Поэтому в большинстве случаев достаточно укрупненной экспертной оценки потерь предприятия, обусловленных несоблюдением требований ЗИ.

Ответственность за нарушения правил коммерческой тайны

В основном предприятия несут значительные потери от утечки информации в результате НСД к ЭВМ. Ключевым моментом, снижающим

вероятность НСД, является система личного кодирования каждого из работников предприятия, ограничивающая возможность работника в использовании тех программ, которые не относятся к его прямым служебным обязанностям.

Определенным сдерживающим фактором предотвращения преступлений в сфере компьютерной информации могут послужить положения нового Уголовного кодекса Российской Федерации (ст. 272), предусматривающего наказание за такого рода преступления от штрафа до лишения свободы на срок до двух лет. Причем если такие действия совершены группой лиц по предварительному сговору или организованной группой, то размеры уголовной ответственности увеличиваются.

Современное международное право не дает четких и однозначных норм, регулирующих данные вопросы. Это объясняется, прежде всего, сложностью и масштабностью проблемы, а также разными подходами к ее решению в зависимости от уровня развития рыночных отношений, конкурентной борьбы, специфики исторических и экономических условий.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

УК РФ (ст. 183) предусмотрена ответственность за сбор сведений, составляющих коммерческую или банковскую тайну, вплоть до лишения свободы на срок до двух лет. Ст. 138 предусматривает также ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Уголовно наказуемым преступлением являются также незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

1.2. Анализ угроз безопасности

Около 90% всей необходимой информации о конкурентах может быть получено легальными методами. Остальную информацию (как правило, наиболее ценную и тщательно охраняемую) дает промышленный шпионаж. Публикации в печати [8] говорят о тесном переплетении в деятельности конкурирующих фирм легальных и нелегальных методов получения информации друг о друге.

Одновременно с развитием промышленного шпионажа постоянно совершенствуются и средства защиты тайны предпринимателей. Так, на-

пример, в промышленно развитых странах уже используются такие прогрессивные новшества, как биометрические системы ограничения допуска.

Для предотвращения утечки коммерческой тайны через работников руководитель предприятия должен знать их реальные права и предоставлять только ту документацию, которая необходима для выполнение служебных функции, а не любую, которую они потребуют. Прежде всего, это относится к действиям работников государственных организаций.

Анализ угроз безопасности проводится с целью определения требований к защищенности циркулирующей в системе информации.

Под угрозой обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Угрозы безопасности обычно подразделяют на естественные и искусственные, а последние, в свою очередь, на непреднамеренные и преднамеренные. Основными видами угроз информационной безопасности являются [4, 5]:

- стихийные бедствия и аварии;
- сбои и отказы оборудования;
- последствия ошибок проектирования и разработки компонентов информационной системы;
- ошибки эксплуатации (пользователей, операторов и другого персонала);
- преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Разделение угроз по степени вероятности исполнения должно проводиться на основе данных конкретного предприятия. Но в целом на первом месте обычно находятся угрозы от непрофессиональных действий сотрудников самого предприятия [12, 16, 21].

Анализ угроз безопасности всегда проводится совместно с анализом каналов проникновения в систему и каналов утечки информации. Все каналы проникновения в систему и утечки информации разделяют на прямые и косвенные. Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение необходимо.

По типу основного средства, используемого для реализации угрозы, все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или техника. По способу получения информации потенциальные каналы доступа можно разделить на физические, электромагнитные, информационные [3].

Доступ к информации без использования программ. Успешное развитие программных средств ЗИ привело к тому, что НСД к информации с использованием программ становится в настоящее время все более затруднительным для злоумышленников. Доступ к информации иначе, чем взлом программного обеспечения, имеет целью незаконное получение паролей к системе или иной информации, которая поможет нарушить безопасность системы.

Одним из способов получения паролей непрограммным путем являются звонки по телефону на предприятие для выявления тех, кто имеет необходимую информацию, и затем звонок администратору от имени служащего с неотложной проблемой доступа к системе. В крупных компаниях лица, ответственные за систему, не знают всех сотрудников, поэтому появляется возможность манипулировать действиями администраторов. Телефон облегчает эту задачу, так как администратор не видит абонента, который может звонить даже из другого города или страны.

Системные администраторы часто сталкиваются с забывчивостью пользователей, особенно если сотрудники редко "входят" в систему. В таких случаях ответственное лицо старается побыстрее положить трубку, и ему хватает того, что пользователь знает свое имя входа в систему (в таких случаях редко спрашивают фамилию, должность сотрудника).

1.3. Неформальная модель нарушителя

Анализ угроз безопасности и каналов утечки позволяет построить неформальную модель нарушителя, которая отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. [1].

Нарушитель – это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства [9].

При разработке модели нарушителя определяются предположения:

- о категориях лиц, к которым может принадлежать нарушитель;
- о мотивах действий нарушителя;
- о квалификации нарушителя и его технической оснащенности;
- о характере возможных действий нарушителей.

Возможны следующие типы нарушителей (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.) [18]:

6. *"Неопытный (невнимательный) пользователь"* – сотрудник организации, который может предпринимать попытки выполнения запрещен-

ных операций, доступа к защищаемым ресурсам организации с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

7. *"Любитель"* – сотрудник организации, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из "спортивного интереса". Может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей других пользователей), недостатки в построении системы защиты и доступные ему штатные и нештатные программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств);

8. *"Мошенник"* – сотрудник организации, который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные аппаратные и программные средства от своего имени или от имени другого сотрудника.

9. *"Внешний нарушитель (злоумышленник)"* – постороннее лицо или сотрудник организации, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения безопасности информации, методов и средств взлома систем защиты, характерных для сетей общего пользования;

10. *"Внутренний злоумышленник"* – сотрудник подразделения организации, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками организации. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства, методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне – из сетей общего пользования.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес. А классификация нарушителей может быть проведена:

- по уровню знаний об ИС;
- уровню возможностей (используемым методам и средствам);

- времени действия;

- месту действия;

Внутренним нарушителем может быть лицо из следующих категорий персонала организации [18]:

- зарегистрированные конечные пользователи ИС организации (сотрудники подразделений организации);

- сотрудники подразделений организации, не допущенные к работе с ИС;

- персонал, обслуживающий технические средства ИС организации (инженеры, техники);

- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);

- технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты ИС);

- сотрудники службы безопасности организации;

- руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями [18]:

- уволенные сотрудники организации;

- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);

- посетители (приглашенные представители организаций, граждане) представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.;

- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

- лица, случайно или умышленно проникшие в ИС организации из внешних (по отношению к организации) сетей телекоммуникации (хакеры).

Пользователи и обслуживающий персонал из числа сотрудников организации имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. По-

лученные в организации знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников организации всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в ИС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными сотрудниками организации и криминальными структурами.

Сотрудники организации, занимающиеся разработкой, поставкой и ремонтом оборудования ИС, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей [10]:

- работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей – сотрудников организации по преодолению системы защиты;

- нарушитель скрывает свои несанкционированные действия от других сотрудников организации;

- несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и ИС, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Но правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и т.п. характеристики – важная составляющая успешного проведения анализа рисков и определения требований к составу и характеристикам КСИБ.

Кратко о главном

Коммерческая тайна является одним из видов конфиденциальной информации. Действующее законодательство предоставляет право администрации предприятия самостоятельно решать многие вопросы обеспечения его безопасности и охраны коммерческой тайны. УК РФ предусматривает ответственность за нарушение правил коммерческой тайны.

Анализ угроз безопасности и каналов утечки проводится с целью определения требований к защищенности циркулирующей в системе информации и позволяет построить неформальную модель нарушителя, которая отражает его практические и теоретические возможности, знания, время и место действия и т.п. Такая модель позволяет определить круг категорий внешних и внутренних нарушителей, установить их возможные мотивы и предположения о характере действий.

Успешное развитие программных средств ЗИ привело к тому, что НСД к информации с использованием программ становится в настоящее время все более затруднительным для злоумышленников и все большую опасность для предприятий вызывает НСД непрограммным путем.

Контрольные вопросы

1. Перечислите категории тайн. Дайте определение *коммерческой тайны*.
2. Какие есть критерии оценки сведений, составляющих коммерческую тайну?
3. Какой экономический ущерб предприятию могут наносить его работники?
4. Какая ответственность установлена законами России за нарушение правил коммерческой тайны?
5. Что такое *угроза информационной безопасности* и какие виды угроз бывают?
6. Классифицируйте каналы проникновения в ИС и каналы утечки информации.
7. Что из себя представляет НСД к информации без использования программ?
8. Дайте определение *нарушителя* и перечислите типы нарушителей.
9. Перечислите категории лиц, которые могут быть внутренними нарушителями.
10. Перечислите категории лиц, которые могут быть внешними нарушителями.
11. Чем определяются действия различных нарушителей?

Глава 2. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Первые стандарты безопасности

Первичная качественная оценка уровня информационной безопасности ОИ может быть проведена на основе анализа соответствия защищаемого ОИ требованиям стандартов информационной безопасности.

Оранжевая книга

Исторически первым стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации информационной безопасности во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" [24]. Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года.

В "Оранжевой книге" доверенная система (*trusted computer system*) определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

"Оранжевая книга" поясняет понятие безопасной системы (*secure system*), которая "управляет с помощью соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию". Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

Одним из основных понятий при оценке степени доверия безопасности является понятие *доверенной вычислительной базы* (ДВБ) (*trusted computing base*). ДВБ – это совокупность защитных механизмов системы (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Ее качество определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Основное назначение ДВБ – выполнять функции МО (*reference monitor*), то есть контролировать допустимость выполнения субъектами

определенных операций над объектами (пассивными сущностями). МО проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором допустимых действий. МО должен обладать тремя качествами: изолированностью (необходимо предупредить возможность отслеживания его работы), полнотой (должен вызываться при каждом обращении) и верифицируемостью (должен быть компактным, чтобы его можно было проанализировать и протестировать).

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

Границу ДВБ называют *периметром безопасности* (*security perimeter*). С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне – нет.

Степень доверия оценивается по двум основным критериям:

- политика безопасности (*security policy*) – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности – это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия;

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

Политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом (*Discretionary Access Control*) – разграничение доступа к объектам, основанное на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состо-

ит в том, что некоторое лицо (владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту;

- безопасность повторного использования объектов (*object reuse*) – предохранение от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти, для дисковых блоков и магнитных носителей в целом;

- метки безопасности (*labels*), описывающие благонадежность субъекта, метка объекта – степень конфиденциальности содержащейся в нем информации;

- принудительное управление доступом (*Mandatory Access Control*). Для реализации принудительного управления с субъектами и объектами ассоциируются метки безопасности. Управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта.

Важным средством обеспечения политики безопасности является свойство протоколирования. Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться анализом регистрационной информации. Цель протоколирования – в каждый момент времени знать, кто работает в системе и что делает. Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей, так и в отношении событий.

Рассматривается два вида *гарантированности* – операционная (*operational*) и технологическая (*life-cycle*). Операционная гарантированность относится к архитектурным и реализационным аспектам системы, в то время как технологическая – к методам построения и сопровождения.

Операционная гарантированность включает в себя проверку архитектуры системы и ее целостности. Основная задача – убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

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

Классы безопасности. Определены четыре уровня доверия – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. Остальные уровни можно сформулировать так:

- уровень C – произвольное управление доступом;
- уровень B – принудительное управление доступом;
- уровень A – верифицируемая безопасность.

По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.

Всего имеется шесть классов безопасности – C1, C2, B1, B2, B3, A1. Необходимо отметить, что каждый следующий класс включает все требования к предыдущему и новые, более жесткие, требования:

1. Класс C1 (*Discretionary Security Protection*). Пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые ДВБ. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от НСД. ДВБ должна поддерживать область для собственного выполнения, защищенную от внешних воздействий и от попыток слежения за ходом работы. Должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов ДВБ.

2. Класс C2 (*Controlled Access Protection*). Все объекты должны подвергаться контролю доступа. Каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем. ДВБ должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой. Тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

3. Класс B1 (*Labeled Security Protection*). ДВБ должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом, а также обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам и взаимную изоляцию процессов путем разделения их адресных пространств.

4. Класс B2 *(Structured Protection)*. Метками должны снабжаться все ресурсы системы, прямо или косвенно доступные субъектам. ДВБ должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации. Должна быть предусмотрена возможность регистрации событий, связан-

ных с организацией тайных каналов обмена с памятью. Модель политики безопасности должна быть формальной. Для ДВБ должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс. В процессе разработки и сопровождения ДВБ должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, исходных текстах, работающей версии объектного кода, тестовых данных и документации.

5. Класс B3 *(Security Domains)*. Для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов. Должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом. ДВБ должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой. Должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий. Должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.

6. Класс A1 (*Verified Design*). Помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;

Интерпретация "Оранжевой книги" для сетевых конфигураций

Документ состоит из двух частей [19]. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Важнейшее понятие из них – *сетевая доверенная вычислительная база* (СДВБ), распределенный аналог ДВБ изолированных систем. СДВБ формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами СДВБ не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования меток безопасности, получается сеть, не удовлетворяющая требованию целостности меток.

Интерпретация отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит криптография, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством по сравнению с "Оранжевой книгой". Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. Доверенная система должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);

- наличие средств реконфигурирования для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;

- рассредоточенность сетевого управления, отсутствие единой точки отказа;

- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);

- выделение подсетей и изоляция групп пользователей друг от друга.

Одним из важнейших является понятие МО. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования МО.

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой МО, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации.

Рекомендации X.800

Выделяют следующие сервисы безопасности [19]:

- *аутентификация*. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и в некоторых случаях периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной);

- *управление доступом*. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети;

- *конфиденциальность данных*. Обеспечивает защиту от несанкционированного получения информации;

- *целостность данных*. Подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности;

- *неотказуемость* (невозможность отказаться от совершенных действий). Обеспечивает два вида услуг – неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

В табл. 2.1 указаны уровни эталонной семиуровневой модели OSI, на которых могут быть реализованы функции безопасности.

