МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И ФИНАНСОВ»

КАФЕДРА ИНФОРМАТИКИ

А.М. БЛИНОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

ЧАСТЬ 1

ИЗДАТЕЛЬСТВО
САНКТ-ПЕТЕРБУРГСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
ЭКОНОМИКИ И ФИНАНСОВ
2010

Рекомендовано научно-методическим советом университета

ББК 65.39
Б 69

Блинов А.М.

Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

В первой части учебного пособия рассматриваются основные разделы дисциплины «Информационная безопасность»: проблемы информационной безопасности, термины и определения, нормативно-правовые документы, стандарты информационной безопасности, модели безопасности.

Предназначено для студентов старших курсов дневной формы обучения специальности 080801 «Прикладная информатика в экономике».

Рецензенты:

канд. техн. наук, доцент, зам. зав. кафедрой информатики и компьютерных технологий СПбГГИ **А.Б. Маховиков**

канд. техн. наук, доцент кафедры информатики и математики СПбГУП **Л.В. Путькина**

ВВЕДЕНИЕ

В учебном пособии рассматривается текущее состояние дел в области информационной безопасности. Приводятся основные термины и определения согласно принятым нормативно-правовым документам на территории России.

Одна из глав посвящена обзору международных оценочных стандартов в области информационной безопасности.

Освещаются вопросы построения защищенных информационных систем на основе применения математических моделей.

Данное учебное пособие предназначено для студентов старших курсов специальности 080801 «Прикладная информатика в экономике». Является первой теоретической частью цикла учебных пособий по информационной безопасности.

ГЛАВА 1. ПОНЯТИЕ И ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблема обеспечения информационной безопасности в рамках любого государства в последнее время все чаще является предметом обсуждения не только в научных кругах, но и на политическом уровне. Данная проблема также становится объектом внимания международных организаций, в том числе и ООН.

Современный этап развития общества характеризуется возрастающей ролью электронных ресурсов, представляющих собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений.

Стремительный рост компьютерных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие достижения в этих сферах, а с другой стороны, стал источником самых непредсказуемых и вредных для человеческого общества последствий. В результате, можно говорить о появлении принципиально нового сегмента международного противоборства, затрагивающего как вопросы безопасности отдельных государств, так и общую систему международной безопасности на всех уровнях.

Событие, произошедшее в октябре 1988 года в США, названо специалистами крупнейшим нарушением безопасности американских компьютерных систем из когда-либо случавшихся. 23-летний студент выпускного курса Корнельского университета Роберт Т. Моррис создал и запустил в компьютерной сети ARPANET программу, представлявшую собой разновидность компьютерных вирусов – сетевых «червей». В результате атаки был полностью или частично заблокирован ряд общенациональных компьютерных сетей, в частности Internet, CSnet, NSFnet, BITnet, ARPANET и военная сеть Milnet. В итоге вирус поразил более 6200 компьютерных систем по всей Америке, включая системы многих крупнейших университетов, институтов, правительственных лабораторий, частных фирм, военных баз, клиник, агентства NASA. Общий ущерб от этой атаки оценивается специалистами минимум в 100 млн долларов. Моррис был исключен из университета с правом повторного поступления через год и приговорен судом к штрафу в 270 тыс. долларов и трем месяцам тюремного заключения.

В 1991 году в ходе операции «Буря в пустыне», с помощью электронных излучателей вооруженным силам США удалось нарушить радио и телефонную связь практически на всей территории Ирака. Систему управления ПВО Ирака спецслужбам США удалось вывести из строя за

счет специальных вирусов, введенных в компьютерную систему из памяти принтеров, приобретенных для этой системы у одной коммерческой фирмы.

Во время войны в Косово, Югославская Федерация, для того чтобы приостановить военные операции, организовала «хакерскую» войну, которая выражалась в совершении атак на определенные веб-сайты США, Великобритании и других стран НАТО, которые поддерживали компьютерные системы Белого Дома и Пентагона. В результате британское метеорологическое бюро было парализовано и не могло предоставлять необходимые метеорологические услуги для воздушных атак НАТО, поэтому некоторые из планов воздушных атак пришлось отменить. Представители объединенного штаба подтвердили использование информационного оружия во время Косовской компании.

Становится очевидной необходимость теоретической разработки международно-правовых основ регулирования взаимоотношений субъектов международного права в сфере качественно изменяющихся под воздействием информационной революции условий обеспечения международной и национальной безопасности, в сфере обеспечения информационной безопасности государства.

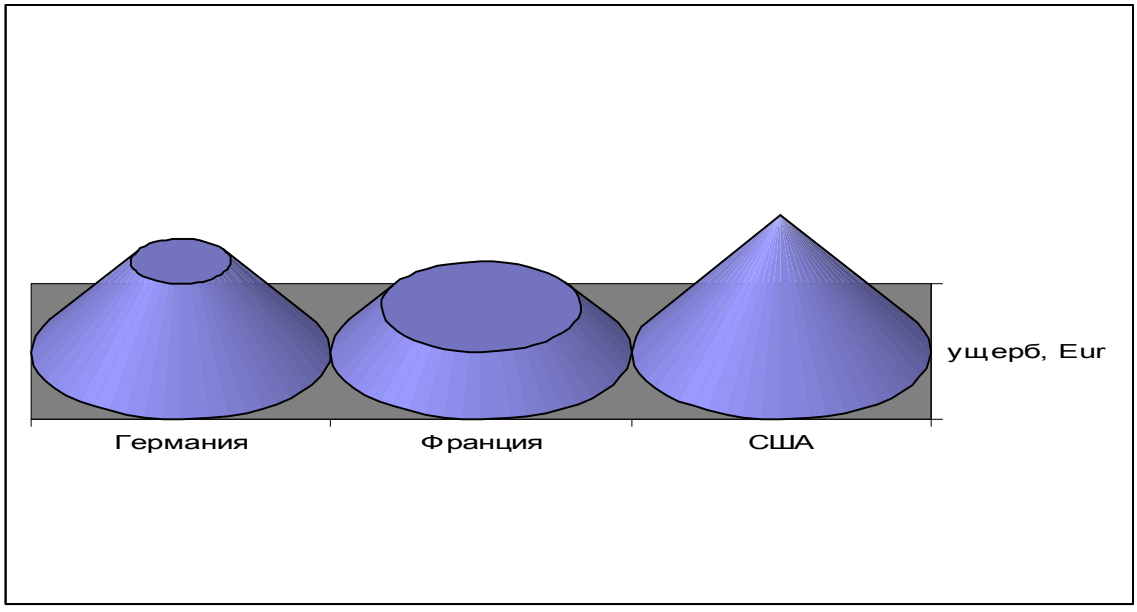

Рис. 1. Соотношение ущербов в связи
с компьютерными преступлениями в разных странах

Новые технологии порождают и новые преступления. Согласно унификации Комитета министров Европейского Совета определены криминальные направления компьютерной деятельности. К ним относятся:

- компьютерное мошенничество;
- подделка компьютерной информации;

- повреждение данных или программ;
- компьютерный саботаж;
- несанкционированный доступ к информации;
- нарушение авторских прав.

Актуальность проблемы информационной безопасности заключается:

- в особом характере общественной опасности возможных преступлений;
- в наличии тенденции к росту числа преступлений в информационной сфере;
- в неразработанности ряда теоретических положений, связанных с информационной безопасностью.

Убытки ведущих компаний в связи с нарушениями безопасности информации составляют миллиарды евро, причем только треть опрошенных компаний смогли определить количественно размер потерь. Так, по данным зарубежных правоохранительных органов, в Германии с использованием компьютеров похищается до 2 млрд евро ежегодно, во Франции – до 1 млрд евро, в США – до нескольких миллиардов евро. Атакам через Интернет подвергались 57% опрошенных, 55% отметили нарушения со стороны собственных сотрудников. По данным МВД РФ в 1997 году было зарегистрировано 7 преступлений в сфере компьютерных технологий, в 1998 году – 66, в 1999 году – 294, в 2002 году – 3782 преступлений, в 2006 году – около 15000.

Проблема обеспечения безопасности носит комплексный характер, для ее решения необходимо сочетание законодательных, организационных и программно-технических мер и средств. В курсе Информационной безопасности нас будут интересовать программно-технические средства, реализующиеся программным и аппаратным обеспечением, решающие разные задачи по защите. Они могут быть встроены в операционные системы, либо могут быть реализованы в виде отдельных продуктов. Во многих случаях центр тяжести смещается в сторону защищенности операционных систем.

23 декабря 1999 года Генеральная Ассамблея ООН приняла резолюцию, в которой выражается озабоченность тем, что распространение и использование современных информационных технологий и средств потенциально может быть использовано в целях, несовместимых с задачами обеспечения международной стабильности и безопасности.