Таблица. 2.1

Распределение функций безопасности по уровням модели OSI

Функции безопасности	Уровень						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

Примечание. Здесь и далее знак + означает наличие данной функции на соответствующем уровне.

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- шифрование;
- электронная цифровая подпись;
- механизмы управления доступом;
- механизмы контроля целостности данных. Различают два аспекта целостности – целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
- механизмы аутентификации. Аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его

использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;

- механизмы нотаризации. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В табл. 2.2 сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Таблица 2.2

Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	–	–	+	–	–	–
Аутентификация источника	+	+	–	–	–	–	–	–
Управление доступом	–	–	+	–	–	–	–	–
Конфиденциальность	+	–	+	–	–	–	+	–
Избирательная конфиденциальность	+	–	–	–	–	–	–	–
Конфиденциальность трафика	+	–	–	–	–	+	+	–
Целостность соединения	+	–	–	+	–	–	–	–
Целостность вне соединения	+	+	–	+	–	–	–	–
Неотказуемость	–	+	–	+	–	–	–	+

2.2. Стандарт ISO/IEC 15408

Стандарт ISO/IEC 15408 – "Критерии оценки безопасности информационных технологий" [22] был издан 1 декабря 1999 года. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени

документов национального и межнационального масштаба. Данный стандарт также часто называют "Общими критериями" (ОК).

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами. В свою очередь, угрозы характеризуются следующими параметрами: источник угрозы, метод воздействия, уязвимые места, которые могут быть использованы, ресурсы, которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в требованиях безопасности, проектировании и эксплуатации.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

Как и "Оранжевая книга", ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Чтобы структурировать пространство требований, в "Общих критериях" введена иерархия "*класс-семейство-компонент-элемент*".

Классы (*class*) определяют наиболее общую, "предметную" группировку требований (например, функциональные требования протоколирования). Семейства (*family*) в пределах класса различаются по строгости и другим нюансам требований. Компонент (*component*) – минимальный набор требований, фигурирующий как целое. Элемент (*element*) – неделимое требование.

Между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в ОК представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

- идентификация и аутентификация;

- защита данных пользователя;

- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);

- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);

- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);

- доступ к объекту оценки;

- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);

- использование ресурсов (требования к доступности информации);

- криптографическая поддержка (управление ключами);

- связь (аутентификация сторон, участвующих в обмене данными);

- доверенный маршрут/канал (для связи с сервисами безопасности).

Некоторые недостатки ОК:

1. Отсутствие иерархической (объектной) структуры компонентов. Для функциональных требований применен "библиотечный подход", они не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

2. Отсутствие архитектурных требований к рассматриваемым субъектам и объектам. Очевидно, что безопасность системы, её соответствие функциональным требованиям напрямую зависит от архитектуры системы, совокупности её компонентов и характера связей между ними.

Требования доверия безопасности. Установление доверия безопасности основывается на активном исследовании объекта оценки. Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка требования для поэтапной детализации функций безопасности;

- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);

- тестирование;

- оценка уязвимостей (включая оценку стойкости функций безопасности);

- поставка и эксплуатация;

- управление конфигурацией;

- руководства (требования к эксплуатационной документации);

- поддержка доверия (для поддержки этапов жизненного цикла после сертификации);

- оценка профиля защиты;

- оценка задания по безопасности.

В ОК сделана весьма полезная вещь, не реализованная для функциональных требований – введены *оценочные уровни доверия*, которые предполагают наличие следующих элементов (каждый уровень, начиная со второго, расширяет набор требований предыдущих):

1. Анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

2. Наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск явных уязвимых мест.

3. Контроль среды разработки и управление конфигурацией объекта оценки.

4. Полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией.

5. Применение формальной модели политики безопасности, функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

6. Реализация предыдущего уровня в структурированном виде.

7. Формальная верификация проекта объекта оценки. Применима к ситуациям чрезвычайно высокого риска.

2.3. Международный стандарт ISO 17799

В 2000 году Международная организация по стандартизации совместно с Международной электротехнической комиссией выпустили международный стандарт ISO/IEC 17799 [23].

Стандарт определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска и т.д. в контексте информационной безопасности. В процессе внедрения стандарта создается так называемая система менеджмента информационной безопасности, цель которой – сокра-

щение материальных потерь, связанных с нарушением информационной безопасности. Важно, что стандарт призван как раз сэкономить предприятию средства, а в некоторых случаях даже спасти от банкротства, и не является каким-то внешним обязательным требованием, приводящим к появлению дополнительной статьи расходов.

ISO 17799 – это модель системы менеджмента, и в этом смысле не является техническим стандартом. Например, он не предписывает использование каких-то определенных алгоритмов шифрования. Единственный пункт стандарта (всего их более 100), непосредственно регламентирующий шифрование, содержит буквально следующее требование: "Особо важная информация должна быть зашифрована". Что считать важной информацией и как производить шифрование, предприятие должно решить самостоятельно, основываясь на общих принципах применения стандарта.

Следует подчеркнуть, что данный подход к информационной безопасности на основе целей менеджмента, а не фиксированных технических спецификаций, является принципиальным для ISO 17799 как стандарта системы управления.

ISO 17799 содержит сто с лишним элементов управления информационной безопасностью, распределенных по нескольким группам:

- *политика в области безопасности*. Задача элемента – обеспечить четкое управление и поддержку политики в области информационной безопасности со стороны руководства предприятия;

- *организация системы безопасности*. Задача элемента – создать организационную структуру, которая будет внедрять и обеспечивать работоспособность системы информационной безопасности в организации;

- *классификация ресурсов и управление*. Задача элемента – поддерживать адекватную информационную безопасность организации путем возложения персональной ответственности, а также классификации информационных ресурсов по необходимости и приоритету защиты;

- *безопасность и персонал*. Задача элемента – уменьшить риск человеческих ошибок, хищений и неправильного использования оборудования, в том числе путем эффективного обучения и внедрения механизма отслеживания инцидентов;

- *физическая и внешняя безопасность*. Задача элемента – предотвратить несанкционированный доступ, повреждение и нарушение работы информационной системы организации;

- *менеджмент компьютеров и сетей*. Задача элемента – обеспечить безопасное функционирование компьютеров и сетей;

- *управление доступом к системе*. Задача элемента – управлять доступом к деловой информации, предотвращать несанкционированный доступ и обнаруживать несанкционированную деятельность;

- *разработка и обслуживание системы*. Задача элемента – обеспечить выполнение требований безопасности при создании или развитии информационной системы организации, поддерживать безопасность приложений и данных;

- *обеспечение непрерывности работы*. Задача элемента – подготовить план действий в случае чрезвычайных обстоятельств для обеспечения непрерывности работы организации;

- *соответствие законодательству*. Задача элемента – обеспечить выполнение требований соответствующего гражданского и уголовного законодательства, включая законы об авторских правах и защите данных.

Такая структура позволяет выбрать те средства управления, которые имеют отношение к конкретной организации или сфере ответственности внутри организации. Выделено также десять так называемых ключевых элементов управления, являющихся фундаментальными:

- политика по информационной безопасности;
- распределение ответственности за информационную безопасность;
- образование и тренинг по информационной безопасности;
- отчетность по инцидентам с безопасностью;
- защита от вирусов;
- обеспечение непрерывности работы;
- контроль копирования лицензируемого программного обеспечения;
- защита архивной документации организации;
- защита персональных данных;
- выполнение политики по информационной безопасности.

Из вышеизложенного видно, что наряду с элементами управления для компьютеров и компьютерных сетей стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, обучение, увольнение с работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

Однако далеко не все положения стандарта применимы в условиях абсолютно каждой организации. Поэтому авторами стандарта был выбран подход, при котором стандарт используется как некая библиотека, из которой следует выбрать элементы, применимые в данных конкретных условиях. Этот выбор проводится на основе оценки риска и тщательно обосновывается.

Существуют различные способы анализа риска от простейших таблиц до сложных компьютеризованных методов, требующих специальной подготовки. Выбор применяемого метода зависит от условий организации. После этапа планирования и разработки системы следует длительный период внедрения.

2.4. Российские стандарты безопасности

В нашей стране при решении задач защиты информации должно обеспечиваться соблюдение указов Президента, федеральных законов, постановлений правительства, руководящих документов Гостехкомиссии, ФСБ и других нормативных документов.

Критерии оценки механизмов защиты программно-технического уровня выражены в Руководящих документах Гостехкомиссии "АС. Защита от НСД к информации. Классификация АС и требования по защите информации", "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации", а также "СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации". Однако сегодня эти Руководящие документы уже устарели, и содержащуюся в них классификацию нельзя признать состоятельной. Достаточно заметить, что классификация разрабатывалась без учета распределенной природы современных АС, а все современные коммерческие системы по своим возможностям превосходят требования первого класса защищенности за исключением требования по использованию сертифицированных криптографических алгоритмов. Развитием нормативной базы является разработка "Профилей защиты" для различных классов систем на базе "Общих критериев". В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии".

Проект Руководящих документов "Специальные требования и рекомендации по защите конфиденциальной информации" (СТР-К), содержит достаточно полный набор требований и рекомендаций организационного уровня по защите речевой информации, информации, обрабатываемой средствами вычислительной техники, а также по защите информации при подключении к сетям общего пользования.

Рассматриваются, в частности, следующие вопросы:

- защита информации на рабочих местах на базе автономных ПК;
- защита информации при использовании съемных накопителей большой емкости для автоматизированных рабочих мест на базе автономных ПК;
- защита информации в локальных сетях;
- защита информации при межсетевом взаимодействии;
- защита информации при работе с системами управления базами данных.

СТР-К может использоваться при проведении аудита и аттестации безопасности АС для оценки полноты и правильности реализации организационных мер защиты информации.

Следует упомянуть также еще один важный, хотя и не новый Руководящий документ – "Классификация автоматизированных систем по уровню защищенности от несанкционированного доступа".

Согласно ему, устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

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

В табл. 2.3 приведены требования ко всем девяти классам защищенности АС. По существу перед нами – минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации.

В России с 2004 года введен в действие ГОСТ 15408-2001 [6, 7], который фактически является стандартом ISO 15408, переведенным на русский язык.

Таблица 2.3

Требования к защищенности автоматизированных систем

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
к программам	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+

Окончание табл. 2.3

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач)	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	-	+	-	+	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+

2.5. Гармонизированные критерии Европейских стран

Принципиально важной чертой Европейских Критериев [19] является отсутствие требований к условиям, в которых должна работать ИС. Так называемый спонсор, то есть организация, запрашивающая сертификацион-

ные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации – оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", Европейские Критерии относятся к гарантированности безопасной работы системы.

Требования к политике безопасности и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оценки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Критерии рассматривают все основные составляющие информационной безопасности – конфиденциальность, целостность, доступность.

В Критериях проводится различие между системами и продуктами. Система – это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт – это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

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

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта – эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассмат-

риваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяются три градации мощности – базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности – от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки – от проектирования до эксплуатации и сопровождения.

Кратко о главном

Качественная оценка уровня ИБ ОИ начинается с анализа соответствия ОИ требованиям стандартов информационной безопасности.

Первым стандартом, получившим широкое распространение, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" ("Оранжевая книга"). Этот стандарт определяет основные понятия безопасности информационных систем и включает четыре уровня доверия и шесть классов безопасности.

Продолжением данного стандарта является его интерпретация для сетевых приложений. Она отличается от самих "Критериев" учетом динамичности сетевых конфигураций.

Стандарт ISO 15408 – "Критерии оценки безопасности информационных технологий" рассматривает объект оценки в контексте среды безопасности, которая характеризуется определенными условиями и угрозами. В этом стандарте структура всех требований основывается на иерархии "класс-семейство-компонент-элемент".

Международный стандарт ISO 17799 определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска и т.д. в контексте информационной безопасности. ISO 17799 – это модель системы менеджмента, и в этом смысле не является техническим стандартом.

В России критерии оценки механизмов защиты программно-технического уровня выражены в Руководящих документах Гостехкомиссии:

- "АС. Защита от НСД к информации. Классификация АС и требования по защите информации";

- "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации";

- "СВТ. Межсетевые экраны. Защита от НСД к информации".

- "Классификация автоматизированных систем по уровню защищенности от несанкционированного доступа".

Принципиально важной чертой Гармонизированных критериев Европейских стран является отсутствие требований к условиям, в которых должна работать ИС. В Критериях проводится различие между системами и продуктами. Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности.

Контрольные вопросы

1. Дайте понятие доверенной вычислительной базы.
2. Что является функциями монитора обращений?
3. Что такое политика безопасности?
4. Какие элементы включает в себя политика безопасности?
5. Что такое уровень гарантированности?
6. Какие виды гарантированности бывают?
7. Что такое классы безопасности и уровни доверия?
8. Какие требования определяются классами С1 и С2?
9. Какие требования определяются классами В1, В2 и В3?
10. Какие требования определяются классом А1?
11. Дайте понятие сетевой доверенной вычислительной базы.
12. Какие существуют сервисы безопасности?
13. Какие существуют механизмы реализации сервисов безопасности?
14. Какие выделяют этапы жизненного цикла объекта оценки?
15. Что такое класс, семейство, компонент и элемент в ISO 15408?
16. Перечислите классы функциональных требований в ISO 15408.
17. Перечислите классы требований доверия в ISO 15408.
18. Перечислите оценочные уровни доверия в стандарте ISO 15408.
19. Перечислите группы элементов управления в стандарте ISO 17799.
20. Перечислите ключевые элементы управления в ISO 17799.

Глава 3. МОДЕЛЬ КОМПЛЕКСНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

3.1. Задачи, принципы построения и направления работ по созданию КСИБ

На каждом конкретном предприятии построение системы ИБ определяется следующими факторами [12]:

- финансовые возможности предприятия;
- технические возможности предприятия;
- размеры предприятия;
- размещение предприятия;
- номенклатура выпускаемой продукции;
- система внутреннего документооборота;
- объем защищаемой информации;
- вид защищаемой информации и др.