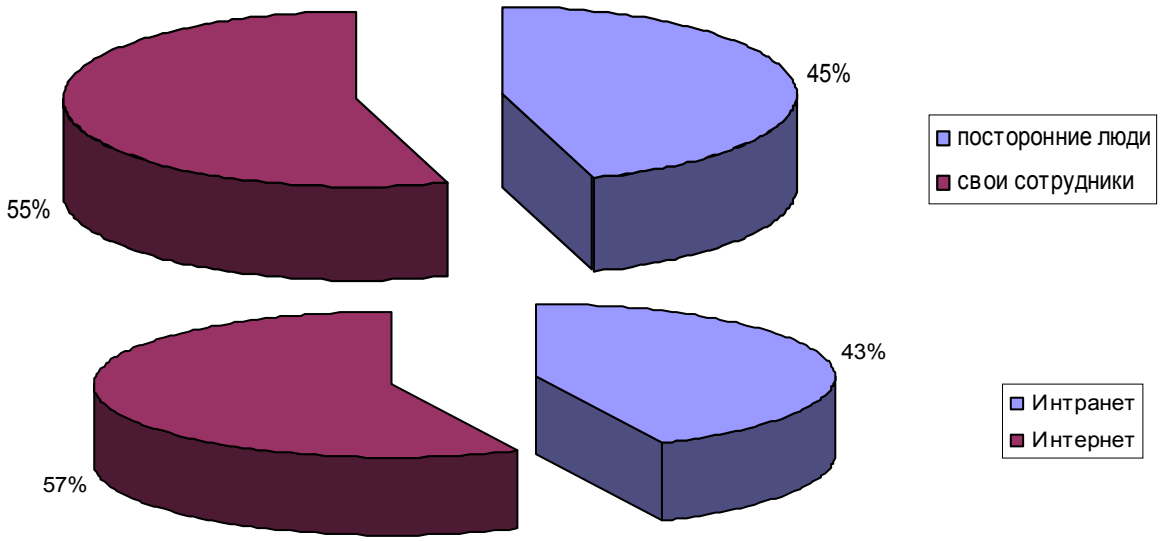

Рис. 2. Соотношение различных видов атак

В России положения, касающиеся информационной безопасности, включены в «Концепцию национальной безопасности РФ», утвержденную Указом Президента РФ от 17.12.1997 г., в ред. Указа Президента от 10.01.2000 г., а также в Военную доктрину РФ, утвержденную Указом Президента РФ от 21.04.2000 г. Кроме того, в рамках Совета безопасности РФ разрабатывается проект «Концепции совершенствования правового обеспечения информационной безопасности РФ».

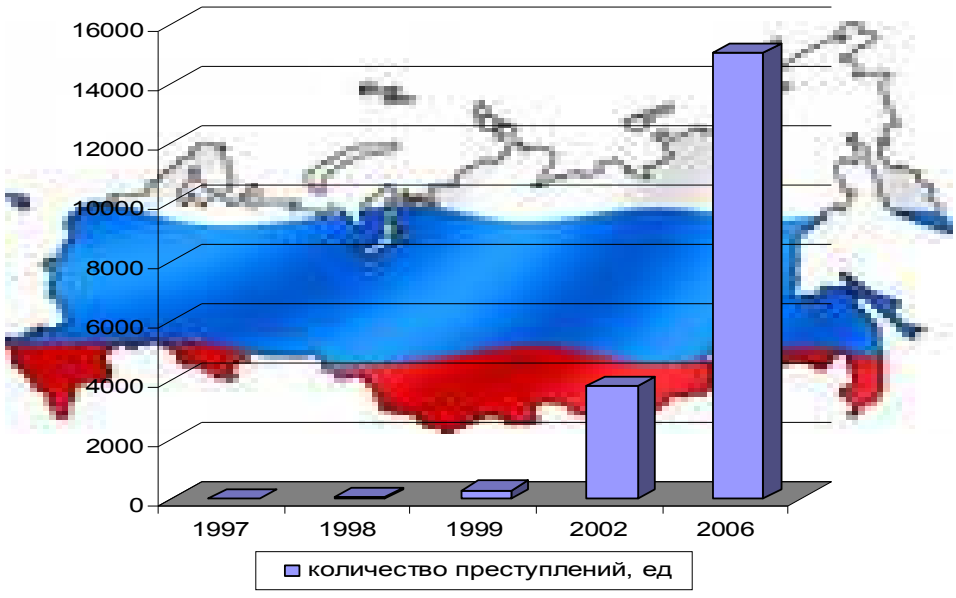

Рис. 3. Рост количества преступлений, регистрируемый на территории РФ

09 сентября 2000 года Президентом РФ была утверждена Доктрина информационной безопасности РФ. Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации, развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

В декабре 2002 года принят ФЗ «О внесении изменений и дополнений в Закон РФ «О правовой охране программ для ЭВМ и баз данных», 29 июля 2004 года подписан Закон «О коммерческой тайне», на рассмотрении в Государственной Думе находится законопроект «Об информации персонального характера». Назрела необходимость разработки и принятия законов «О служебной тайне», «О профессиональной тайне».

Принятие указанных законов обусловлено положениями Доктрины информационной безопасности РФ, в которой в качестве основных составляющих национальных интересов России в информационной сфере выделяются меры правового характера, обеспечивающие конституционные права человека и гражданина свободно искать, передавать, производить и распространять информацию любым законным способом, конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Необходимо сказать, что кроме вышеуказанных законов за последнее десятилетие в России реализован комплекс мер по совершенствованию обеспечения информационной безопасности. Для правового обеспечения информационной безопасности приняты Федеральные законы «О государственной тайне», «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», а также ряд других нормативных актов. В новых Гражданском и Уголовном кодексах предусмотрена ответственность за правонарушения и преступления в информационной сфере.

Специалистам в области информационной безопасности сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин.

Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины.

Во-первых, стандарты и спецификации – одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях

информационной безопасности. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами.

Во-вторых, и те и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов.

Отмеченная роль стандартов зафиксирована в основных понятиях закона РФ «О техническом регулировании» от 27 декабря 2002 года:

- ***стандарт*** – документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;
- ***стандартизация*** – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Примечательно также, что в число принципов стандартизации, провозглашенных в статье 12 упомянутого закона, входит принцип применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если «такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения». С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. В курсе рассматриваются наиболее важные из них, знание которых необходимо и разработчикам средств защиты, и системным администраторам, и руководителям соответствующих подразделений и даже пользователям.

Среди множества различных стандартов и спецификаций, можно выделить две группы документов, которые будут рассмотрены в данном курсе:

- оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;
- спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы, разумеется, дополняют друг друга. Оценочные стандарты описывают важнейшие, с точки зрения информационной безопасности, понятия и аспекты информационных систем (ИС), играя роль организационных и архитектурных спецификаций. Спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования.

Из числа **оценочных** необходимо выделить **стандарт** Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaluation Criteria – TCSEC) и его интерпретацию для сетевых конфигураций (Trusted Network Interpretation), «Гармонизированные критерии Европейских стран» (Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France – Germany – the Netherlands – the United Kingdom), международный стандарт «Критерии оценки безопасности информационных технологий» (Common Criteria for Information Technology Security Evaluation (CCITSE), и, конечно, Руководящие документы Гостехкомиссии России. К этой же группе относятся: Федеральный стандарт США **(**Federal Information Processing Standardization, FIPS) «Требования безопасности для криптографических модулей» (FIPS 140-2), Британский стандарт BS 7799 часть 2 «Управление информационной безопасностью. Практические правила» (Information Security Management Systems – Specification with guidance for use), а также международный стандарт ISO/IEC 17799 «Информационная технология. Практический кодекс по менеджменту информационной безопасности» (Information Technology – Code of practice for information security management), являющийся изложением BS 7799 часть 1.

Технические спецификации, применимые к современным распределенным ИС, создаются, главным образом, «Тематической группой по технологии Интернет» (Internet Engineering Task Force, IETF) и ее подразделением – рабочей группой по безопасности. Ядром рассматриваемых технических спецификаций служат документы по безопасности на IP-уровне (IPsec). Кроме этого, анализируется защита на транспортном уровне (Transport Layer Security, TLS), а также на уровне приложений (спецификации GSS-API, Kerberos). Акцентируется внимание на административном и процедурном уровнях безопасности («Руководство по информационной безопасности предприятия», «Как выбирать поставщика интернет-услуг», «Как реагировать на нарушения информационной безопасности»).

В вопросах сетевой безопасности невозможно разобраться без освоения спецификаций X.800 «Архитектура безопасности для взаимодействия открытых систем», X.500 «Служба каталогов: обзор концепций, моделей и сервисов» и X.509 «Служба каталогов: каркасы сертификатов открытых ключей и атрибутов».

Это «стандартный минимум», которым должны активно владеть все действующие специалисты в области информационной безопасности.

По существу, проектирование системы безопасности подразумевает ответы на следующие вопросы:

- какую информацию защищать;
- какого рода атаки на безопасность системы могут быть предприняты;
- какие средства использовать для защиты информации каждого вида.

Поиск ответов на данные вопросы называется **формированием политики безопасности**, которая помимо чисто технических аспектов включает также и решение организационных проблем. На практике реализация политики безопасности состоит в присвоении субъектам и объектам идентификаторов, фиксации набора правил, позволяющих определить, имеет ли данный субъект авторизацию, достаточную для предоставления к данному объекту указанного типа доступа.

Формируя политику безопасности, необходимо учитывать несколько базовых принципов. Так, Зальтцер и Шредер на основе своего опыта работы сформулировали следующие рекомендации для проектирования системы безопасности операционных систем:

- Проектирование системы должно быть открытым. Нарушитель и так все знает (криптографические алгоритмы открыты).
- Не должно быть доступа по умолчанию. Ошибки с отклонением легитимного доступа будут обнаружены скорее, чем ошибки там, где разрешен неавторизованный доступ.
- Нужно тщательно проверять текущее авторство. Так, многие системы проверяют привилегии доступа при открытии файла и не делают этого после. В результате пользователь может открыть файл и держать его открытым в течение недели и иметь к нему доступ, хотя владелец уже сменил защиту.
- Давать каждому процессу минимум возможных привилегий.
- Защитные механизмы должны быть просты, постоянны и встроены в нижний слой системы, это не аддитивные добавки (известно много неудачных попыток «улучшения» защиты слабо приспособленной для этого ОС MS-DOS).
- Важна физиологическая приемлемость. Если пользователь видит, что защита требует слишком больших усилий, он от нее откажется.
- Ущерб от атаки и затраты на ее предотвращение должны быть сбалансированы.

Приведенные соображения показывают необходимость продумывания и встраивания защитных механизмов на самых ранних стадиях проектирования системы.