Формирование новых хозяйственных связей предприятий приводит к возникновению проблемы взаимной защиты коммерческой тайны торговых партнеров. В практике работы зарубежных фирм предусмотрен порядок специальных договоров по взаимной ЗИ, переданной друг другу в ходе делового сотрудничества.

Задачи КСИБ

По результатам проведенного анализа возможных угроз ИБ можно сформулировать перечень основных задач, которые должны решаться КСИБ [15, 17]:

- управление доступом пользователей к ресурсам РТКС;
- защита данных, передаваемых по каналам связи;
- регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;
- контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках НСД к ресурсам системы;
- контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;
- обеспечение замкнутой среды проверенного ПО с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ и

средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;

- управление средствами системы защиты.

Основные принципы построения КСИБ

Принцип системности. Системный подход предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности. При создании КСИБ необходимо учитывать все слабые места системы обработки информации на предприятии, а также характер, возможные объекты и направления атак на систему со стороны нарушителей. КСИБ должна строиться с учетом не только всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности предполагает согласованное применение разнородных средств при построении целостной системы ИБ, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Принцип непрерывности защиты. ЗИ – это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.).

Принцип разумной достаточности. Создать абсолютно непреодолимую систему безопасности принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми, что поднимает проблему анализа рисков.

Принцип гибкости управления и применения. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуата-

ции, могут обеспечивать как чрезмерный, так и недостаточный уровень безопасности. Для обеспечения возможности изменения уровня защищенности средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются.

Принцип открытости алгоритмов и механизмов защиты. Суть принципа состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Чрезвычайно важно, чтобы знание алгоритмов работы системы защиты не давало возможности ее преодоления даже автору.

Принцип простоты применения защитных мер и средств. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

Направления работ по созданию КСИБ

Разработка КСИБ должна проходить в трех параллельных направлениях: методическом, организационном и техническом.

Методическое направление предусматривает разработку *концепции безопасности*. Мероприятия по созданию системы безопасности, реализуемые вне единого комплекса мер, прописанных в рамках концепции безопасности, бесперспективны с точки зрения ожидаемого результата.

Под концепцией понимается взаимоувязанный комплекс организационно-технических мер, методологических указаний, регламентов, комплектов форм типовых документов и т.д., решающих задачи ЗИ.

Концепция безопасности – это документ, в котором [9, 18]:

- применяется методика определения и описания информационных потоков (ИП), представляющая собой формальное и точное описание работы с информацией, с учетом их изменений со временем;
- определены критерии, по которым принимается решение о появлении или прекращении конкретного ИП;
- анализируются, описываются и фиксируются ИП, существующие на текущий момент;
- определяются для каждого ИП фазы существования информации;
- определяются категории конфиденциальной информации и разрабатывается классификация информации по этим категориям;

- создается матрица конфиденциальности;

- определяются возможные пути разглашения конфиденциальной информации, т.е. модель угроз;

- для каждой угрозы и атаки определяется модель нарушителя, включающая профессиональный круг лиц, к которому принадлежит нарушитель, мотивация и цели нарушителя, его предполагаемая квалификация и характер возможных действий;

- определяются уровни риска для всей матрицы конфиденциальности, вероятности реализации каждой атаки, стоимость ущерба при каждой атаке и усредненные вероятные величины убытков (риски);

- определяется порядок изменения Концепции безопасности.

Разработка Концепции безопасности сводится к следующим практическим шагам [15]:

1. определение используемых руководящих документов и стандартов, а также основных положений политики ИБ;
2. определение подходов к управлению рисками;
3. структуризация контрмер по уровням.

В рамках организационного направления работ создается организационная компонента КСИБ – совокупность правил (руководящих документов) и технических средств, регламентирующих деятельность сотрудников при обращении с информацией независимо от форм ее представления.

Организационное направление включает в себя:

- разработку регламента обеспечения безопасности;

- применение методологии при работе с персоналом;

- работы по уточнению требований к характеристикам защищенности системы;

- анализ информационной структуры предприятия;

- разнесение субъектов и объектов информационных отношений по категориям конфиденциальности;

- определение допустимых форм их взаимодействий и т.д.

Регламент обеспечения безопасности – комплект документов, регламентирующий правила обращения с конфиденциальной информацией (КИ) в зависимости от фазы ее обработки и категории конфиденциальности. В регламенте должен быть определен комплекс методических, административных и технических мер, включающих в себя [9]:

- создание подразделения, ответственного за обеспечение КИ;

- определение порядка допуска сотрудников к КИ и обязанностей, ограничений и условий, накладываемых на них;

- определение сотрудников, допущенных к КИ;

- классификацию КИ и работу с ней по категориям;

- порядок изменения категории конфиденциальности работ и информации;

- требования к помещениям, в которых проводятся конфиденциальные работы и обрабатывается КИ, по категориям;

- требования к конфиденциальному делопроизводству;

- требования к учету, хранению и обращению с конфиденциальными документами;

- меры по контролю за обеспечением конфиденциальности работ и информации;

- план мероприятий по противодействию атаке на КИ;

- план мероприятий по восстановлению КИ;

- определение ответственности за разглашение КИ.

Для регламента обеспечения безопасности должны быть разработаны следующие документы [9]:

1. общие документы:

- инструкция по обеспечению режима конфиденциальности на предприятии;

- требования к пропускному и внутриобъектовому режиму;

- общие требования к системе разграничения доступа в помещении;

- регламент взаимодействия Служб обеспечения конфиденциальности и безопасности;

2. документы по работе с кадрами:

- инструкция по работе с кадрами, подлежащими допуску к КИ;

- требования к лицам, оформляемым на должность, требующую допуска к КИ;

3. документы по защите ИС. Они регламентируют:

- режим конфиденциальности при обработке КИ с применением средств вычислительной техники;

- требования к защищенности ИС;

- концепцию безопасности ИС;

- порядок анализа существующей ИС.

Техническая компонента КСИБ – комплекс технических средств и технологий ЗИ при ее обработке, хранении и передаче, включая криптографические средства. Техническая компонента создается в рамках технического направления работ [1, 14, 17, 20].

При реализации технического направления проводится сбор исходных данных для разработки технических предложений по оснащенности автоматизированной системы обработки, хранения и передачи информации средствами ЗИ, позволяющими реализовать требуемый уровень защищенности.

Этапы построения КСИБ предприятия

Первый и самый важный этап – *информационное обследование.* Именно на этом этапе определяются приоритеты в обеспечении безопасности предприятия. На этом же этапе строится также формальная модель нарушителя. Модель описывает квалификацию злоумышленника, имеющиеся средства для реализации тех или иных атак, время и место действия и т.д. По результатам этапа вырабатываются рекомендации по устранению выявленных угроз, правильному выбору и применению средств защиты.

Вторым этапом является *разработка организационно-распорядительных документов* для службы безопасности и отдела ЗИ, регламентирующих проведение всего спектра защитных мероприятий, взаимодействие с внешними организациями, привлечение к ответственности нарушителей.

Следующим этапом построения КСИБ служит *приобретение, установка и настройка рекомендованных средств и механизмов ЗИ.*

С течением времени имеющиеся средства защиты устаревают, выходят новые версии систем обеспечения ИБ, постоянно расширяется список найденных брешей в защите, меняются технология обработки информации, программные и аппаратные средства, происходит смена персонала предприятия. Следовательно, построение системы безопасности не заканчивается на предыдущем этапе, а переходит в качественно новую форму *постоянного поддержания необходимого уровня.* Значит необходимо периодически пересматривать разработанные организационно-распорядительные документы, проводить обследование системы и ее подсистем, обучать новый персонал, обновлять средства защиты.

3.2. Формальная модель КСИБ

Основой формального описания систем защиты можно считать модель системы защиты с полным перекрытием [2], в которой рассматривается взаимодействие "области угроз", "защищаемой области" и "системы защиты".

Таким образом, имеем три множества:

$T = \{t_i\}$ – множество угроз безопасности,

$O = \{o_j\}$ – множество объектов (ресурсов) защищенной системы,

$S = \{s_k\}$ – множество механизмов безопасности АС.

Элементы этих множеств находятся между собой в определенных отношениях, собственно и описывающих систему защиты. Для описания системы защиты обычно используется графовая модель. Множество отношений угроза – объект образует двухдольный граф $\{<T, O>\}$. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего набора S; в результате получается трехдольный граф $\{<T, S, O>\}$.

Развитие модели предполагает введение еще двух элементов.

V – набор уязвимых мест, определяемый подмножеством декартова произведения $T*O$: $v_r = <t_i, o_j>$. Под уязвимостью системы защиты понимают возможность осуществления угрозы T в отношении объекта O. (На практике под уязвимостью системы защиты обычно понимают не саму возможность осуществления угрозы безопасности, а те свойства системы, которые либо способствуют успешному осуществлению угрозы, либо могут быть использованы злоумышленником для осуществления угрозы.)

B – набор барьеров, определяемый декартовым произведением $V*S$: $b_l = <t_i, o_j, s_k>$, представляющих собой пути осуществления угроз безопасности, перекрытые средствами защиты.

В результате получаем систему, состоящую из пяти элементов: $<T, O, S, V, B>$, описывающую систему защиты с учетом наличия в ней уязвимостей.

Для системы с полным перекрытием для любой уязвимости имеется устраняющий ее барьер. Иными словами, в подобной системе защиты для всех возможных угроз безопасности существуют механизмы защиты, препятствующие осуществлению этих угроз. Данное условие является первым фактором, определяющим защищенность АС; второй фактор – прочность механизмов защиты.

В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы. В действительности же механизмы защиты обеспечивают лишь некоторую степень сопротивляемости угрозам безопасности. Поэтому в качестве характеристик элемента набора барьеров $b_l = <t_i, o_j, m_k>$, $b_l \in B$ может рассматриваться набор $<P_l, D_l, R_l>$, где P_l – вероятность появления угрозы, D_l – величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы), а R_l – степень сопротивляемости механизма защиты S_k, характеризующаяся вероятностью его преодоления.

Прочность барьера $b_l = <t_i, o_j, s_k>$ характеризуется величиной остаточного риска X_l, связанного с возможностью осуществления угрозы t_i в

отношении объекта автоматизированной системы o_j при использовании механизма защиты s_k. Эта величина определяется по формуле

$$X_l = P_k D_k (1 - R_k). \quad (3.1)$$

Для определения величины защищенности Z можно использовать соотношение

$$Z = \frac{1}{\sum_{\forall b_k \in B} (P_k D_k (1 - R_k))}, \quad (3.2)$$

где $P_k, D_k, R_k \in (0,1)$.

Знаменатель определяет суммарную величину остаточных рисков, связанных с возможностью осуществления угроз T в отношении объектов автоматизированной системы O при использовании механизмов защиты S. Суммарная величина остаточных рисков характеризует общую уязвимость системы защиты, а защищенность определяется как величина, обратная уязвимости. При отсутствии в системе барьеров b_k, перекрывающих определенные уязвимости, степень сопротивляемости механизма защиты R_k принимается равной нулю.

На практике получение точных значений приведенных характеристик барьеров затруднено, поскольку понятия угрозы, ущерба и сопротивляемости механизма защиты трудно формализовать. Так, оценку ущерба в результате несанкционированного доступа к информации политического и военного характера точно определить вообще невозможно, а определение вероятности осуществления угрозы не может базироваться на статистическом анализе.

Вместе с тем, для защиты информации экономического характера, допускающей оценку ущерба, разработаны стоимостные методы оценки эффективности средств защиты. Для этих методов набор характеристик барьера дополняет величина F_l – затраты на построение средства защиты барьера b_l. В этом случае выбор оптимального набора средств защиты связан с минимизацией суммарных затрат $A=\{a_l\}$, состоящих из затрат $F=\{f_l\}$ на создание средств защиты и возможных затрат в результате успешного осуществления угроз $N=\{n_l\}$.

Построение моделей системы защиты и анализ их свойств составляют предмет "теории безопасных систем", еще только оформляющейся в качестве самостоятельного направления.

Формальные подходы к решению задачи оценки защищенности из-за трудностей, связанных с формализацией, широкого практического распространения не получили. Значительно более действенным является исполь-

зование неформальных классификационных подходов. Вместо стоимостных оценок используют категорирование: нарушителей (по целям, квалификации и доступным вычислительным ресурсам); информации (по уровням критичности и конфиденциальности); средств защиты (по функциональности и гарантированности реализуемых возможностей) и т.п. Такой подход не дает точных значений показателей защищенности, однако позволяет классифицировать АС по уровню защищенности и сравнивать их между собой. Примерами классификационных методик, получивших широкое распространение, могут служить разнообразные критерии оценки безопасности ИТ, принятые во многих странах в качестве национальных стандартов, устанавливающие классы и уровни защищенности. Результатом развития национальных стандартов в этой области является обобщающий мировой опыт международный стандарт ISO 15408.

3.3. Механизм функционирования КСИБ

Механизм должен обеспечивать [1, 14, 20]:

- непрерывность защиты КИ;
- целенаправленность и конкретность защиты сведений в интересах решения определенных задач;
- активность защиты, обеспечивающую предупреждение возможной утечки сведений;
- надежность, предполагающую разумное дублирование средств защиты;
- универсальность, позволяющую ликвидировать угрозу утечки информации независимо от места ее появления.

Необходимо, чтобы этот механизм предусматривал взаимную ответственность персонала и руководства за сохранность коммерческой тайны, а перечень сведений, относимых к ней, следует регулярно пересматривать в зависимости от изменения направлений и результатов деятельности предприятия. Такой перечень в целом включает следующее:

- организационная структура предприятия;
- основные элементы системы безопасности;
- процедуры доступа к средствам связи и информационным сетям;
- финансовые отчеты и прогнозы;
- маркетинг и стратегия ценообразования;
- техническая спецификация существующей и перспективной продукции;
- перспективные планы развития производства.

Кратко о главном

На каждом конкретном предприятии построение системы ИБ определяется различными факторами. По результатам проведенного анализа возможных угроз ИБ можно сформулировать перечень основных задач, которые должны решаться КСИБ.

Построение КСИБ должно базироваться на принципах системности, комплексности, непрерывности защиты, разумной достаточности, простоты управления, открытости алгоритмов и механизмов защиты.

Разработка КСИБ должна проходить в трех параллельных направлениях: методическом, организационном и техническом.

Основой формального описания систем защиты можно считать модель системы защиты с полным перекрытием, в которой рассматривается взаимодействие следующих множеств:

- угроз безопасности,
- ресурсов защищаемой системы,
- механизмов безопасности,
- уязвимых мест,
- барьеров.

Механизм функционирования КСИБ должен предусматривать взаимную ответственность персонала и руководства за сохранность коммерческой тайны.

Контрольные вопросы

1. Какими факторами определяется построение системы КСИБ?
2. Каковы задачи, которые должны решаться КСИБ?
3. В чем сущность принципов системности и комплексности?
4. В чем сущность принципов непрерывности защиты и разумной достаточности?
5. В чем сущность принципов открытости алгоритмов защиты и простоты применения защитных мер и средств?
6. Что предусматривает методическое направление работ по созданию КСИБ?
7. Что определяет концепция безопасности?
8. Что предусматривает организационное направление работ по созданию КСИБ?
9. Перечислите этапы построения КСИБ.
10. Какие множества рассматривает формальная модель КСИБ?
11. Что должен обеспечивать механизм функционирования КСИБ?

Глава 4. МЕТОДЫ КАЧЕСТВЕННОЙ ОЦЕНКИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Оценка уровня информационной безопасности

Типовая методика анализа защищенности ИС предприятия включает:

- изучение исходных данных по ИС;
- оценку рисков, связанных с осуществлением угроз безопасности в отношении ресурсов предприятия;
- анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима ИБ и оценку их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам;
- ручной анализ конфигурационных файлов маршрутизаторов и прокси-серверов, почтовых и DNS-серверов;
- сканирование внешних сетевых адресов локальной сети;
- сканирование ресурсов локальной сети изнутри;
- анализ конфигурации серверов и рабочих станций при помощи специализированных программных агентов.

Перечисленные технические методы предполагают применение как активного, так и пассивного тестирования системы защиты. Активное тестирование заключается в эмуляции действий потенциального злоумышленника; пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с использованием списков проверки. Тестирование может производиться вручную или с использованием специализированных программных средств.

Исходные данные

В соответствии с требованиями Руководящих документов при проведении работ по аттестации безопасности ИС, включающих в себя предварительное обследование и анализ защищенности объектов информатизации, заказчиком работ должны быть предоставлены следующие исходные данные:

- полное и точное наименование ОИ и его назначение. Характер обрабатываемой информации (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень ее секретно-

сти, определенный в соответствии с тем или иным перечнем (государственным, отраслевым, ведомственным, предприятия);

- организационная структура ОИ;

- перечень помещений, состав комплекса технических средств, входящих в ОИ, в которых (на которых) обрабатывается указанная информация. Особенности и схема расположения ОИ с указанием границ контролируемой зоны;

- структура программного обеспечения, используемого на аттестуемом ОИ и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией;

- общая функциональная схема ОИ, включая схему источников питания и режимы обработки защищаемой информации;

- наличие и характер взаимодействия с другими ОИ;

- состав и структура системы ЗИ на аттестуемом ОИ;

- перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом ОИ и имеющих соответствующий сертификат, предписание на эксплуатацию;

- сведения о разработчиках системы ЗИ, наличие у сторонних разработчиков лицензий на проведение подобных работ;

- наличие на ОИ службы безопасности;

- наличие и основные характеристики физической защиты объекта (помещений, где обрабатывается защищаемая информация и хранятся носители информации);

- наличие проектной и эксплуатационной документации на ОИ и другие исходные данные по объекту, влияющие на ИБ.

Для оценки текущего положения дел с обеспечением безопасности наиболее значимо предоставление перечисленных ниже сведений об ОИ:

- нормативно-распорядительная документация по проведению регламентных работ и обеспечению политики безопасности, должностные инструкции, процедуры и планы предотвращения и реагирования на попытки НСД к информационным ресурсам, топология корпоративной сети, структура информационных ресурсов с указанием степени критичности или конфиденциальности каждого из них, размещение информационных ресурсов в ИС, организационная структура пользователей и обслуживающих подразделений, размещение линий передачи данных, схемы и характеристики систем электропитания и заземления объектов, используемые системы сетевого управления и мониторинга;

- проектная документация – функциональные схемы, описание автоматизированных функций, описание основных технических решений;

- эксплуатационная документация – руководства пользователей и администраторов, использующих программные и технические средства ЗИ.

4.2. Оценка рисков

Анализ рисков начинается с формализации системы приоритетов организации в области ИБ. Для оценки ценности ресурсов необходимо выбирать подходящую систему критериев. Критерии должны позволять описать потенциальный ущерб, связанный с нарушением конфиденциальности, целостности, доступности.

Кроме критериев, учитывающих финансовые потери, в коммерческих организациях могут присутствовать критерии, отражающие [12]:

- ущерб репутации организации;

- неприятности, связанные с нарушением действующего законодательства;

- ущерб для здоровья персонала;

- ущерб, связанный с разглашением персональных данных отдельных лиц;

- финансовые потери от разглашения информации;

- финансовые потери, связанные с восстановлением ресурсов;

- потери, связанные с невозможностью выполнения обязательств;

- ущерб от дезорганизации деятельности.

В правительственных учреждениях могут добавляться критерии, отражающие такие области, как национальная безопасность и международные отношения.

Затем производится выбор подходящей технологии анализа рисков.

Существуют различные подходы к оценке рисков [12]. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму ИБ, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Минимальным требованиям к режиму ИБ соответствует базовый уровень ИБ. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, НСД и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов.

Повышенные требования. В случаях, когда нарушения режима ИБ чреваты тяжелыми последствиями, базовый уровень требований к режиму ИБ является недостаточным. Для того чтобы сформулировать дополнительные требования, необходимо:

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
- оценить вероятность угроз;
- определить уязвимость ресурсов.

Исходными данными являются результаты опроса сотрудников, базы данных со статистикой по классам рисков. В результате выполнения этого этапа должен быть написан документ "Анализ рисков".

Для базового уровня ИБ документ будет содержать раздел: "Классы рисков, принимаемых во внимание при построении подсистемы ИБ".

Для повышенного уровня ИБ документ будет содержать разделы:

- "Оценка ценности информационных ресурсов";
- "Возможные пути нарушения режима ИБ (модель угроз)";
- "Модель нарушителя по выбранным классам угроз";
- "Оценка параметров угроз и уязвимых мест ИС".

Выделяется четыре подхода к управлению рисками [12]:

1. Уменьшение риска. Многие риски могут быть существенно уменьшены путем использования весьма простых и дешевых контрмер. Например, грамотное управление паролями снижает риск НСД.
2. Уклонение от риска. От некоторых классов рисков можно уклониться. Например, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска НСД в локальную сеть со стороны Web-клиентов.
3. Изменение характера риска. Если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки.
4. Принятие риска. Многие риски не могут быть уменьшены до пренебрежимо малой величины. На практике, после принятия стандартного набора контрмер, ряд рисков уменьшается, но остается все еще значимым. Необходимо знать остаточную величину риска.

Исходными данными являются результаты опроса сотрудников, экспертные оценки возможности применения стандартных подходов к управлению рисками. В результате выполнения этапа для принимаемых во вни-

мание рисков должна быть предложена стратегия управления, излагаемая в документе "Управление рисками":

- выделение рисков, уровень которых недопустимо высок;
- стратегия управления рисками;
- выбор варианта контрмер.

4.3. Тестирование систем информационной безопасности

Тестирование системы защиты проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей. Традиционно используются два основных метода тестирования: по методу "черного ящика" и по методу "белого ящика" [13].

Тестирование по методу "черного ящика" предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. Против объекта испытаний реализуются все известные типы атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, содержащие базу данных с описанием известных уязвимостей ОС, маршрутизаторов, сетевых служб и т.п., а также алгоритмов осуществления попыток вторжения.

Метод "белого ящика" предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяется наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам. Выводы о наличии уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного программного обеспечения, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные средства анализа защищенности системного уровня.

Тест на проникновение. Тестирование системы защиты – это метод выявления недостатков безопасности с точки зрения постороннего человека (взломщика). Он позволяет протестировать схему действий, которая раскрывает и предотвращает внутренние и внешние попытки проникновения и сообщает о них. Используя этот метод, можно обнаружить даже те

недостатки защиты, которые не были учтены в самом начале, при разработке политики безопасности. Тест должен разрешить два основных вопроса:

- все ли пункты политики безопасности достигают своих целей и используются так, как это было задумано;

- существует ли что-либо, не отраженное в политике безопасности, что может быть использовано для осуществления целей злоумышленника?

Все попытки должны контролироваться обеими сторонами – как "взломщиком", так и "клиентом". Это поможет протестировать систему гораздо эффективнее. Необходимо также свести к минимуму количество людей, знающих о проведении эксперимента. При тестировании могут быть затронуты деликатные вопросы частной жизни сотрудников и безопасности организации, поэтому желательно получить предварительное разрешение на проведение такой акции. Ваше непосредственное начальство обязательно должно быть в курсе происходящего.

Профессионалам в области безопасности при проведении теста необходимо иметь такое же положение, как и у потенциального злоумышленника: в их распоряжении должны быть время, терпение и максимальное количество технических средств, которые могут быть использованы взломщиком. Более того, проверяющим следует расценить это как вызов своему профессионализму, а значит, проявить столько же рвения, сколько и взломщик, иначе тесты могут не достичь необходимого результата.

Осведомленность играет ведущую роль в защите предприятия от проникновения в информационные системы. Осведомленность является ключевым моментом и вследствие того, что это предварительная, предупреждающая мера, нацеленная на усвоение самими служащими основных принципов и необходимых правил защиты. Разумеется, этот аспект требует обучения и тестирования сотрудников.

Кратко о главном

Качественные методы оценки ИБ предполагают оценку уровня ИБ, анализ рисков и тестирование СИБ.

Оценка уровня ИБ позволяет на основе некоторого набора исходных данных (организационная структура и функциональная схема ОИ, структура программного обеспечения, используемого на аттестуемом ОИ, нали-

чие и характер взаимодействия с другими ОИ и др.) выявить качественное соответствие или несоответствие СИБ определенным требованиям.

Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму ИБ, характера принимаемых во внимание угроз и эффективности потенциальных контрмер.

Анализ рисков необходим для выбора подхода к управлению рисками. Такими подходами являются: уменьшение риска, уклонение от риска, изменение характера риска или принятие риска.

Тестирование системы защиты проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к атакам, а также с целью поиска уязвимостей и может проводиться по методу "белого ящика" или по методу "черного ящика".

Контрольные вопросы

1. Что включает в себя типовая методика анализа защищенности ИС предприятия?
2. Какие исходные данные необходимы для анализа защищенности ОИ?
3. Назовите основные критерии оценки рисков.
4. Какие существуют подходы к оценке рисков?
5. Какие типовые разделы должен содержать документ "Анализ рисков"?
6. Какие существуют подходы к управлению рисками?
7. Какова цель тестирования системы защиты?
8. Что из себя представляет тестирование по методу "черного ящика"?
9. Что из себя представляет тестирование по методу "белого ящика"?
10. Что из себя представляет тест на проникновение?
11. Какую роль в ИБ играет осведомленность сотрудников предприятия?

Глава 5. МЕТОДЫ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

5.1. Метод экспертных оценок

В основе метода экспертных оценок информационной безопасности [8] лежит понятие *профиля защиты* (ПЗ) стандарта ISO/IEC 15408. Стандарт ISO/IEC 15408 [22] определяет ПЗ как совокупность функциональных и гарантийных требований, позволяющих реализовать систему защиты с необходимым уровнем ИБ. Методология оценки ИБ ПЗ основана на использовании методов анализа и оценки активов организации, уязвимостей, угроз ИБ, возможных атак и целей безопасности. Атака действенна, если существующая угроза T_i, используя уязвимость V_i объекта оценки, приводит к риску R потери активов организации. Снижение риска потери активов возможно при правильном выборе функциональных требований, политик безопасности организации S_{Pi} и разумных предположений R_{Ai} относительно свойств объекта оценки и его среды функционирования.

Формально описать вероятности отдельных угроз, атак, эффективности отдельных политик безопасности очень сложно. В связи с этим, для получения количественной оценки риска используются экспертные оценки, основанные на использовании кластера исходов (рис. 5.1), представляющего собой дерево иерархий с вершинами $Z_1, \ldots Z_i, \ldots Z_n$. Каждая из вершин кластера исходов соответствует элементу множества значений анализируемого показателя $\{T_i\}, \{V_i\}, \{S_{Pi}\}, \{R_{Ai}\}$.

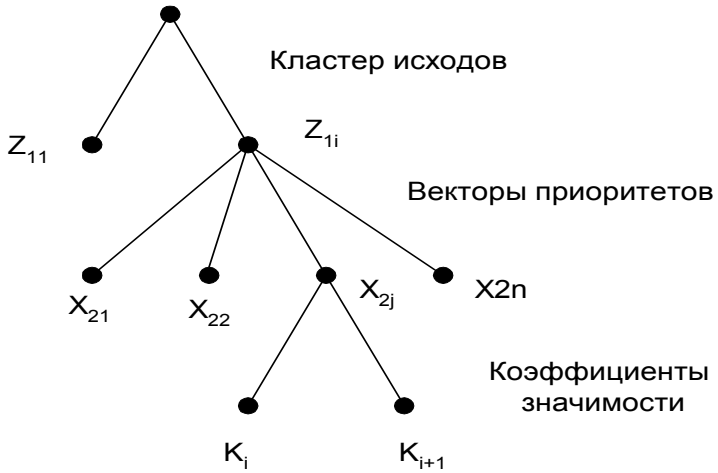

Рис. 5.1. Иерархия кластеров

* Глава написана совместно с М.А. Кулаковым

Значимость элементов кластера определяется на основе матрицы парных сравнений *[Z]* и вектора приоритетов X_i, определяющего ранжировку элементов кластера исходов.