ГЛАВА 2. ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В Доктрине информационной безопасности Российской Федерации дается определение информационной безопасности. Под ***информационной безопасностью Российской Федерации*** понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В литературе отмечаются неоднозначные подходы к определению понятия информационной безопасности. Так, по мнению М.В. Арсентьева, информационная безопасность – снятие информационной неопределенности относительно объективно и субъективно существующих реальных и потенциальных угроз за счет контроля над мировым информационным пространством и наличие возможностей, условий и средств для отражения этих угроз, что в совокупности определяет уровень (степень) информационной безопасности каждого субъекта.

В.Ю. Статьев и В.А. Тиньков определяют информационную безопасность как защиту информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей его инфраструктуре.

А.Д. Урсул определяет информационную безопасность как состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям.

Введем ряд определений.

Информация – это сведения о лицах, предметах, фактах, событиях и процессах. Выделяется более двадцати видов информации по ее отраслевой принадлежности и востребованности в обществе (правовая, научная, финансовая, банковская, коммерческая, медицинская и т.д.). Нет объективной необходимости обеспечивать защиту всей информации, поэтому принято подразделять информацию на открытую и ограниченного доступа. Для эффективного решения задач защиты информации целесообразно в качестве объекта защиты выбирать информацию ограниченного доступа.

Информацию ограниченного доступа можно подразделить на конфиденциальную информацию и государственную тайну. **Конфиденциальная информация** – доверительная, не подлежащая огласке информация, доступ к которой ограничивается в соответствии с законодательством. Конфиденциальность информации определяет и доверяет посторонним лицам владелец этой информации.

К конфиденциальной информации относятся сведения, составляющие тайну частной жизни, профессиональную, служебную, коммерческую тайну.

Тайна частной жизни – это охраняемые законом конфиденциальные сведения, составляющие личную и семейную тайну лица, незаконное собирание или распространение которых причиняет вред правам и законным интересам этого лица и предоставляет ему право на защиту в соответствии с законодательством Российской Федерации.

Профессиональная тайна – это охраняемые законом конфиденциальные сведения, доверенные или ставшие известными лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которых может повлечь за собой вред правам и законным интересам другого лица, доверившего эти сведения, и привлечение к ответственности в соответствии с действующим законодательством.

Служебная тайна – это охраняемая законом конфиденциальная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости, а также ставшая известной в государственных органах и органах местного самоуправления только на законном основании и в силу исполнения их представителями служебных обязанностей, имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам.

Коммерческая тайна – это охраняемые законом конфиденциальные сведения в области производственно-хозяйственной, управленческой, финансовой деятельности организации, имеющие действительную или потенциальную ценность в силу неизвестности их третьим лицам, к ним нет свободного доступа на законном основании, обладатель сведений принимает меры к их конфиденциальности, незаконное получение, использование или разглашение которых создает угрозу причинения вреда владельцу этих сведений и предоставляет ему право на возмещение причиненных убытков или уголовно-правовую защиту в соответствии с законодательством Российской Федерации.

В отличие от конфиденциальной информации государственная тайна определяется государством через соответствующие государственные органы, получение и разглашение этой информации строго регламентировано нормативными актами, информация имеет гриф секретности. Содержание государственной тайны находит свое законодательное закрепление в Законе РФ «О государственной тайне». **Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

В этом же Законе РФ «О государственной тайне» прописаны такие принципы как законность, обоснованность и своевременность.

Принцип законности – в широком смысле принцип точного и неукоснительного исполнения всеми органами государства, должностными лицами и гражданами требований закона. Принцип законности служит базой для законотворчества в части правового обеспечения защиты информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, системы регулирования возникающих при этом отношений.

Принцип обоснованности. Защите подлежит прежде всего информация ограниченного доступа, т.е. информация, незаконное получение и распространение которой может причинить вред гражданину, обществу и государству. Необоснованная защита информации, прежде всего ограничение доступа к ней, посягает на конституционные права граждан на информацию, а в отдельных случаях препятствует развитию экономики, научно-технического прогресса, отношений в жизненно важных областях деятельности общества и государства. Принцип обоснованности заключается в установлении путем экспертной оценки целесообразности ограничения доступа к конкретной информации, выделении вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов личности, общества, государства, разработки адекватных мер противодействия внешним и внутренним угрозам информационной безопасности.

Принцип своевременности защиты информационной сферы позволяет реализовать процедуру предварительного ограничения доступа к защищаемой информации, осуществлять ее защиту и заключается в установлении ограничений на распространение этой информации с момента ее получения, разработки или заблаговременно. Значение этого принципа заключается прежде всего в том, что ограничение доступа к защищаемой информации, информационным системам, если не исключает полностью, то делает маловероятной возможность совершения преступных посягательств в данной сфере. На практике своевременность достигается путем разработки и четкого исполнения положений концепции и системы защиты объекта. Особое значение данного принципа проявляется в тех случаях, когда та или иная тема, проект, исследование находятся на стадии разработки, изучения, анализа, и при этом разработчики не уделяют должного внимания ограничению доступа к результатам работы, используют незащищенные каналы и средства связи, ЭВМ, привлекают к работе непроверенных специалистов и т.д. Как известно, новые разработки, направления исследований, технологии представляют повышенный интерес и являются приоритетным направлением в деятельности разведывательных органов иностранных государств, промышленного шпионажа, конкурентов, преступных элементов.

Ответственность за посягательство на указанные виды тайны предусмотрена в Уголовном кодексе РФ (ст. 137, 138, 142, 183, 275, 276, 283, 284). В УК РФ 1996 года включена новая, не известная прежнему уголовному законодательству России, глава 28 «Преступления в сфере компьютерной информации» (ст. 272, 273, 274). Указанные нормы уголовного закона входят в систему правовых мер, направленных на защиту информации, прав и законных интересов граждан, общества и государства в информационной сфере.

Право на информацию складывается из двух элементов – права на получение информации и права на ее распространение. Первое относится не к гражданским, частным, а к публичным правам. Право же на передачу информации имеет гражданско-правовое содержание, оно представляет собой исключительное право. Законом РФ «О правовой охране программ для ЭВМ и баз данных» регулируются отношения, возникающие в связи с правовой охраной и использованием программ для ЭВМ и баз данных. В статье 12 данного закона права на программу для ЭВМ или базу данных отнесены к исключительным правам владельца информации.

В содержание информационной безопасности входит информационная сфера. Определение информационной сферы сформулировано в ФЗ «Об участии в международном информационном обмене». **Информационная сфера** – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Как уже отмечалось, в основе понятия «информационная безопасность» лежит понятие «безопасность», нашедшее свое отражение в Законе РФ «О безопасности».

Безопасность – это состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз. К жизненно важным интересам закон относит совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Основные объекты безопасности: личность, ее права и свободы; общество, его материальные и духовные ценности; государство, его конституционный строй, суверенитет и территориальная целостность.

Таким образом, **информационная безопасность** – состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие.

Рассматривая это определение, необходимо отметить, что одним из важнейших аспектов информационной безопасности является определение и классификация возможных угроз безопасности.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Классификацию угроз можно представить в виде таблицы 1.

Таблица 1

Виды угроз

Угрозы		Внешние	Внутренние
Естественные	Преднамеренные	Развитие технологий	
	Непреднамеренные	Стихийные бедствия	1. Отказ техники 2. Технические сбои
Искусственные	Преднамеренные	1. Разработка ПО 2. Угроза целостности 3. Отказ в обслуживании	1. Угроза раскрытия (нарушение конфиденциальности) 2. Угроза целостности 3. Отказ в обслуживании
	Непреднамеренные	1. Политические факторы 2. Социальные факторы	Ошибки ПО

Среди возможных угроз можно выделить следующие:

- По источнику угрозы:
  - внешние – связанные со стихийными бедствиями, техногенными, политическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями;

- внутренние – связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения.

- По природе возникновения:
  - естественные (объективные) – вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;
  - искусственные (субъективные) – вызванные воздействием на информационную сферу человека.
    - непреднамеренные (случайные) угрозы – ошибки программного обеспечения, персонала, отказы вычислительной и коммуникационной техники и т.д.;
    - преднамеренные (умышленные) угрозы – неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д. Преднамеренные угрозы обусловлены действиями людей.
- По цели реализации:
  - нарушение конфиденциальности (угроза раскрытия) заключается в том, что информация становится известной пользователю, который не авторизован для этого. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен несанкционированный доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой раскрытия используется термин «утечка информации»;
  - нарушение целостности (угроза целостности) включает в себя любое несанкционированное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда нарушитель преднамеренно изменяет информацию, мы говорим, что целостность этой информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка. Санкционированными изменениями являются те, которые сделаны определенными лицами с обоснованной целью;
  - нарушение доступности (угроза отказа служб /отказа в обслуживании) возникает всякий раз, когда в результате преднамеренных действий, предпринятых другим пользователем, умышленно блокируется доступ к некоторому ресурсу вычислительной системы. Например, если один пользователь запрашивает доступ к службе, а другой предпринимает что-либо для недопущения этого доступа, мы говорим, что имеет место отказ службы. Бло-

кирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан. Наиболее частые примеры атак, связанных с отказом служб, включают в себя ресурсы общего пользования (принтеры или процессоры).

- По характеру воздействия:
  - активные;
  - пассивные.
- По объекту воздействия угрозы:
  - воздействующие на информационную среду в целом;
  - воздействующие на отдельные элементы информационной среды.

Основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами (действиями людей), так как они являются основной причиной и движущей силой преступлений и правонарушений. В то же время средства вычислительной техники (прежде всего ЭВМ), встраиваясь в систему отношений по поддержанию информационной безопасности, оказывают на них определенное воздействие. В отдельных случаях ЭВМ функционируют как источники повышенной опасности, и тогда нарушение установленных правил их эксплуатации может привести к нарушению информационной безопасности.

Отметим, что реализованная угроза называется **атакой.**

Следующим в нашем рассмотрении, но не менее важным, является понятие защищенности.

Под **защищенностью** понимается совокупность правовых, научно-технических, специальных, организационных мер, направленных на своевременное выявление, предупреждение и пресечение неправомерного получения и распространения защищаемой информации, осуществляемых органами законодательной, исполнительной и судебной власти, общественными и иными организациями и объединениями, гражданами, принимающими участие в обеспечении информационной безопасности в соответствии с законодательством, регламентирующим отношения в информационной сфере.

Правовые меры – деятельность законодательных органов по созданию правовой базы, обеспечивающей надлежащее формирование, распространение и использование информации; регулирующей деятельность субъектов, осуществляющих создание, преобразование и потребление информации; предусматривающей ответственность за нарушения в информационной сфере, меры обеспечения безопасности и правовой защиты информации, информационной инфраструктуры.

Научно-технические меры – деятельность субъектов, осуществляющих свою работу в информационной сфере, направленная на своевременное и активное использование достижений научно-технического прогресса в обеспечении информационной безопасности, а также участие в разработке новых технологий, программ, научно обоснованных способов защиты информации.

Специальные меры – деятельность государственных органов, уполномоченных осуществлять разведывательные, контрразведывательные, оперативно-розыскные мероприятия, направленные на упреждающее получение информации о планах, намерениях, устремлениях специальных служб, информационных и иных организаций, конкурентов и частных лиц, с использованием специальных технических средств, иных источников информации, указанных в Федеральном законе «Об оперативно-розыскной деятельности».

Организационные меры – деятельность субъектов по обеспечению физической, технической защиты информации, оборудования и носителей информации. Разработка и внедрение программ информационной безопасности и контроль за их выполнением, взаимодействие и обмен опытом защиты информации с правоохранительными, информационными органами. Работа по подбору, допуску и проверке персонала, подготовка и обучение сотрудников приемам работы с охраняемой информацией и ее носителями.

Отметим, что информационная безопасность в современных условиях приобретает все большую актуальность и значимость, является одним из приоритетных направлений обеспечения национальной безопасности России, а также международной безопасности.

ГЛАВА 3. ОЦЕНОЧНЫЕ СТАНДАРТЫ

Перед началом рассмотрения оценочных стандартов, необходимо упомянуть о том, что существуют и другие виды стандартов, такие как стандарты управления информационной безопасностью, стандарты безопасности информационных технологий и многие другие. В данном издании мы ограничимся исследованием именно оценочных стандартов.

3.1. Критерии оценки доверенных компьютерных систем Министерства обороны США

«Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaluation Criteria – TCSEC), получившие неформальное, но прочно закрепившееся название «Оранжевая книга», были разработаны и опубликованы Министерством обороны США в 1983 г. с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному программному и информационному обеспечению компьютерных систем, и выработки методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах, в основном военного назначения (полный перечень «Радужной серии» книг можно прочитать в Приложении 1).

В данном документе были впервые определены такие понятия, как «политика безопасности», «корректность» и др. Согласно «Оранжевой книге» безопасная компьютерная система – это система, поддерживающая управление доступом к обрабатываемой в ней информации так, что только соответствующим образом авторизованные пользователи или процессы (субъекты), действующие от их имени, получают возможность читать, записывать, создавать и удалять информацию. Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

Общая структура требований TCSEC

В «Оранжевой книге» предложены четыре категории требований: политика, подотчетность, гарантии и документирование, в рамках которых сформулированы базовые требования безопасности. Рассмотрим некоторые из них подробнее.

- **Политика**

Требование 1. Политика безопасности. Система должна поддерживать точно определенную политику безопасности (мандатную или дискреционную). Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом.

- **Подотчетность (аудит)**

Требование 2. Идентификация и аутентификация. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Требование 3. Регистрация и учет. Для определения степени ответственности пользователей за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе (т.е. должен существовать объект компьютерной системы, потоки от которого и к которому доступны только субъекту администрирования). Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

- **Гарантии (корректность)**

Требование 4. Контроль корректности функционирования средств защиты. Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты, Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 5. Непрерывность защиты. Все средства защиты (в том числе и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одной из ключевых аксиом, используемых для формального доказательства безопасности системы.

- **Документирование**

Требование 6. Документирование. В каждом классе необходимо выделять набор документов, который адресован разработчикам, пользователям и администраторам системы в соответствии с их полномочиями. Эта документация может состоять из:

- Руководства пользователя по особенностям безопасности.
- Руководства по безопасным средствам работы.
- Документации о тестировании.
- Проектной документации.

Классы защищенности компьютерных систем по TCSEC

«Оранжевая книга» предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Каждая группа включает один или несколько классов. Группы D и A содержат по одному классу (классы D и A соответственно), группа C-классы C1, C2, а группа B – классы B1, B2, B3, характеризующиеся различными наборами требований защищенности. Уровень защищенности возрастает от группы D к группе A, а внутри группы – с увеличением номера класса. Усиление требований осуществляется с постепенным смещением акцентов от положений, определяющих наличие в системе каких-то определенных механизмов защиты, к положениям обеспечивающих высокий уровень гарантий того, что система функционирует в соответствии требованиям политики безопасности. Например, по реализованным механизмам защиты классы B3 и A1 идентичны.

Все эти требования могут быть представлены в виде таблицы.

Таблица 2

Требования	C1	…	B3	A1
1. Требование 1	–	…	–	–
2. Требование 2	–	…	+	=
3. Требование 3	–	…	+	+
…	…	…	…	…

«–» – нет требований по этому классу

«+» – новые или дополнительные требования

«=» – требования совпадают с требованиями предыдущего класса

Перечень требований по Оранжевой книге в виде таблицы можно посмотреть в Приложении 2. Опишем смысл требований в словесной форме.

Так как центральным объектом исследования и оценки по TCSEC является доверительная база вычислений (Trusted Computing Base, TCB), необходимо коротко познакомиться с этим понятием.

Рассмотрим концепцию монитора ссылок, отражающую свойства механизмов безопасности. В данной концепции сеанс работы пользователя в компьютерной системе характеризуется инициированием процесса, который работает в интересах пользователя и выполняет последовательность операций доступа к объектам системы. Очевидно, что должна существовать некая процедура принятия решений о том, какой из запрашиваемых доступов разрешить, а какой нет. По-другому это можно представить как фильтр, через который должны пройти все запросы на доступ, созданные субъектами. Схема такого фильтра получила название **монитора ссылок**.

Основной характеристикой монитора ссылок является то, что он или разрешает запрос на доступ, или запрещает, возможно, уведомляя об этом субъекта. Монитор ссылок может быть описан в терминах функции с запросами на обслуживание, разрешениями доступа, другими компонентами состояния системы на входе (т.е. элементами области определения) и разрешениями или запретами на обслуживание на выходе (т.е. элементами области значения).

Таким образом, монитор ссылок должен удовлетворять трем требованиям:

- ни один запрос на доступ субъекта к объекту не должен проходить мимо монитора ссылок;
- целостность монитора ссылок должна строго контролироваться;
- представление монитора ссылок должно быть достаточно простым для доказательства корректности его работы.

Однако совершенно необязательно, чтобы безопасная система включала в свою архитектуру отдельный модуль (возможно, называемый модулем монитора ссылок), который бы обрабатывал запросы. Способ выполнения обработки запросов определяется проектировщиками и разработчиками системы.

Если в начале проектирования безопасных систем данный монитор реализовывался в виде отдельного модуля, встроенного в операционную систему, то в настоящее время существует тенденция к реализации данной концепции в форме совместно работающего программного и аппаратного обеспечения, называемого **ТСВ системы.**

Более того, на основании наличия компактного ядра безопасности ТСВ системы мы делаем заключение о свойствах безопасности системы в целом. Говоря о некотором свойстве системы, можно строить доказательство двумя способами: либо показать, что система ведет себя корректно всегда, либо показать, что система никогда не выполняет некорректных действий.

Основной причиной выделения программного обеспечения ТСВ системы является необходимость независимости свойства безопасности сис-

темы от программного обеспечения системы, не входящего в состав TCB. Программное обеспечение TCB системы обычно много компактнее и проще, чем программное обеспечение системы в целом.

Возвращаясь к TCSEC…

Группа D. Минимальная защита

Класс D. Минимальная защита. Класс D зарезервирован для тех систем, которые были представлены на сертификацию (оценку), но по какой-либо причине ее не прошли.

Группа C. Дискреционная защита

Группа C характеризуется наличием дискреционного управления доступом и аудитом действий субъектов.

Класс C1. Системы на основе дискреционного разграничения доступа. TCB систем, соответствующих этому классу защиты, удовлетворяет неким минимальным требованиям безопасного разделения пользователей и данных. Она определяет некоторые формы разграничения доступа на индивидуальной основе, т.е. пользователь должен иметь возможность защитить свою информацию от ее случайного чтения или уничтожения. Пользователи могут обрабатывать данные как по отдельности, так и от имени группы пользователей.

Политика безопасности. TCB должна определять и управлять доступом между поименованными объектами и субъектами (пользователями или их группами) в компьютерной системе. Механизм защиты должен позволять пользователям определять и контролировать распределение доступа к объектам по поименованным пользователям, их группам или по тем и другим.

Подотчетность. Пользователи должны идентифицировать себя перед TCB в случае выполнения ими любых действий, ею контролируемых, при этом должен быть использован хотя бы один из механизмов аутентификации (например, пароль). Данные аутентификации должны быть защищены от доступа неавторизованного пользователя.

Гарантии. TCB обеспечивает ее собственную работу и защиту от внешнего воздействия. Ресурсы системы, контролируемые TCB, являются подмножеством множества всех ресурсов. Тестирование TCB должно выполняться согласно документации для обеспечения гарантии того, что нет явных путей обхода системы защиты неавторизованным пользователем или иного расстройства системы защиты.