Каждый путь в дереве иерархий соответствует элементу множества значений отдельных показателей $\{T_i\}$, $\{S_{Pi}\}$, $\{R_{Ai}\}$ и для этого пути можно определить коэффициент значимости K_i, как произведение значений векторов приоритетов кластеров исходов, соответствующих этому пути:

$$K_i = X_{1i} \cdot X_{2j} \cdot \ldots \cdot X_{gl}, \qquad \sum_i K_i = 1. \tag{5.1}$$

При этом выбор разработчиком ПЗ конкретных элементов множеств $\{T_i\}$, $\{S_{Pi}\}$, $\{R_{Ai}\}$ равносилен исключению из соответствующих деревьев иерархии отдельных элементов, что уменьшает суммарное значение коэффициентов значимости K_i с 1 до некоторой величины $P<1$. Точка с координатами $\{P_T, P_{SP}, P_{RA}\}$ определяет исходное состояние ПЗ. Данная точка соответствует в процессе проектирования ПЗ этапу "Среда безопасности", когда выбраны уязвимости и соответствующие им угрозы, определены политики безопасности и сформулированы предположения. Выбор конкретных элементов множеств $\{(V/T)_i\}$, $\{S_{Pi}\}$, $\{R_{Ai}\}$ всегда связан с риском того, что выбранные множества не обеспечат нужной совокупности целей безопасности, вследствие чего появится возможность проведения злоумышленником целенаправленных атак и потеря активов. Условиями, способствующими риску, являются:

- недостаток имеющейся у разработчика информации (список уязвимостей не полон, часть угроз не идентифицирована, политики безопасности в силу экономических, юридических особенностей могут быть выполнены лишь частично);

- недостаток времени и имеющихся ресурсов. Специфика разрабатываемого ПЗ зачастую требует введения новых целей и разработки для них специальных функциональных требований безопасности. А это всегда связано с дополнительными и не малыми временными, ресурсными и стоимостными затратами.

Риск исходного состояния ПЗ можно представить вектором с координатами $\{0, 0, 0\}$ и $\{P_T, P_{SP}, P_{RA}\}$, а мерой риска может служить длина этого вектора (рис. 5.1), определяемая как

$$R = \sqrt{P_T^2 + P_{SP}^2 + P_{RA}^2}. \tag{5.2}$$

В данном случае R определяет верхнюю границу риска, которая априорно существует до определения целей безопасности. При выборе целей безопасности, исходя из уязвимостей, угроз, политик безопасности и пред-

положений, разработчику ПЗ рекомендуется использовать таблицы соответствия: "Детальная политика безопасности – Цели безопасности" и таблицу соответствия "Угрозы – Атаки – Цели безопасности" из профилирующей базы знаний "*CC Profiling Knowledge Base*".

На рис. 5.2 показана последовательность формирование целей безопасности для вариантов ПЗ, исходя из существующих уязвимостей, угроз, атак.

Для исходного состояния ПЗ рассчитываются суммарный коэффициент значимости атак P_A и суммарный коэффициент значимости политик безопасности P_{SP} (соотношения (5.3)):

$$P_A = \sum_{i=1}^{n} K_{Ai}\,, \qquad P_{SP} = \sum_{j=1}^{m} K_{SPj}\,. \tag{5.3}$$

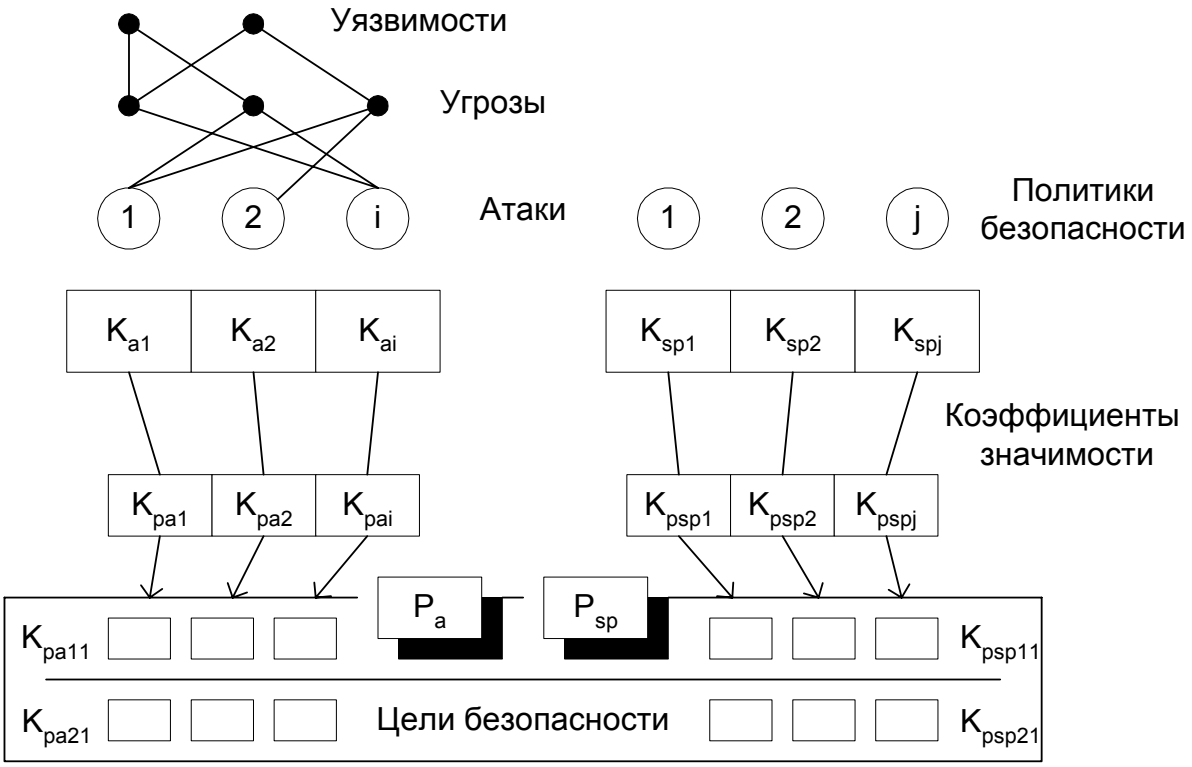

Рис. 5.2. Формирование вариантов ПЗ

Стандарт ISO/IEC 15408 позволяет выбрать цели безопасности, нейтрализующие возможные атаки, способствующие реализации политик безопасности и в конечном счете снижающие величины P_A, и P_{SP} на величины, определяемые соотношениями (5.4)

$$\Delta P_A = \sum_{j=1}^{n-1}\left(\prod_{j=1}^{n}(K_{Ai}\cdot K_{PAi})\right)_j, \qquad \Delta P_{SP} = \sum_{j=1}^{m-1}\left(\prod_{j=1}^{m}(K_{SPi}\cdot K_{PSPi})\right)_j. \tag{5.4}$$

Риск потерь активов для ПЗ, соответствующего выбранным целям безопасности можно оценить согласно соотношению (5.5)

$$R = \sqrt{\left(P_A - \Delta P_A\right)^2 + \left(P_{SP} - \Delta P_{SP}\right)^2} \ . \qquad (5.5)$$

На рис. 5.3 показана графическая интерпретация процесса целенаправленного выбора варианта ПЗ, имеющего минимальное значение риска потери активов.

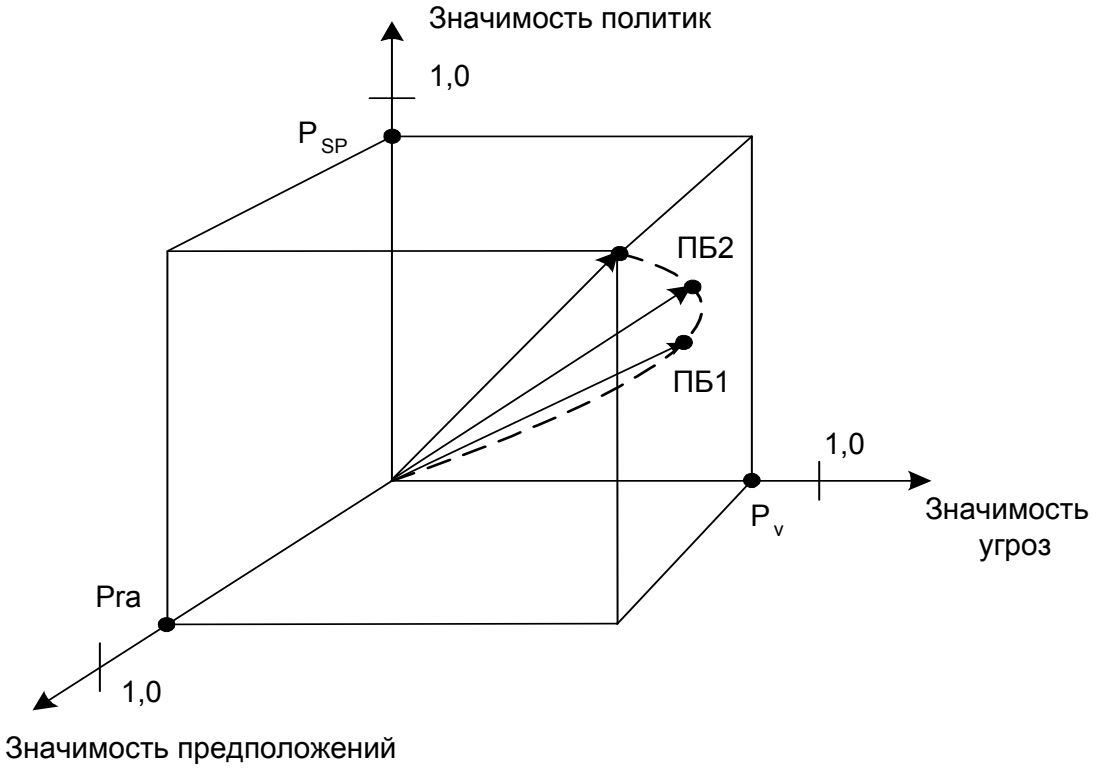

Рис. 5.3. Графическая интерпретация риска потери активов ПЗ

5.2. Метод информационных потоков

Рассмотрим распределенную вычислительную сеть, имеющую следующую топологию (рис. 5.4).

Эта вычислительная сеть включает в себя две доверенных между собой локальных сети, связанных через Интернет. Первая локальная сеть включает в себя: *FIREWALL* – межсетевой фильтр, *DOM1* – сервер (контроллер домена), *SMTP1* – почтовый сервер и состоит из двух сегментов. К

первому сегменту относятся ПК *PC11,…,PC1n*, а во второй сегмент входят рабочие станции *PC21,…,PC2m*.

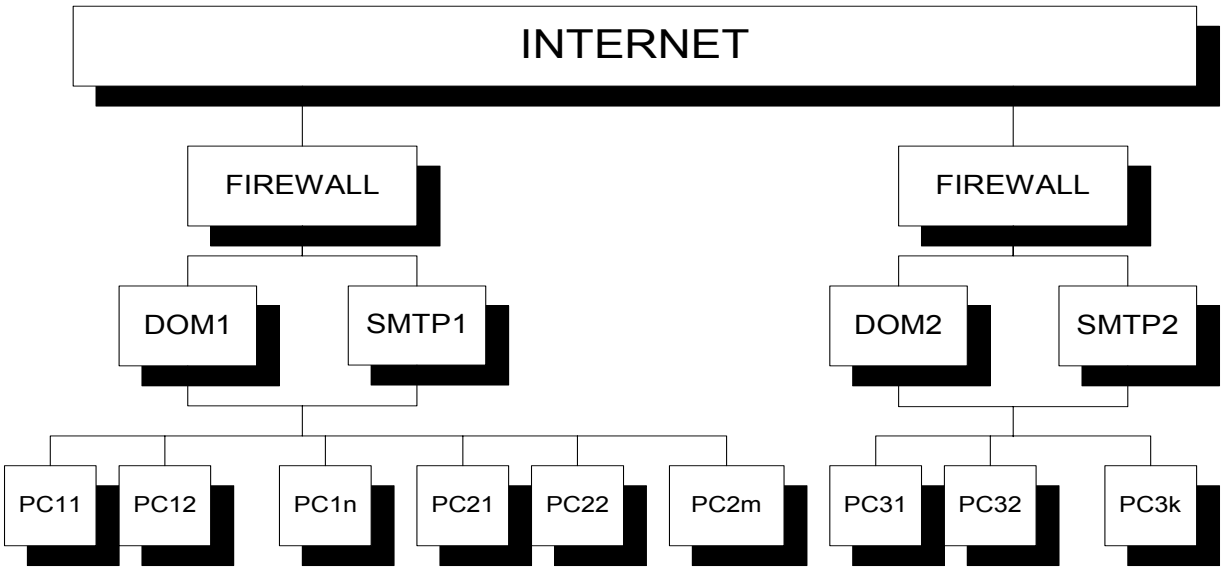

Рис. 5.4. Примерная топология сети

Пусть вторая локальная сеть состоит из *FIREWALL* – межсетевого фильтра, *DOM2* – сервера, *SMTP2* – почтового сервера, рабочих станций *PC31,…,PC3k*. Будем считать, что каждый компьютер является персональным, т.е. на нем работает и обладает правами доступа только один конкретный пользователь.

Определим информационный поток (коммуникационный трафик) как передачу информации через сеть. Рассмотрим набор всевозможных информационных потоков рассматриваемой распределенной вычислительной сети.

Преобразуем вычислительную сеть рис. 5.4 к рис. 5.5, который иллюстрирует возможные варианты соединений (сетевых трафиков) между отправителем a_i и получателем b_i.