Документация должна включать:

- описание реализованных в TCB механизмов защиты, их взаимодействия и руководство пользователя по их использованию;
- руководство для администратора системы на гарантирование системы защиты;

- документацию по тестам, включающую описание того, как механизмы безопасности должны тестироваться и как интерпретировать результаты тестов;
- документацию по проекту, описывающую философию системы защиты и того, как эта философия реализована в ТСВ (если ТСВ состоит из нескольких модулей, то должен быть описан интерфейс между ними).

Класс С1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.

Класс С2. Системы, построенные на основе управляемого дискреционного разграничения доступа.

Системы, сертифицированные по данному классу, должны удовлетворять всем требованиям, изложенным в классе С1. Однако, системы класса С2 поддерживают более тонкую, чем в классе С1, политику дискреционного разграничения доступа, делающую пользователя индивидуально ответственным за свои действия после процедуры аутентификации в системе, а также аудит событий, связанных с безопасностью системы.

Политика безопасности. ТСВ должна осуществлять контроль за распространением прав доступа. Механизм дискреционного контроля доступа должен при каждом действии пользователя или его отсутствии обеспечивать защиту объектов от неавторизованного воздействия. При этом должен определяться доступ для каждого отдельного пользователя. Наделять пользователей правом доступа к объекту могут только авторизованные для этого пользователи. Никакая информация (в том числе шифрованная) о предшествующих действиях субъекта не может быть получена субъектом, получившим после первого доступ к системе. Реализация этого требования обеспечивает очищение ресурсов после освобождения их процессами системы.

Подотчетность. ТСВ должна обеспечивать индивидуальную ответственность пользователей за осуществляемые ими действия, обеспечивая возможность ассоциировать пользователя с любым событием аудита. При этом должен поддерживаться и защищаться журнал аудита, доступ к нему разрешаться только тем, кто специально для этого авторизован. Аудиту подлежит следующий стандартный набор событий, среди которых:

- идентификация и аутентификация пользователя;
- размещение объектов в адресном пространстве процессов пользователей (например, чтение информации из файлов);
- уничтожение объектов;
- действия, осуществляемые администраторами системы.

При этом запись журнала аудита должна снабжаться необходимым набором атрибутов:

- дата и время события;
- идентификатор пользователя, инициировавшего событие;
- тип события (например, вход в систему, получение доступа к файлу на чтение и т.д.);
- результат: успех или неуспех выполнения события.

Если требуется, надо указывать дополнительные сведения, например имя объекта, к которому происходит обращение. Для удобства изучения данных журнала аудита должны быть предусмотрены средства фильтрации записей по заданным признакам.

Гарантии. ТСВ должна изолировать подлежащие защите ресурсы так, чтобы выполнялись требования контроля доступа и аудита.

Тестирование должно включать поиск и просмотр очевидных брешей системы защиты, позволяющих нарушить изолированность ресурсов или допустить неавторизованный доступ к данным аутентификации или журнала аудита.

Документация должна дополнительно (по сравнению с классом С1) включать описание событий, заносимых в журнал аудита.

Группа В. Мандатное управление доступом

Основные требования этой группы – мандатное (полномочное) управление доступом с использованием меток безопасности, реализация некоторой формальной модели политики безопасности, а также наличие спецификаций на функции ТСВ. В системах этой группы постепенно к классу В3 должен быть реализован в полном объеме монитор ссылок, который должен контролировать все доступы субъектов к объектам системы.

Класс В1. Системы класса В1 должны удовлетворять требованиям класса С2. Кроме того, должны быть выполнены следующие дополнительные требования.

Политика безопасности. ТСВ должна обеспечивать пометку каждого субъекта и объекта системы. Метки секретности должны представлять уровень доступа субъекта и уровень секретности объекта, которым они соответствуют. Именно эти метки должны служить основой для принятия решения ТСВ при запросе субъекта доступа к объекту. При передаче информации по каналам ввода/вывода ТСВ должна снабжаться соответствующими метками секретности. ТСВ должна также соответствующе маркировать метками секретности весь читаемый вывод. Доступ на чтение от субъекта к объекту может быть разрешен, только если уровень допуска субъекта не ниже уровня секретности объекта, а неиерархические категории первого включают все неиерархические категории второго. Доступ на запись от субъекта к объекту, контролируемый ТСВ, может быть разрешен, только если уровень допуска субъекта не выше уровня секретности объекта, а все неиерархические категории первого входят в неиерархические категории второго.

Подотчетность. Аудиту подлежат любые изменения меток секретности читаемого вывода.

Гарантии. ТСВ должна обеспечивать изоляцию процессов системы, через выделение им соответствующего адресного пространства.

Целью тестирования является:

- Поиск всех каналов проникновения внешних субъектов с целью получения несанкционированного доступа к информации.
- Получение гарантии того, что никакой неавторизованный для этого специально пользователь не может ввести ТСВ в состояние, в котором она не способна отвечать на запросы других субъектов.

ТСВ должна быть построена на основе неформальной или формальной политики безопасности, которая должна поддерживаться на протяжении всего жизненного цикла системы.

Документация должна дополнительно включать:

- Для системного администратора описание функций, относящихся к безопасности ТСВ, а также описание путей и методов наилучшего использования защитных свойств системы; описания выполняемых процедур, предупреждений и привилегий, необходимых для контроля за безопасной работой системы.
- Описание формальной или неформальной политики безопасности, а также, как она реализована в системе.

Класс B2. Структурированная защита. Выполняются все требования класса защиты B1. Кроме того, в системах класса B2 ТСВ основывается на четко определенной и хорошо документированной формальной модели политики безопасности, требующей, чтобы мандатная и дискреционная системы разграничения доступа были распространены на все субъекты и объекты компьютерной системы. ТСВ должна быть четко структурирована на элементы, критичные с точки зрения безопасности и некритичные. Интерфейс ТСВ должен быть хорошо определен и ее проект и конечный результат должны быть подвергнуты полной проверке и тестированию. Механизм аудита должен быть усилен, введен контроль за конфигурацией системы. Система должна быть устойчива к внешнему проникновению.

Политика безопасности. ТСВ должна уведомлять каждого работающего в системе пользователя о любых изменениях его уровня секретности, а последний должен иметь возможность запрашивать у системы полную информацию о своей метке секретности. ТСВ должна поддерживать минимальные и максимальные метки секретности любого присоединенного физического устройства, которые должны определять непосредственное физическое окружение этого устройства.

Подотчетность. ТСВ должна обеспечить защищенный канал между собой и пользователем, осуществляющим вход в систему и аутентифика-

цию. Инициатором осуществления соединения через такой защищенный канал может выступать только пользователь.

Гарантии. ТСВ должна быть внутренне структурирована на хорошо определенные, в большой степени независимые модули. Все элементы ТСВ должны быть идентифицированы, а интерфейс между ними полностью определен. ТСВ должна обеспечить разделение функций оператора и администратора системы.

Разработчики системы должны полностью выявить скрытые каналы утечки и провести их инженерное обследование с целью измерения информационного потока для каждого канала. ТСВ должна быть рассмотрена по всем положениям, относящимся к ее устойчивости к проникновению. Тестирование ТСВ должно показать, что она функционирует согласно представленной в описании высокоуровневой спецификации.

Формальная модель политики безопасности должна поддерживаться ТСВ на протяжении всего жизненного цикла компьютерной системы. Должна существовать служба управления конфигурацией системы и должны быть предоставлены средства для создания новых версий ТСВ.

Документация должна дополнительно включать:

- для системного администратора – описание того, как безопасно создать новую ТСВ;
- результаты проверки эффективности использованных методов по сокращению мощности скрытых каналов утечки информации.

Проектная документация должна включать описание интерфейса между модулями ТСВ. Должно быть представлено описание высокоуровневых спецификаций и того, что они точно соответствуют интерфейсу ТСВ. Документация должна представлять результаты анализа скрытых каналов и затрат, необходимых для их сокращения.

Класс В3. Домены безопасности. В системах класса В3 ТСВ должна удовлетворять всем требованиям предыдущего класса и дополнительно требованиям монитора ссылок, который должен быть:

- защищен от несанкционированного изменения или порчи;
- обрабатывать все обращения;
- прост для анализа и тестирования.

ТСВ должна быть структурирована таким образом, чтобы исключить код, не имеющий отношения к безопасности системы.

Дополнительно должно быть обеспечено:

- поддержка администратора безопасности;
- расширение механизма аудита с целью сигнализации о любых с событиях, связанных с безопасностью;
- поддержка процедуры восстановления системы.

Политика безопасности. Не включает существенных дополнительных требований по сравнению с предыдущим классом защиты.

Подотчетность. Должно быть обеспечено создание защищенного канала для любого соединения пользователя с ТСВ (вход в систему, аутентификация, изменение секретных свойств объектов). Должен быть реализован механизм, осуществляющий анализ и накопление данных о событиях, имеющих отношения к безопасности и могущих послужить причиной нарушения политики безопасности. Этот механизм должен уведомлять администратора безопасности, когда превышается некоторый порог срабатывания. Если это событие или последовательность событий продолжается, то система должна предпринять наименее разрушительное действие для их блокирования.

Гарантии. ТСВ должна быть разработана и структурирована с использованием полного, концептуально – целостного механизма защиты с точно определенной семантикой. Сложность ТСВ должна быть минимизирована. Должен быть исключен код, не имеющий отношения к безопасности системы.

Функции, не связанные с управлением безопасностью и выполняемые пользователем, выступающим в роли администратора безопасности системы, должны быть ограничены набором только тех функций, которые делают более эффективным выполнение этой роли.

Должен быть обеспечен механизм восстановления при сбоях компьютерной системы без нарушения ее безопасности.

На этапе тестирования не должно быть найдено проектных брешей в системе защиты.