Для любых информационных потоков (ИП) между отправителем и X_i и получателем Y_i возможны следующие варианты:

- ИП, который пересекает защищенную Сеть 1 ($i=1$);
- ИП, который выходит из защищенной Сети 1 и не входит в Сеть 2 ($i=2$);
- ИП, который выходит из общей сети (Интернет) и входит в Сеть 1 ($i=3$);
- ИП между доверенными Сетями 1 и 2 ($i=4$);

- ИП, который не затрагивает ни одну из доверенных Сетей (*i=5*);
- ИП внутри защищенной Сети (*i=6*).

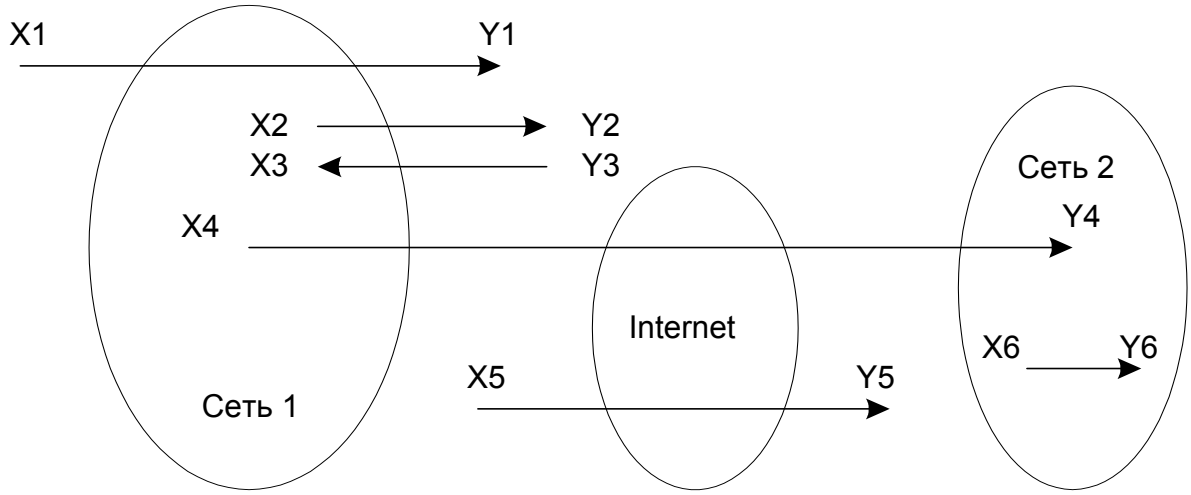

Рис. 5.5. Информационные потоки

В рамках этой модели не имеет смысла рассматривать вариант 5, т.к. этот ИП не представляет угрозы для безопасности защищаемых Сетей 1 и 2. Под АБ будем понимать совокупность необходимых функций защиты и их расположения относительно ИП в рассматриваемой сети.

Под проектированием АБ будем понимать указанные средства, реализующие соответствующую функцию (функции) защиты с необходимым набором параметров, их размещение в вычислительной сети и связь друг с другом.

Для реализации функций управления доступом имеет смысл составить матрицу разрешенных связей, определяющих права доступа (p_k, i, j) пользователей к тем или иным сетевым ресурсам $U=<p_k,1,j,...,p\ k,n,j>$, где j обозначает тип доступа (например, доступ на чтение, доступ на запись и т.д.), k – порядковый номер пользователя, а n – число пользователей. Возможный тип доступа определяется используемой операционной системой. В общем случае, матрица разрешенных связей является трехмерной и заполняется в соответствии с действующей политикой безопасности, которая считается заданной.

Для дальнейшей формализации задач проектирования АБ рассмотрим типовой набор функций защиты, реализуемых в распределенных вычислительных системах. В настоящее время применяются следующие виды функций защиты: идентификация, аутентификация, аудит, контроль целостности, прокси-технология, шифрование информации.

В процессе идентификации устанавливается взаимно однозначное соответствие между множеством сущностей системы и множеством идентификаторов. Идентификация позволяет различать сущности системы при контроле доступа, аудите и т.д.

Аутентификация представляет собой проверку подлинности идентификаторов. Аутентификация гарантирует подлинность субъекта. В результате аутентификации подлинность участника протокола подтверждается в контексте коммуникационных связей. Участник протокола – это субъект, обладающий одним или более неповторяющимися идентификаторами. Субъекты могут воспользоваться аутентификационной службой для проверки подлинности заявленных участников. В задачу функции аутентификации входит проверка аутентичности коммуникационного трафика на основе идентификаторов и аутентификационной информации (например, особых данных протокола аутентификации).

Если для какого-нибудь коммуникационного трафика вычисление функции аутентификации опустить, то становятся возможными некоторые атаки, типа подделки адреса. Более того, при запросе доступа источником, имеющим неопознанный идентификатор, механизмы управления доступом могут выдавать некорректный результат. Все то же самое относится и к выходному трафику. Вот почему эта функция является необходимой компонентой управления сетевым доступом.

Функция аудита позволяет вести непрерывный упорядоченный журнал важных системных событий: какое событие считать важным, определяется действующей политикой безопасности. Способ записи должен быть согласован, так чтобы информацией могли воспользоваться такие системы, как утилиты оповещения, средства анализа контрольного журнала, средства обнаружения команд.

Систему аудита следует строить таким образом, чтобы при возникновении системных нарушений можно было бы восстановить события, приведшие к этим нарушениям. Кроме того, система аудита допускает наблюдение за системой до возникновения нарушения, что позволяет заметить попытку нарушения и принять необходимые меры.

Аудит не подразумевает хранения избыточной информации, кроме той, которая необходима для поддержания единообразия. Однако для обеспечения отказоустойчивости, в частности, в неблагоприятных ситуациях, когда часть контрольной информации умышленно уничтожена, имеет смысл хранить в нескольких местах избыточную информацию: избыточность позволяет проводить перекрестный контроль правильности информации.

Функция целостности защищает коммуникационный трафик от незамеченных или несанкционированных изменений, таких как добавление, замена или удаление. Она не предотвращает эти нарушения, а лишь обнаруживает и помечает их. Известно множество средств, позволяющих обнаруживать изменение данных, от схем проверки контрольной суммы (циклический контроль избыточности (CRC)) до криптографически защищенных цифровых подписей.

Возможность атаки соединения (например, активной атаки протокола TCP) возникает даже в том случае, когда всего лишь одна порция обмена не обработана функцией целостности. Таким образом, функция целостности необходима для защиты от активного сетевого перехвата. В некоторых случаях можно, а иногда и желательно, дополнительно проводить проверку конфиденциальности данных, хотя и не обязательно обеспечивать целостность путем зашифрования всего потока данных. Службы обеспечения конфиденциальности и целостности преследуют различные цели и обладают различными рабочими характеристиками.

Прокси-технология заключается в подмене IP-адреса участника информационного потока и применяется для скрытия реальной топологии сети, например, количества машин в защищенной сети и т.д.

Шифрование применяется для защиты от несанкционированного доступа к конфиденциальной информации при передаче ее через общую сеть между двумя доверенными сетями.

Построение алгоритма распределения функций безопасности

1. Защита от внешних воздействий (со стороны Интернета)

Из рис. 5.5 следует, что внешнюю опасность для защищаемой сети представляют ИП *i=1,2,3,4*. В настоящее время устройством, обеспечивающим защиту от внешних угроз, является межсетевой фильтр (комплекс программно-аппаратных решений, который защищает ИС от несанкционированных коммуникационных трафиков из Интернет в защищаемую сеть). Функции, возложенные на межсетевой фильтр, в принципе, могут находиться в любом месте защищаемой сети, но исходя из требований сохранения максимальной пропускной способности канала и минимальной стоимости дополнительно устанавливаемого оборудования и программного обеспечения, межсетевой фильтр, который является шлюзом между защищаемой локальной сетью и открытой сетью Интернет, должен располагаться на входе в защищаемую сеть. При этом межсетевой фильтр может быть реализован как на отдельном персональном компьютере, так и на нескольких компьютерах.

2. Защита от внутренних атак

Установка межсетевого фильтра, к сожалению, не обеспечивает защиту локальной сети от внутренних атак. Для внутренней защиты локальной сети на сервере, который является контроллером домена (PDC), необходимо реализовать следующие функции защиты – идентификацию, аутентификация, аудит и контроль целостности информации. Аутентификация должна использоваться со средствами шифрования. Авторизация прав пользователей на доступ к ресурсам выполняется в зависимости от имени пользователя, группы, принадлежности к домену… исходя из политики безопасности. Если серверов несколько (например, для каждого домена свой сервер или существует BDC – резервный сервер), то на каждом из них необходимо реализовать все данные функции защиты.

Если в рассматриваемой системе существует маршрутизатор, то его можно принять за основу для создаваемого комплекса мер безопасности. Если маршрутизатор отсутствует, то в любом случае необходимо будет добавить по крайней мере один компьютер, выполняющий функции межсетевого фильтра. После этого на межсетевой фильтр устанавливаются относящиеся к нему функции безопасности.

Затем на каждом сервере (контроллере домена) надо установить соответствующие ему функции безопасности. Изначально предполагается, что система содержит по крайней мере один сервер и одну рабочую станцию. После чего необходимо реализовать соответствующие функции безопасности на каждой рабочей станции.

В данном методе применяется алгоритм проектирования АБ ИС. Предлагаемый алгоритм является универсальным, не зависящим от топологии рассматриваемой сети (основные требования к сети даны выше), он может быть применен к произвольному количеству защищаемых локальных сетей, кроме того, распределение функций безопасности может производиться для каждой локальной сети независимо от других.

5.3. Графовый метод

Существует метод оценки защищенности, сущность которого состоит в построении оценки защищенности объектов на основе характеристик защитных для этого объекта механизмов и определении достаточности системы ЗИ.

В общем случае объект исследования представляется в виде графа (рис. 5.6), вершинами которого являются так называемые "*модули защиты*" и защищаемые объекты, а *связи* – это возможные пути продвижения

нарушителя. Под "модулем защиты" понимают некоторый конечный результат разложения системы защиты, который можно представить в виде элемента задержки.

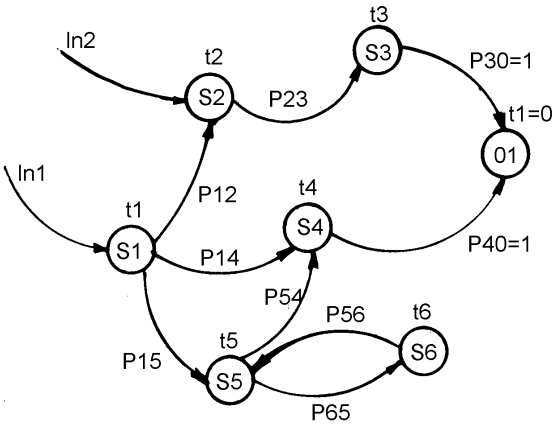

Рис. 5.6. Представление упрощенной модели в виде графа

Таким образом, получившийся граф позволяет проследить возможные пути продвижения "нарушителя" к защищаемому объекту.

Вершина графа, характеризующая "модуль защиты", обладает временем задержки, имеет выходы (ребра графа). Вероятности всех выходящих из одной вершины ребер подчиняются формуле полной вероятности:

$$\sum_{\forall j} P_{ij} = 1 \qquad (5.6)$$

Особенности вершины графа, характеризующей объект защиты, даны в табл. 5.1. Вероятность входа в вершину равна 1. Выход из вершины является точкой выхода из графа. Время задержки в вершине равно 0.

Таблица 5.1

Вершина G_i	Вероятность входа в вершину k	Время задержки	Вероятность выхода из вершины j
Модуль защиты	P_{ki}	$t_{\text{здр } i}$	P_{ij}
Объект	1	0	"Точка выхода"

Цель нарушителя – достичь объекта защиты, преодолев все необходимые модули защиты. На практике такая возможность ограничивается временем. В любой защищенной системе встроены средства обнаружения нарушителя. Существует такая величина, как время обнаружения попытки несанкционированного доступа и проведения мероприятий по его пресечению (t_p). Таким образом, факт защищенности выражается преобладанием времени взлома системы над временем обнаружения попытки несанкционированного доступа (НСД) и проведения мероприятий по его пресечению:

$$t_p < t_{\text{взл}} . \qquad (5.7)$$

Результат исследования должен отображать степень защиты объекта, а оценка может быть представлена как выдача статистического параметра ($t_{\text{взл}}$ – время взлома), характеризующего защищенность системы/объекта в системе; выдача относительного оценочного параметра, характеризующего степень защищенности.

Относительный оценочный параметр $L = t_{взл} / t_p$ отображает достаточность системы защиты при его сопоставлении с выражением (5.7).

В общем случае модель защищаемой системы следующая:

$$\Theta = \{ S, O, I_n \}, \quad (5.8)$$

где S – множество модулей защиты; O – множество объектов защиты; I_n – множество "точек входа" в модель.

Величина $S = \{M, R\}$,

где параметр R характеризует наличие в модуле защиты средств обнаружения нарушителя, а также интервал времени от момента начала доступа к модулю защиты до выдачи информации о попытке НСД $(R = t_{НСД})$; случайный процесс $M = \{f(t), P, A\}$, здесь $f(t)$ – функция плотности вероятности времени взлома для модуля защиты; P – распределение вероятности переходов из данной вершины, $P_i = \{P_{ij}, P_{ij} \neq 0\}$, $\sum_{\forall j} P_{ij} = 1$, A – матрица логических условий; $A = A_{i,j}(t)$ – функция, описывающая возможность перемещения нарушителя по происшествии какого-либо события в системе независимо от $f(t)$.

Множество $O = \{Z, C\}$,

где Z – "кольцо защиты", которое состоит, с одной стороны, из множества модулей защиты, окружающих объект O_i; с другой стороны, Z – множество модулей защиты, при взломе которых можно считать, что НСД состоялся.

Рассмотрим стоимость объекта защиты C. В общем случае это функция времени $C = f(t)$. Параметр введен для определения взаимной ценности объектов, а также оправданности затрат на построение системы защиты.

Исследование подобной модели (5.8) аналитическими методами затруднено, поэтому приведем некоторые упрощения:

1. Величину $f(t)$ заменим на $t_{ср}$ (среднее время взлома модуля защиты). Получаем, что модули защиты характеризуются средним временем задержки $t_{ср}$. Под величиной $t_{ср}$ также можно понимать среднее время, необходимое для взлома модуля защиты.
2. Исключим матрицу логических условий A.
3. Будем считать, что ценность объекта защиты во много раз преобладает над стоимостью организации системы его защиты:

$$\Theta = \{ S, Z, I_n \}, \quad (5.9)$$

где S – множество модулей защиты; Z – вырожденный объект защиты, характеризующийся кольцом защиты; I_n – множество "точек входа" в модель.

Множество $S = \{M, R\}$, где параметр R характеризует наличие в модуле защиты средств обнаружения "взлома", а также интервал времени от момента начала доступа к модулю защиты до выдачи информации о по-

пытке НСД ($R=t_{НСД\ i}$); $M = \{t_{ср}, P\}$, здесь $t_{ср}$ – среднее время взлома модуля защиты; P – распределение вероятности переходов из данной вершины:

$$P_i = \{P_{ij}\ , P_{ij} \neq 0\}, \quad \sum_{ij} P_{ij} = 1. \qquad (5.10)$$

Входными параметрами такой модели (5.9) будут:

- взаимные связи модулей защиты с временными параметрами, как характеристика модуля защиты S;
- наличие средств обнаружения "взлома" R для каждого модуля защиты;
- время t_r, необходимое для проведения мероприятий по его пресечению.

Выходным параметром можно считать значение оценочного параметра L.

Для получения относительного оценочного параметра $L = t_{взл} / t_p$ необходимо знать t_p – время обнаружения попытки НСД ($t_{НСД}$) и проведения мероприятий по его пресечению t_r:

$$t_p = t_{НСД} + t_r, \qquad (5.11)$$

где $t_{НСД}$ отсчитывается с момента входа нарушителя в систему (в "точку входа") до выдачи информации о попытке НСД и является тоже величиной составной:

$$t_{НСД} = t_{0i} + t_{НСД\ I}, \qquad (5.12)$$

здесь t_{0i} – время с момента входа нарушителя в систему (в "точку входа") до попадания в вершину с наличием средств обнаружения нарушителя; $t_{НСД\ i}$ – интервал времени от момента начала доступа к i-му модулю защиты до выдачи информации о попытке НСД.

Получаем формулу для вычисления относительного оценочного параметра

$$L = t_{взл} / (t_{0i} + t_{НСД\ i} + t_r). \qquad (5.13)$$

Оперируя графом защищаемой системы для исследования защищенности конкретного объекта, выделяем его "кольцо защиты" Z и вычисляем среднее время прохождения нарушителя от каждого из входов до выхода, характеризующегося соответствующей вершиной. Одновременно с этим вычисляем $t_{НСД}$, а также вероятность использования данного пути (D_k). Так как переходы между вершинами являются величинами независимыми, можно воспользоваться формулой произведения вероятностей

$$D_k = \prod_{i=1}^{m} P_{ij}, \qquad (5.14)$$

где m – длина пути l, измеренная в "пройденных вершинах".

Искомый параметр $L = \min(\forall \mathrm{D_k}), \quad \mathrm{k} = (1, \mathrm{N})$.

Анализируя значения L, можно делать следующие выводы:

- при $L \geq 1$ объект защищен адекватно;
- при очень больших значениях L появляется возможность упрощения системы защиты с целью экономии средств на ее организацию. Также лю-

бой модуль защиты на практике вносит некоторые неудобства в работу защищаемой системы, и его удаление улучшает ее основные характеристики (быстродействие, мобильность и т.д.);

- при $L<1$ – степень защиты объекта недостаточна, необходимы мероприятия по увеличению параметра L.

Проведенное исследование позволяет строить два вида оценки:

- оценка защищенности конкретного объекта в вычислительной системе;

- оценка защищенности всей системы, т.е. совокупность защищенностей каждого объекта в системе (иными словами, оценка защищенности всей системы может характеризоваться наихудшей оценкой защищенности объекта в вычислительной системе).

Таким образом, представленный метод позволяет учитывать взаимные связи между компонентами системы защиты независимо от их практического исполнения.

5.4. Метод весовых коэффициентов

Исходными данными для проведения оценки и анализа служат результаты анкетирования субъектов отношений, предназначенные для уяснения направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых автоматизированной системой и условий расположения и эксплуатации объекта. Благодаря такому подходу возможно:

- установить приоритеты целей безопасности для субъекта отношений;
- определить перечень актуальных источников угроз;
- определить перечень актуальных уязвимостей;
- оценить взаимосвязь угроз, источников угроз и уязвимостей;
- определить перечень возможных атак на объект;
- описать возможные последствия реализации угроз.

Результаты проведения оценки и анализа могут быть использованы при выборе адекватных оптимальных методов парирования угрозам, а также при аудите реального состояния информационной безопасности объекта для целей его страхования.

При определении актуальных угроз, экспертно-аналитическим методом определяются объекты защиты, подверженные воздействию той или иной угрозы, характерные источники этих угроз и уязвимости, способствующие реализации угроз.

На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей, из которой определяются возможные последствия реализации угроз (атаки) и вычисляется коэффициент опасности этих атак как произведение коэффициентов опасности соответствующих угроз и источников угроз, определенных ранее.

Кратко о главном

В основе метода экспертных оценок информационной безопасности лежит понятие профиля защиты стандарта ISO/IEC 15408. Формально описать вероятности отдельных угроз, атак, эффективности отдельных политик безопасности очень сложно. В связи с этим, для получения количественной оценки риска используются экспертные оценки, основанные на использовании кластера исходов.

Метод информационных потоков применим для распределенной вычислительной системы. Он позволяет построить алгоритм распределения функций безопасности с учетом всех видов информационных потоков, имеющих отношение к оцениваемой ИС.

Сущность графового метода состоит в построении оценки защищенности объектов на основе характеристик защитных для этого объекта механизмов и определении достаточности системы ЗИ. Объект исследования представляется в виде графа, вершинами которого являются модули защиты и защищаемые объекты, а связями – возможные пути продвижения нарушителя. Результат исследования должен отображать степень защиты объекта, а оценка может быть представлена как выдача статистического параметра "время взлома".

Исходными данными для оценки по методу весовых коэффициентов служат результаты анкетирования субъектов отношений, предназначенные для уяснения направленности их деятельности, предполагаемых приоритетов целей безопасности, задач, решаемых автоматизированной системой и условий расположения и эксплуатации объекта. На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей.

Контрольные вопросы

1. На чем основан метод экспертных оценок?
2. Как определить риски через коэффициенты значимости?
3. Какие варианты информационных потоков могут быть между отправителем и получателем?
4. Как строится алгоритм распределения функций безопасности?
5. В чем суть графового метода оценки защищенности?
6. Каким образом определяется факт защищенности?
7. От чего зависит оценочный параметр защищенности?
8. Какие выводы можно сделать, если параметр защищенности меньше 1, больше 1 и много больше 1?

Глава 6. КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Качественные и количественные аспекты оценки эффективности защиты

Во многих работах по защите информации [11 – 13] были изложены основные постулаты, смысл которых в следующем: абсолютную защиту создать нельзя; СЗИ должна быть комплексной; СЗИ должна быть адаптируемой к изменяющимся условиям.

К этим аксиомам нужно добавить и другие суждения. Во-первых, СЗИ должна быть именно системой, а не простым, во многом случайным и хаотичным набором некоторых технических средств и организационных мероприятий, как это зачастую наблюдается на практике. Во-вторых, системный подход к защите информации должен применяться, начиная с подготовки технического задания и заканчивая оценкой эффективности и качества СЗИ в процессе ее эксплуатации.

Прежде всего, СЗИ должна иметь целевое назначение. Причем, чем более конкретно сформулирована цель ЗИ, детально уяснены имеющиеся для этого ресурсы и определен комплекс ограничений, тем в большей степени можно ожидать получение желаемого результата. Если цель обеспечения информационной безопасности проста (формулируется скалярным показателем) и принципиально достижима, то достаточно сравнительно несложных по составу и структуре средств ЗИ.

Однако при расширении круга проблем, которые нужно решать для обеспечения интегральной информационной безопасности, содержание целевого назначения системы на формализованном уровне приобретает многомерный, векторный характер. При этом значимость свойств отдельных элементов СЗИ снижается, а на первый план выдвигаются общесистемные задачи – определение оптимальной структуры и режимов функционирования системы, организация взаимодействия между ее элементами, учет влияния внешней среды и др. При целенаправленном объединении элементов в систему последняя приобретает специфические свойства, изначально не присущие ни одной из ее составных частей. При системном подходе имеют первостепенное значение только те свойства элементов, которые определяют взаимодействие друг с другом и оказывают влияние на систему в целом, а также на достижение поставленной цели.

Результативное решение задач анализа и синтеза СЗИ не может быть обеспечено одними лишь способами умозрительного описания их поведения в различных условиях – ЗИ выдвигает проблемы, требующие количественной оценки характеристик. Такие данные, полученные экспериментально или путем математического моделирования, должны раскрывать свойства СЗИ. Основным из них является эффективность, под которой понимается степень соответствия результатов защиты информации поставленной цели. Последняя, в зависимости от имеющихся ресурсов, знаний разработчиков и других факторов, может быть достигнута в той или иной мере, при этом возможны альтернативные пути ее реализации. Эффективность имеет непосредственную связь с другими системными свойствами, в том числе качеством, надежностью, управляемостью, помехозащищенностью, устойчивостью. Поэтому количественная оценка эффективности позволяет измерять и объективно анализировать основные свойства систем на всех стадиях их жизненного цикла, начиная с этапа формирования требований и эскизного проектирования.

Зачастую заказчик СЗИ плохо представляет себе значение того или иного средства и его вклад в общий уровень безопасности и в результате происходит увеличение затрат при практической неопределенности достигнутого эффекта. Как следствие, далеко не всегда заказчик СЗИ получает то, что ему реально нужно, и не может объективно проверить и оценить качество и эффективность предложенного решения.

Средства ЗИ в соответствии с действующими нормами и правилами подлежат обязательной или добровольной сертификации. Однако сертификация не является совершенным инструментом и не дает необходимых гарантий. В лучшем случае проверяется только 85 % всех возможных состояний, а обычно – 60 – 70 %.

Указывается, что сертификация продукции на соответствие требованиям государственных стандартов по безопасности информации или иных нормативных документов, утвержденных Гостехкомиссией РФ, подтверждается с определенной степенью достоверности. Однако чему конкретно должна быть равна эта достоверность, является ли этот термин эквивалентным вероятностно-статистическому пониманию, не говорится. Между тем, на испытательные центры (лаборатории), проводящие испытания образцов сертифицируемой продукции и участвующие в предварительной проверке ее производства, прямо возложена ответственность за достоверность результатов. При таком положении дел нормативное требование обеспечения достоверности результатов испытаний отдельных средств и, тем более всей СЗИ, остается пустой декларацией. Таким образом, даже если элементы СЗИ формально успешно прошли все сертификационные

испытания и имеют полный комплект удостоверяющих документов, это отнюдь не означает того, что реально будет обеспечен требуемый уровень качества.

Создание и эксплуатация ИС должны проводиться в соответствии с существующим законодательством и требованиями нормативно-технических документов. Данное положение, разумеется, применимо к любому виду организованной деятельности, однако ИТ развиваются исключительно быстрыми темпами, и почти всегда нормативная база отстает от потребностей практики. Здесь подобное отставание законов, нормативных актов, национальных и отраслевых стандартов, а также методического обеспечения, оказывается особенно критичным.

Трудности объективного подтверждения эффективности СЗИ коренятся в несовершенстве существующей нормативной базы, а также в сложившихся в ИТ подходах, принципиально отличающихся от разработанных в традиционной инженерии. Специалистами, например, отмечается недостаточная проработанность такого аспекта нормативного обеспечения, как система показателей информационной безопасности. В неудовлетворительном состоянии находится система критериев безопасности, в том числе, таких, как эффективность СЗИ. К серьезным проблемам относится и игнорирование стохастичной природы событий и явлений, которые возникают в процессе защиты информации, абстрагирование от их экономического содержания в нормативном, методическом и прикладном аспектах.

Эти же замечания можно отнести и к международной нормативной базе по информационной безопасности, включающей около 50 международных стандартов ИСО/МЭК на критерии оценки безопасности ИТ и методы защиты средств и систем ИТ. Применение методов функциональной стандартизации в области информационной безопасности изложены в международном стандарте ИСО/МЭК 15408-99 "Критерии оценки безопасности информационных технологий". Фактически, "Общие критерии" предлагают набор исторически сложившихся и, самое главное, привычных в отрасли подходов к безопасности, которые используются, чтобы создавать изделия или системы, отражающие не столько потребности заказчика, сколько возможности разработчика. Важно отметить, что по своей сути они являются не критериями в полном смысле этого термина, а неким подобием общих технических требований, определяющих облик систем в зависимости от их назначения и условий функционирования.

При создании и развитии сложных, распределенных, тиражируемых информационных систем требуется, как известно, гибкое формирование и применение гармонизированных совокупностей базовых стандартов и нормативных документов разного уровня, выделение в них требований и рекомендаций, необходимых для реализации заданных функций информа-

ционных систем. Такие совокупности базовых стандартов должны адаптироваться и конкретизироваться применительно к определенным классам проектов, функций, процессов и компонентов информационных систем.

В связи с этой потребностью выделилось и сформировалось понятие "профилей" как основного инструмента функциональной стандартизации. Понятно, что число возможных профилей защиты во много раз превышает исходное количество документов, на которых они могут базироваться, поэтому провести априорную оценку эффективности всех возможных профилей невозможно. С другой стороны, профиль защиты должен создаваться или выбираться исходя из требований к показателям информационной безопасности, установленных заказчиком заранее. Принятые подходы, включая те из них, которые указаны в существующих стандартах, не позволяют сделать такой выбор, чрезвычайно важный для практики. Оценку же эффективности профилей защиты можно осуществить только с использованием комплексных показателей, которые имеют вероятностный или стоимостной характер. При этом следует обратить внимание, что, в отличие от официальных нормативных документов, в аналитических материалах, опубликованных сотрудниками Гостехкомиссии, прямо указывается на необходимость использования в качестве основного критерия эффективности СЗИ соответствующей вероятности.