Должно быть четко показано, что высокоуровневая спецификация ТСВ соответствует модели политики безопасности.

Документация дополнительно должна включать:

- для системного администратора – описание процедур, которые могут дать гарантию, что система начала свою работу безопасно;
- неформальное доказательство того, что все элементы ТСВ соответствуют высокоуровневой спецификации.

Группа А. Верифицированная защита

Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (дискреционного и мандатного). Требуется, чтобы было формально показано соответствие архитектуры и реализации ТСВ требованиям безопасности.

Класс А1. Формальная верификация. Критерий защиты класса А1 не определяет дополнительные по сравнению с классом В3 требования к архитектуре или политике безопасности компьютерной системы. Дополнительным свойством систем, отнесенных к классу А1, является проведен-

ный анализ ТСВ на соответствие формальным высокоуровневым спецификациям и использование технологий проверки с целью получения высоких гарантий того, что ТСВ функционирует корректно.

Наиболее важные требования к классу А1 можно объединить в пять групп:

- Формальная модель политики безопасности должна быть четко определена и документирована, должно быть дано математическое доказательство того, что модель соответствует своим аксиомам и что их достаточно для поддержания заданной политики безопасности.
- Формальная высокоуровневая спецификация должна включать абстрактное определение выполняемых ТСВ функций и аппаратный и/или встроенный программный механизм для обеспечения разделения доменов.
- Формальная высокоуровневая спецификация ТСВ должна демонстрировать соответствие модели политики безопасности с использованием, где это возможно, формальной технологии (например, где имеются проверочные средства) и неформальной во всех остальных случаях.
- Должно быть неформально показано и обратное – соответствие элементов ТСВ формальной высокоуровневой спецификации. Формальная высокоуровневая спецификация должна представлять собой универсальный механизм защиты, реализующий политику безопасности. Элементы этого механизма должны быть отображены на элементы ТСВ.
- Должны быть использованы формальные технологии для выявления и анализа скрытых каналов. Неформальная технология может быть использована для анализа скрытых временных каналов. Существование оставшихся в системе скрытых каналов должно быть оправдано.

Более строгие требования предъявляются к управлению конфигурацией системы и конкретному месту дислокации (развертывания) системы.

Перечисленные требования не затрагивают группы Политика безопасности и Подотчетность и сконцентрированы в группе Гарантии с соответствующим описанием в группе Документация.

Интерпретация и развитие TCSEC

Опубликование TCSEC стало важным этапом как в постановке основных теоретических проблем компьютерной безопасности, так и в указании направления их решения. Тем не менее, в ходе применения ее основных положений выяснилось, что часть практически важных вопросов осталась за рамками данного стандарта. Кроме того, с течением времени ряд положений устарел и потребовал пересмотра.

Круг специфических вопросов по обеспечению безопасности компьютерных сетей и систем управления базами данных нашел отражение в отдельных документах, изданных Национальным центром компьютерной безопасности США в виде дополнений к «Оранжевой книге»:

- «Интерпретация TCSEC для компьютерных сетей».
- «Интерпретация TCSEC для систем управления базами данных».

Эти документы содержат трактовку основных положений «Оранжевой книги» применительно к соответствующим классам систем обработки информации.

Устаревание ряда положений TCSEC обусловлено прежде всего интенсивным развитием компьютерных технологий и переходом с вычислительных комплексов типа IBM-360 к рабочим станциям, высокопроизводительным персональным компьютерам и сетевой модели вычислений. Именно для того, чтобы исключить возникшую в связи с изменением аппаратной платформы некорректность некоторых положений «Оранжевой книги», адаптировать их к современным условиям и сделать адекватными нуждам разработчиков и пользователей программного обеспечения, и была проделана значительная работа по интерпретации и развитию положений этого стандарта. В результате возник целый ряд сопутствующих «Оранжевой книге» документов, многие из которых стали ее неотъемлемой частью. К наиболее часто упоминаемым относятся:

- «Руководство по произвольному управлению доступом в безопасных системах».
- «Руководство по управлению паролями».
- «Руководство по применению критериев безопасности компьютерных систем в специфических средах».
- «Руководство по аудиту в безопасных системах».
- «Руководство по управлению конфигурацией в безопасных системах».

Количество подобных вспомогательных документов, комментариев и интерпретаций значительно превысило объем первоначального документа, и в 1995 г. Национальным центром компьютерной безопасности США был опубликован документ под названием "Интерпретация критериев безопасности компьютерных систем", объединяющий все дополнения и разъяснения. При его подготовке состав подлежащих рассмотрению и толкованию вопросов обсуждался на специальных конференциях разработчиков и пользователей защищенных систем обработки информации. В результате открытого обсуждения была создана база данных, включающая все спорные вопросы, которые затем в полном объеме были проработаны специально созданной рабочей группой. В итоге появился документ, проинтегрировавший все изменения и дополнения к TCSEC, сделанные с момента ее опубликования, что привело к обновлению стандарта и позволило применять его в современных условиях.

Критерии TCSEC Министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на

проектировщиков, разработчиков, потребителей и специалистов по сертификации систем безопасности компьютерных систем. В свое время этот документ явился значительным шагом в области безопасности информационных технологий и послужил отправной точкой для многочисленных исследований и разработок. Основной отличительной чертой этого документа, как уже отмечалось, является его ориентация на системы военного применения, причем в основном на операционные системы. Это предопределило доминирование требований, направленных на обеспечение конфиденциальности обрабатываемой информации и исключение возможностей ее разглашения. Большое внимание уделено меткам конфиденциальности (грифам секретности) и правилам экспорта секретной информации.

Требования по гарантированию политики безопасности отражены достаточно поверхностно, соответствующий раздел по существу ограничивается требованиями контроля целостности средств защиты и поддержания их работоспособности, чего явно недостаточно.

3.2. Стандарт BS 7799-1

Первая часть стандарта, по-русски именуемая «Информационная технология. Практический кодекс по менеджменту информационной безопасности», содержит систематический, весьма полный, универсальный перечень регуляторов безопасности, полезный для организации практически любого размера, структуры и сферы деятельности. Она предназначена для использования в качестве справочного документа руководителями и рядовыми сотрудниками, отвечающими за планирование, реализацию и поддержание внутренней системы информационной безопасности.

Согласно стандарту, цель информационной безопасности – обеспечить бесперебойную работу организации, по возможности предотвратить и/или минимизировать ущерб от нарушений безопасности.

Управление информационной безопасностью позволяет коллективно использовать данные, одновременно обеспечивая их защиту и защиту вычислительных ресурсов.

Подчеркивается, что защитные меры оказываются значительно более дешевыми и эффективными, если они заложены в информационные системы и сервисы на стадиях задания требований и проектирования.

Следующие факторы выделены в качестве определяющих для успешной реализации системы информационной безопасности в организации:

- цели безопасности и ее обеспечение должны основываться на производственных задачах и требованиях. Функции управления безопасностью должно взять на себя руководство организации;

- необходима явная поддержка и приверженность к соблюдению режима безопасности со стороны высшего руководства;
- требуется хорошее понимание рисков (как угроз, так и уязвимостей), которым подвергаются активы организации, и адекватное представление о ценности этих активов;
- необходимо ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации.

Во второй части стандарта BS 7799-2:2002 «Управление информационной безопасностью. Практические правила» предметом рассмотрения, как следует из названия, является система управления информационной безопасностью.

Под системой управления информационной безопасностью (СУИБ) (Information Security Management System, ISMS) понимается часть общей системы управления, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. Эту систему составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

В основу процесса управления положена четырехфазная модель, включающая:

- планирование;
- реализацию;
- оценку;
- корректировку.

По-русски данную модель можно назвать ПРОК (в оригинале – Plan-Do-Check-Act, PDCA). Детальный анализ каждой из выделенных фаз и составляет основное содержание стандарта BS 7799-2:2002.

3.2.1. Регуляторы безопасности и реализуемые ими цели

3.2.1.1. Регуляторы общего характера

Мы приступаем к рассмотрению десяти групп регуляторов безопасности, выделенных в стандарте BS 7799.

К ***первой группе*** отнесено то, что связано с ***политикой безопасности***, а именно:

- документально оформленная политика;
- процесс ревизии политики.

Цель регуляторов этой группы – определить стратегию управления безопасностью и обеспечить ее поддержку.

Вторая группа регуляторов безопасности касается ***общеорганизационных аспектов***. По сравнению с первой она более многочисленна и наделена внутренней структурой. Ее ***первая подгруппа*** – инфраструктура

информационной безопасности – преследует цель управления безопасностью в организации и включает следующие регуляторы:

- создание сообщества по управлению информационной безопасностью;
- меры по координации действий в области информационной безопасности;
- распределение обязанностей в области информационной безопасности;
- утверждение руководством (административное и техническое) новых средств обработки информации;
- получение рекомендаций специалистов по информационной безопасности;
- сотрудничество с другими организациями (правоохранительными органами, поставщиками информационных услуг и т.д.);
- проведение независимого анализа информационной безопасности.

Регуляторы ***второй подгруппы*** **–** безопасность доступа сторонних организаций – предназначены для обеспечения безопасности вычислительных и информационных ресурсов, к которым имеют доступ сторонние организации. Этих регуляторов два:

- идентификация рисков, связанных с подключениями сторонних организаций, и реализация соответствующих защитных мер;
- выработка требований безопасности для включения в контракты со сторонними организациями.

Цель ***третьей подгруппы*** – обеспечение информационной безопасности при использовании услуг внешних организаций. Предлагается выработать требования безопасности для включения в контракты с поставщиками информационных услуг.

Очень важна ***третья группа*** регуляторов безопасности – ***классификация активов и управление ими***. Необходимым условием обеспечения надлежащей защиты активов является их идентификация и классификация. Должны быть выработаны критерии классификации, в соответствии с которыми активы тем или иным способом получают метки безопасности.