Нормативные документы по оценке безопасности ИТ практически не содержат конкретных методик, в результате чего величина разрыва между общими декларациями и конкретным инструментарием по реализации и контролю их положений является недопустимой. Исходя же из своего предназначения, методическая база должна охватывать все критически важные аспекты обеспечения и проверки выполнения требований, предъявляемых к информационной безопасности.

Объективным видом оценки эффективности СЗИ является функциональное тестирование, предназначенное для проверки фактической работоспособности реализованных механизмов безопасности и их соответствия предъявленным требованиям, а также обеспечивающее получение статистических данных. В силу того, что средства безопасности обладают ограниченными возможностями по противодействию угрозам, всегда существует вероятность нарушения защиты, даже если во время тестирования механизмы безопасности не были обойдены или блокированы. Для оценки этой вероятности должны проводиться дополнительные исследования.

В методическом плане определение эффективности СЗИ должно заключаться в выработке суждения относительно пригодности способа действий персонала или приспособленности технических средств к достижению цели защиты информации на основе измерения соответствующих показателей, например, при функциональном тестировании.

Таким образом, при использовании современной методической базы, оценка эффективности СЗИ носит в основном нечеткий, субъективный характер; практически полностью отсутствуют нормированные количественные показатели, учитывающие возможные случайные или преднамеренные воздействия. В результате достаточно сложно, а зачастую и невозможно, оценить качество функционирования информационной системы при наличии несанкционированных воздействий на ее элементы, а, соответственно, и определить, чем один вариант проектируемой системы лучше другого.

Представляется, что решением проблемы комплексной оценки эффективности СЗИ является использование системного подхода, позволяющего еще на стадии проектирования количественно оценить уровень безопасности и создать механизм управления рисками. Однако этот путь реализуем при наличии соответствующей системы показателей и критериев.

В соответствии с современной теорией оценки эффективности систем, качество любого объекта, в том числе и СЗИ, проявляется лишь в процессе его использования по назначению, поэтому наиболее объективным является оценивание по эффективности применения.

Проектирование, организация и применение СЗИ фактически связаны с неизвестными событиями в будущем и поэтому всегда содержат элементы неопределенности. Кроме того, присутствуют и другие причины неоднозначности, такие как недостаточно полная информация для принятия управленческих решений или социально-психологические факторы. Поэтому, например, этапу проектирования СЗИ естественным образом сопутствует значительная неопределенность.

По мере реализации проекта ее уровень снижается, но никогда эффективность СЗИ не может быть адекватно выражена и описана детерминированными показателями. Процедуры испытаний, сертификации или лицензирования не устраняют полностью неопределенность свойств СЗИ или ее отдельных элементов и не учитывают случайный характер атак. Поэтому объективной характеристикой качества СЗИ – степенью ее приспособленности к достижению требуемого уровня безопасности в условиях реального воздействия случайных факторов может служить только вероятность, характеризующая степень возможностей конкретной СЗИ при заданном комплексе условий.

В общей теории систем такая характеристика называется вероятностью достижения цели операции или вероятностью выполнения задачи системой. Данная вероятность должна быть положена в основу комплекса показателей и критериев оценки эффективности СЗИ. При этом критериями оценки служат понятия пригодности и оптимальности. Пригодность означает выполнение всех установленных к СЗИ требований, а оптимальность – достижение одной из характеристик экстремального значения при

соблюдении ограничений и условий на другие свойства системы. При выборе конкретного критерия необходимо его согласование с целью, возлагаемой на СЗИ.

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

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

Однако в такой методике есть ряд отрицательных моментов. Во-первых, оценка оптимального уровня гарантий безопасности в определяющей степени зависит от ущерба, связанного с ошибкой в выборе конкретного значения показателя эффективности. Во-вторых, для получения численных оценок риска необходимо знать распределение ряда случайных величин. Это, конечно, в определенной степени ограничивает количественное исследование уровней гарантий безопасности, предоставляемых СЗИ, но, тем не менее, во многих практических случаях такие оценки можно получить, например, с помощью имитационного моделирования или по результатам активного аудита СЗИ.

6.2. Оценка экономической эффективности КСИБ

Для оценки экономической эффективности формальную модель КСИБ необходимо дополнить множеством сотрудников предприятия $Y = \{y_q\}$, обращающихся к объекту o_j с вероятностью t_{qj}. Сумма вероятностей равна 1.

$$\sum_{\forall q}\sum_{\forall j} t_{qj} = 1. \qquad (6.1)$$

Использование объекта приносит доход предприятию w_j. Доход, получаемый от всех обращений к объекту,

$$e_j = w_j \sum_{\forall q} t_{qj} \,. \tag{6.2}$$

Весь доход от использования всех объектов

$$Д = \sum_{\forall j} w_j \sum_{\forall q} t_{qj} \,. \tag{6.3}$$

Пусть имеется множество хакеров, каждый из которых может с вероятностью p_{lj} обратиться к области j. А вероятность успешного получения доступа равна τ_{xj}. Математическое ожидание потерь от одного хакера в отношении объекта o_j

$$DX_{lj} = S_j \; p_{lj} \; \tau_{lj} \,. \tag{6.4}$$

Потери от всех хакеров в отношении объекта o_j

$$DX_j = S_j \sum_{\forall l} p_{lj} \; \tau_{lj} \,. \tag{6.5}$$

И потери для всего предприятия

$$П = \sum_{\forall j} S_j \sum_{\forall l} p_{lj} \; \tau_{lj} \,. \tag{6.6}$$

Для j-го объекта стоимость его защиты определяется его характеристиками o_j и характеристиками механизма защиты m_k:

$$z_j = \alpha_k + \beta_k \cdot o_j \,. \tag{6.7}$$

Стоимость защиты всех объектов определяется из соотношения

$$C = \sum_{\forall j} z_j \,. \tag{6.8}$$

А полные затраты равны сумме потерь от взлома и стоимости защиты

$$З_{полн} = П + C. \tag{6.9}$$

Экономическая эффект от КСИБ определяется разностью доходов и затрат

$$Э = Д - З_{полн}. \tag{6.10}$$

Следовательно экономическая эффективность

$$ЭФФ = \frac{Д - З_{полн}}{З_{полн}} \,. \tag{6.11}$$

Кратко о главном

Результативное решение задач анализа и синтеза СЗИ не может быть обеспечено одними лишь способами умозрительного описания их поведения в различных условиях – ЗИ выдвигает проблемы, требующие количественной оценки характеристик. Такие данные, полученные экспериментально или путем математического моделирования, должны раскрывать свойства СЗИ. Основным из них является эффективность, под которой понимается степень соответствия результатов защиты информации поставленной цели.

Эффективность, в зависимости от имеющихся ресурсов, знаний разработчиков и других факторов, может быть достигнута в той или иной мере, при этом возможны альтернативные пути ее реализации. Она имеет непосредственную связь с другими системными свойствами, в том числе качеством, надежностью, управляемостью, помехозащищенностью, устойчивостью. Поэтому количественная оценка эффективности позволяет измерять и объективно анализировать основные свойства систем на всех стадиях их жизненного цикла, начиная с этапа формирования требований и эскизного проектирования.

Для предприятия эффективность прежде всего связана с экономическими вопросами. Оценка экономической эффективности возможна на основе формальной модели КСИБ с использованием вероятностного подхода

Контрольные вопросы

1. Что означает понятие *эффективности* СЗИ?
2. В чем заключаются трудности объективного подтверждения эффективности СЗИ?
3. Каковы качественные аспекты оценки эффективности?
4. Каковы количественные аспекты оценки эффективности?
5. Какими множествами необходимо дополнить формальную модель КСИБ для оценки экономической эффективности?

ЗАКЛЮЧЕНИЕ

Эффективность работы любого предприятия напрямую зависит от защищенности его информационных ресурсов и безопасности всех субъектов, участвующих в процессе производства и использующих эти ресурсы. Решение этой проблемы только путем усиления уровня защищенности ресурсов не позволяет достичь результата, адекватного требованиям современного общества.

Построение системы информационной безопасности, обеспечивающей выполнение таких требований, возможно только с использованием системного подхода для учета всех взаимосвязанных факторов, значимых для решения проблемы обеспечения безопасности объектов и субъектов предприятия, включая оценки рисков, экономическую эффективности и др.

Одним из важнейших шагов усиления безопасности предприятия является привлечение внимания людей к вопросам безопасности, осознание сотрудниками всей серьезности проблемы и принятие политики безопасности организации, изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения. Осведомленность должна быть включена во все уровни организации, начиная с самого верхнего, где и принимается политика безопасности. На основе этой политики и распределения ответственности создается модель защиты.

Обзор качественных и количественных методов показывает, что в настоящее время не существует универсального метода оценки степени

защищенности ИС. Существующая нормативная база может достаточно адекватно оценить степень защищенности ИС. Однако такая оценка будет учитывать лишь организационные, экономические, человеческие факторы. Отрицательным моментом такого вида оценок является недостаточный учет технических и количественных показателей системы.

Существующие методы количественной оценки позволяют оценить лишь часть технических и количественных показателей ИС.

Однобокость качественных и количественных оценок определяет необходимость интеграции этих методов. Созданные таким образом на основе системного подхода с учетом временных показателей комплексные методы оценки защищенности позволят учитывать как технические, так и качественные показатели ИС. В то же время вероятностный характер отдельных параметров защиты говорит о том, что итоговая оценка защищенности также будет носить вероятностный характер.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. *Анин, Б. Ю.* Защита компьютерной информации / Б. Ю. Анин. – СПб. : БХВ-Петербург, 2000. – 376 с. – ISBN 5-8206-0104-1.
2. *Астахов, А.* Анализ защищенности корпоративных систем / А. Астахов // Открытые системы, 2002. – № 7 – 8.
3. *Барсуков, В. С.* Безопасность: технологии, средства, услуги / В. С. Барсуков. – М. : Кудиц-Образ, 2001. – 500 с. – ISBN 5-93378-017-0.
4. *Он же*. Обеспечение информационной безопасности / В. С. Барсуков. – М. : Эко-Трендз, 1998.
5. *Водолазкий, В. В*. Современные технологии безопасности / В. В. Водолазкий. – М. : Нолидж, 2000. – 496 с. – ISBN 5-89251-073-5.
6. ГОСТ Р ИСО/МЕК 15408-1-2001 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Часть 1. Введение и общая модель.
7. ГОСТ Р ИСО/МЕК 15408-2-2001. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Часть 2. Функциональные требования безопасности.
8. *Захаров, А. П.* Методология оценки информационной безопасности профиля защиты / А. П. Захаров. – http://beda.stup.ac.ru/rv-conf/.
9. Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ Гостехкомиссии России. – М. : Военное изд-во, 1992.
10. Защита программ и данных: учебник / П. Ю. Белкин [и др.] – М. : Радио и связь, 1999. – 188 с. – ISBN 5-256-01533-8.
11. *Илларионов, Ю. А*. Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах : монография / Ю. А. Илларионов, М. Ю. Монахов ; Владим. гос. ун-т. – Владимир, 2004. – 212 с. – ISBN 5-89368-493-1.
12. *Конев, И. Р.* Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2004. – 752 с. – ISBN 5-94157-280-8.
13. *Монахов, М. Ю*. Информационные образовательные сети. Основы теории и методика применения : монография / М. Ю. Монахов ; Владим. гос. ун-т. – Владимир, 2001.
14. Организация и современные методы защиты информации / под общ. ред. С. А. Диева, А. Г. Шаваева. – М. : Банковский деловой центр, 1998. – 472 с. – ISBN 5-89280-022-9.
15. *Петраков, А. В*. Основы практической защиты информации / А. В. Петраков. – М. : МТУСИ, 2001. – 360 с. – ISBN 5-256-01592-2.

16. *Петраков, А. В*. Охрана и защита современного предприятия / А. В. Петраков, П. С. Дорошенко, Н. В. Савлуков. – М. : МТУСИ, 2001.
17. *Романец, Ю. В*. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М. : Радио и связь, 1999. – 376 с. – ISBN 5-256-01518-4.
18. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Термины и определения : Руководящий документ Гостехкомиссии России. – М. : Военное изд-во, 1992.
19. *Столлингс, В*. Основы защиты сетей. Приложения и стандарты / В. Столлингс. – М. : Вильямс, 2002. – 432 с. – ISBN 5-8459-0293-3.
20. *Хорев, А. А*. Способы и средства защиты информации / А. А. Хорев. – М. : МОРФ, 1999. – 256 с. – ISBN 5-7695-1839-1.
21. *Шлыков, В. В.* Безопасность предприятия в условиях рынка : учеб. пособие для вузов / В. В. Шлыков. – Рязань : Горизонт, 1997.
22. International standard ISO/IEC 15408:1999, “Information technology – Security techniques –Evaluation criteria for IT security – Part 1- Part 3”.
23. International standard ISO/IEC 17799:1999, “Information technology – Code of practice for information security managment”.
24. Trusted computer system evaluation criteria (Orange Book). – Department of Defence Standart, USA, 1983.

Учебное издание

Комплексная защита объектов информатизации. Книга 10

ПОЛЯНСКИЙ Дмитрий Александрович

ОЦЕНКА ЗАЩИЩЕННОСТИ

Учебное пособие

Редактор Е.В. Невская
Корректор Е.В. Афанасьева
Компьютерная верстка С.В. Павлухиной

ЛР № 020275. Подписано в печать 03.11.05.
Формат 60x84/16. Бумага для множит. техники. Гарнитура Таймс.
Печать на ризографе. Усл. печ. л. 4,65. Уч-изд. л. 4,95. Тираж 100 экз.
Заказ
Издательство
Владимирского государственного университета.
600000, Владимир, ул. Горького, 87.