Регуляторы ***четвертой группы – безопасность персонала*** – охватывают все этапы работы персонала, и первый из них – документирование ролей и обязанностей в области информационной безопасности при определении требований ко всем должностям. В соответствии с этими требованиями должны производиться отбор новых сотрудников, заключаться соглашения о соблюдении конфиденциальности, оговариваться в контрактах другие условия.

Для сознательного поддержания режима информационной безопасности необходимо обучение всех пользователей, регулярное повышение их квалификации.

Наряду с превентивными, стандарт предусматривает и меры реагирования на инциденты в области безопасности, чтобы минимизировать ущерб и извлечь уроки на будущее. Предусмотрены уведомления (доклады) об инцидентах и замеченных уязвимостях, нештатной работе программного обеспечения. Следует разработать механизмы оценки ущерба от инцидентов и сбоев и дисциплинарного наказания провинившихся сотрудников.

Пятая группа регуляторов направлена на обеспечение ***физической безопасности и безопасности окружающей среды***. Она включает три подгруппы:

- организация защищенных областей;
- защита оборудования;
- меры общего характера.

Для организации защищенных областей требуется определить периметры физической безопасности, контролировать вход в защищенные области и работу в них, защитить производственные помещения (особенно имеющие специальные требования по безопасности) и места погрузо-/разгрузочных работ, которые, по возможности, надо изолировать от производственных помещений.

Чтобы предупредить утерю, повреждение или несанкционированную модификацию оборудования рекомендуется размещать его в защищенных областях, наладить бесперебойное электропитание, защитить кабельную разводку, организовать обслуживание оборудования, перемещать устройства (в том числе за пределы организации) только с разрешения руководства, удалять информацию перед выведением из эксплуатации или изменением характера использования оборудования.

К числу мер общего характера принадлежат политика чистого рабочего стола и чистого экрана, а также уничтожение активов – оборудования, программ и данных – только с разрешения руководства.

3.2.1.2. Регуляторы технического характера

Шестая группа – меры по безопасному ***администрированию систем и сетей*** разделены в стандарте BS 7799 на семь подгрупп:

- операционные процедуры и обязанности;
- планирование и приемка систем;
- защита от вредоносного программного обеспечения;
- повседневное обслуживание;
- администрирование сетей;
- безопасное управление носителями;
- обмен данными и программами с другими организациями.

1. Документирование операционных процедур и обязанностей преследует цель обеспечения корректного и надежного функционирования средств обработки информации. Требуется обязательно контролировать все изменения этих средств. Доклады о нарушениях безопасности должны быть своевременными и эффективными. Разделение обязанностей должно препятствовать злоупотреблению полномочиями. Средства разработки и тестирования необходимо отделить от производственных ресурсов. Для безопасного управления внешними ресурсами предлагается предварительно оценить риски и включить в контракты со сторонними организациями соответствующие положения.

2. Планирование и приемка систем призваны минимизировать риск их отказа. Для этого рекомендуется отслеживать и прогнозировать вычислительную нагрузку, требуемые ресурсы хранения и т.д. Следует разработать критерии приемки новых систем и версий, организовать их тестирование до введения в эксплуатацию.

3. Защита от вредоносного программного обеспечения должна включать как превентивные меры, так и меры обнаружения и ликвидации вредоносного ПО.

4. Под повседневным обслуживанием в стандарте имеется в виду резервное копирование, протоколирование действий операторов, регистрация, доведение до сведения руководства и ликвидация сбоев и отказов.

5. Вопросы администрирования сетей в стандарте, по сути, не раскрываются, лишь констатируется необходимость целого спектра регуляторов безопасности и документирования обязанностей и процедур.

6. Безопасное управление носителями подразумевает контроль за съемными носителями, безвредную утилизацию отслуживших свой срок носителей, документирование процедур обработки и хранения информации, защиту системной документации от несанкционированного доступа.

7. Более детально регламентирован обмен данными и программами с другими организациями. Предлагается заключать формальные и неформальные соглашения, защищать носители при транспортировке, обеспечивать безопасность электронной коммерции, электронной почты, офисных систем, систем общего доступа и других средств обмена. В качестве универсальных защитных средств рекомендуются документированная политика безопасности, соответствующие процедуры и регуляторы.

Седьмая группа – самая многочисленная – группа регуляторов, относящихся к ***управлению доступом к системам и сетям***. Она состоит из восьми подгрупп:

- производственные требования к управлению доступом;
- управление доступом пользователей;
- обязанности пользователей;

- управление доступом к сетям;
- управление доступом средствами операционных систем;
- управление доступом к приложениям;
- контроль за доступом и использованием систем;
- контроль мобильных пользователей и удаленного доступа.

1. Производственные требования к управлению доступом излагаются в документированной политике безопасности, которую необходимо проводить в жизнь.

2. Управление доступом пользователей должно обеспечить авторизацию, выделение и контроль прав в соответствии с политикой безопасности. Этой цели служат процедуры регистрации пользователей и ликвидации их системных счетов, управление привилегиями в соответствии с принципом их минимизации, управление паролями пользователей, а также дисциплина регулярной ревизии прав доступа.

3. Обязанности пользователей, согласно стандарту, сводятся к правильному выбору и применению паролей, а также к защите оборудования, остающегося без присмотра.

4. Управление доступом к сетям опирается на следующие регуляторы:

- политика использования сетевых услуг (прямой доступ к услугам должен предоставляться только по явному разрешению);
- задание маршрута от пользовательской системы до используемых систем (предоставление выделенных линий, недопущение неограниченного перемещения по сети и т.д.);
- аутентификация удаленных пользователей;
- аутентификация удаленных систем;
- контроль доступа (особенно удаленного) к диагностическим портам;
- сегментация сетей (выделение групп пользователей, информационных сервисов и систем);
- контроль сетевых подключений (например, контроль по предоставляемым услугам и/или времени доступа);
- управление маршрутизацией;
- защита сетевых сервисов (должны быть описаны атрибуты безопасности всех сетевых сервисов, используемых организацией).

5. Управление доступом средствами операционных систем направлено на защиту от несанкционированного доступа к компьютерным системам. Для этого предусматриваются:

- автоматическая идентификация терминалов;
- безопасные процедуры входа в систему (следует выдавать как можно меньше информации о системе, ограничить разрешаемое количество неудачных попыток, контролировать минимальную и максимальную продолжительность входа и т.п.);

- идентификация и аутентификация пользователей;
- управление паролями, контроль их качества;
- разграничение доступа к системным средствам;
- уведомление пользователей об опасных ситуациях;
- контроль времени простоя терминалов (с автоматическим отключением по истечении заданного периода);
- ограничение времени подключения к критичным приложениям.

6. Для управления доступом к приложениям предусматривается разграничение доступа к данным и прикладным функциям, а также изоляция критичных систем, помещение их в выделенное окружение.

7. Контроль за доступом и использованием систем преследует цель выявления действий, нарушающих политику безопасности. Для ее достижения следует протоколировать события, относящиеся к безопасности, отслеживать и регулярно анализировать использование средств обработки информации, синхронизировать компьютерные часы.

8. Контроль мобильных пользователей и удаленного доступа должен основываться на документированных положениях политики безопасности.

3.2.1.3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия

Восьмая группа – регуляторы группы ***«разработка и сопровождение информационных систем»*** охватывают весь жизненных цикл систем.

1. Первым шагом является анализ и задание требований безопасности. Основу анализа составляют:

- необходимость обеспечения конфиденциальности, целостности и доступности информационных активов;
- возможность использования различных регуляторов для предотвращения и выявления нарушений безопасности и для восстановления нормальной работы после отказа или нарушения безопасности.

В частности, следует рассмотреть необходимость:

- управления доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- протоколирования для повседневного контроля или специальных расследований;
- контроля и поддержания целостности данных на всех или избранных стадиях обработки;
- обеспечения конфиденциальности данных, возможно, с использованием криптографических средств;

- выполнения требований действующего законодательства, договорных требований и т.п.;
- резервного копирования производственных данных;
- восстановления систем после отказов (особенно для систем с повышенными требованиями к доступности);
- защиты систем от несанкционированных модификаций;
- безопасного управления системами и их использования сотрудниками, не являющимися специалистами.

2. Подгруппа регуляторов, обеспечивающих безопасность прикладных систем, включает:

- проверку входных данных;
- встроенные проверки корректности данных в процессе их обработки;
- аутентификацию сообщений как элемент контроля их целостности;
- проверку выходных данных.

3. Третью подгруппу рассматриваемой группы составляют криптографические регуляторы. Их основой служит документированная политика использования средств криптографии. Стандартом предусматривается применение шифрования, электронных цифровых подписей, средств управления ключами.

4. Четвертая подгруппа – защита системных файлов – предусматривает:

- управление программным обеспечением, находящимся в эксплуатации;
- защиту тестовых данных систем;
- управление доступом к библиотекам исходных текстов.

5. Регуляторы пятой подгруппы направлены на обеспечение безопасности процесса разработки и вспомогательных процессов. В нее входят следующие регуляторы:

- процедуры управления внесением изменений;
- анализ и тестирование систем после внесения изменений;
- ограничение на внесение изменений в программные пакеты;
- проверка наличия скрытых каналов и троянских программ;
- контроль за разработкой ПО, выполняемой внешними организациями.

Девятая группа – группа ***«управление бесперебойной работой организации»*** исключительно важна, но устроена существенно проще. Она включает пять регуляторов, направленных на предотвращение перерывов в деятельности предприятия и защиту критически важных бизнес-процессов от последствий крупных аварий и отказов:

- формирование процесса управления бесперебойной работой организации;
- выработка стратегии (на основе анализа рисков) обеспечения бесперебойной работы организации;
- документирование и реализация планов обеспечения бесперебойной работы организации;
- поддержание единого каркаса для планов обеспечения бесперебойной работы организации, чтобы гарантировать их согласованность и определить приоритетные направления тестирования и сопровождения;
- тестирование, сопровождение и регулярный пересмотр планов обеспечения бесперебойной работы организации на предмет их эффективности и соответствия текущему состоянию.

Процесс планирования бесперебойной работы организации должен включать в себя:

- идентификацию критически важных производственных процессов и их ранжирование по приоритетам;
- определение возможного воздействия аварий различных типов на производственную деятельность;
- определение и согласование всех обязанностей и планов действий в нештатных ситуациях;
- документирование согласованных процедур и процессов;
- подготовку персонала к выполнению согласованных процедур и процессов в нештатных ситуациях.

Для обеспечения бесперебойной работы организации необходимы процедуры трех типов:

- процедуры реагирования на нештатные ситуации;
- процедуры перехода на аварийный режим;
- процедуры возобновления нормальной работы.

Примерами изменений, которые могут потребовать обновления планов, являются:

- приобретение нового оборудования или модернизация систем;
- новая технология выявления и контроля проблем, например, обнаружения пожаров;
- кадровые или организационные изменения;
- смена подрядчиков или поставщиков;
- изменения, внесенные в производственные процессы;
- изменения, внесенные в пакеты прикладных программ;
- изменения в эксплуатационных процедурах;
- изменения в законодательстве.

Назначение регуляторов последней, ***десятой группы – контроль соответствия требованиям***. В ***первую подгруппу*** входят регуляторы соответствия действующему законодательству:

- идентификация применимых законов, нормативных актов и т.п.;
- обеспечение соблюдения законодательства по защите интеллектуальной собственности;
- защита деловой документации от утери, уничтожения или фальсификации;
- обеспечение защиты персональных данных;
- предотвращение незаконного использование средств обработки информации;
- обеспечение выполнения законов, касающихся криптографических средств;
- обеспечение сбора свидетельств на случай взаимодействия с правоохранительными органами.

Ко ***второй подгруппе*** отнесены регуляторы, контролирующие соответствие политике безопасности и техническим требованиям. Руководители всех уровней должны убедиться, что все защитные процедуры, входящие в их зону ответственности, выполняются должным образом и что все такие зоны регулярно анализируются на предмет соответствия политике и стандартам безопасности. Информационные системы нуждаются в регулярной проверке соответствия стандартам реализации защитных функций.

Регуляторы, относящиеся к аудиту информационных систем, объединены в ***третью подгруппу***. Их цель – максимизировать эффективность аудита и минимизировать помехи, создаваемые процессом аудита, равно как и вмешательство в этот процесс. Ход аудита должен тщательно планироваться, а используемый инструментарий – защищаться от несанкционированного доступа.

3.3. Стандарт BS 7799-2. Четырехфазная модель процесса управления информационной безопасностью

Мы приступаем к детальному рассмотрению четырехфазной модели процесса управления информационной безопасностью (планирование – реализация – оценка – корректировка, ПРОК), описанной в стандарте BS 7799-2:2002.

Процесс управления имеет циклический характер; на фазе ***первоначального планирования*** осуществляется вход в цикл. В качестве первого шага должна быть определена и документирована политика безопасности организации.

Затем определяется область действия системы управления информационной безопасностью. Она может охватывать всю организацию или ее части. Следует специфицировать зависимости, интерфейсы и предположения, связанные с границей между СУИБ и ее окружением; это особенно важно, если в область действия попадает лишь часть организации. Большую область целесообразно поделить на подобласти управления.

Результат анализа рисков – выбор регуляторов безопасности. План должен включать график и приоритеты, детальный рабочий план и распределение обязанностей по реализации этих регуляторов.

На второй фазе – ***фазе реализации*** – руководством организации выделяются необходимые ресурсы (финансовые, материальные, людские, временные), выполняется реализация и внедрение выбранных регуляторов, сотрудникам объясняют важность проблем информационной безопасности, проводятся курсы обучения и повышения квалификации. Основная цель этой фазы – ввести риски в рамки, определенные планом.

Оценка (третья фаза) может выполняться в нескольких формах:

- регулярные (рутинные) проверки;
- проверки, вызванные появлением проблем;
- изучение опыта (положительного и отрицательного) других организаций;
- внутренний аудит СУИБ;
- инспекции, проводимые по инициативе руководства;
- анализ тенденций.

Аудит должен выполняться регулярно, не реже одного раза в год. В процессе аудита следует убедиться в следующем:

- политика безопасности соответствует производственным требованиям;
- результаты анализа рисков остаются в силе;
- документированные процедуры выполняются и достигают поставленных целей;
- технические регуляторы безопасности (например, межсетевые экраны или средства ограничения физического доступа) расположены должным образом, правильно сконфигурированы и работают в штатном режиме;
- действия, намеченные по результатам предыдущих проверок, выполнены.

Даже если недопустимых отклонений не выявлено и уровень безопасности признан удовлетворительным, целесообразно зафиксировать изменения в технологии и производственных требованиях, появление новых угроз и уязвимостей, чтобы предвидеть будущие изменения в системе управления.

- Назначение фазы оценки – проанализировать, насколько эффективно работают регуляторы и система управления информационной безопасностью в целом. Кроме того, следует принять во внимание изменения, произошедшие в организации и ее окружении, способные повлиять на результаты анализа рисков. При необходимости намечаются корректирующие действия, предпринимаемые в четвертой фазе.

Систему управления информационной безопасностью надо постоянно совершенствовать, чтобы она оставалась эффективной. Эту цель преследует четвертая фаза рассматриваемого в стандарте цикла – ***корректировка***. Она может потребовать как относительно незначительных действий, так и возврата к фазам планирования (например, если появились новые угрозы) или реализации (если следует осуществить намеченное ранее).

Коррекция должна производиться, только если выполнено по крайней мере одно из двух условий:

- выявлены внутренние противоречия в документации СУИБ;
- риски вышли за допустимые границы.

При корректировке прежде всего следует устранить несоответствия следующих видов:

- отсутствие или невозможность реализации некоторых требований СУИБ;
- неспособность СУИБ обеспечить проведение в жизнь политики безопасности или обслуживать производственные цели организации.

3.4. Сведения о других международных стандартах

Как уже отмечалось, после «Оранжевой книги» была выпущена целая **«Радужная серия»** (см. *Приложение 1*). С концептуальной точки зрения, наиболее значимый документ в ней – **"Интерпретация «Оранжевой книги» для сетевых конфигураций"** (Trusted Network Interpretation). Он состоит из двух частей. Первая содержит собственно интерпретацию, во второй описываются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Важнейшее понятие, введенное в первой части, – сетевая доверенная вычислительная база. Другой принципиальный аспект – учет динамичности сетевых конфигураций. Среди защитных механизмов выделена криптография, помогающая поддерживать как конфиденциальность, так и целостность.

Новым для своего времени стал системный подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.

Следующий документ это **«Гармонизированные критерии Европейских стран» (ITSEC).** Нужно отметить, что в них отсутствуют априорные требования к условиям, в которых должна работать информационная система. Предполагается, что сначала формулируется цель оценки, затем орган сертификации определяет, насколько полно она достигается, т.е. в какой мере корректны и эффективны архитектура и реализация механизмов безопасности в конкретной ситуации. Чтобы облегчить формулировку цели оценки, стандарт содержит описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

В «Гармонизированных критериях» подчеркивается различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие – объект оценки.

Функциональность (F) и эффективность (E) оцениваются раздельно. Соответствие классов безопасности ITSEC и TCSEC показано в таблице 3.

Таблица 3

ITSEC	E0	F-C1, E1	F-C2, E2	F-B1, E3	F-B2, E4	F-B3, E5	F-B3, E6
TCSEC	D	C1	C2	B1	B2	B3	A1

«Гармонизированные критерии Европейских стран» стали весьма передовым документом для своего времени, они подготовили появление международного стандарта ***ISO/IEC 15408:1999 «Критерии оценки безопасности информационных технологий» (Common Criteria for Information Technology Security Evaluation (CCITSE)),*** для удобства, в литературе сокращают до ***Общие критерии (Common Criteria).***

Многие правительственные организации и частные компании приобретают только те системы, которые удовлетворяют определенному набору требований. Группа государств, объединив свои усилия в рамках Международной организации по стандартизации (ISO), разработала новый стандарт безопасности ISO 15408, призванный отразить возросший уровень сложности технологий и растущую потребность в международной стандартизации. Страны, ратифицировавшие Common Criteria, рассчитывают, что его использование приведет к повышению надежности продуктов, в которых применяются технологии защиты данных; он поможет потребителям информационных технологий лучше ориентироваться при выборе программного обеспечения, а пользователям приобрести уверенность в безопасности ИТ-продуктов.

В соответствии с требованиями Общих критериев, продукты определенного класса (например, операционные системы) оцениваются на соот-

ветствие ряду функциональных критериев и критериев надежности – так называемых ***профилей защиты*** (Protection Profiles). Существуют различные определения профилей защиты в отношении операционных систем, брандмауэров, смарт-карт и прочих продуктов, которые должны соответствовать определенным требованиям в области безопасности.

На сегодняшний день Общие критерии – самый полный и современный оценочный стандарт, он не содержит предопределенных классов безопасности. Такие классы можно строить, опираясь на заданные требования. Подчеркнем, что безопасность в Общих критериях рассматривается не статично, а в соответствии с жизненным циклом объекта оценки. Кроме того, последний предстает в контексте среды безопасности, характеризующейся определенными условиями и угрозами.

Общие критерии содержат два основных вида ***требований безопасности*** **(**Security Assurance Requirements, SARs):

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

Требования безопасности формулируются, и их выполнение проверяется для определенного объекта оценки – аппаратно-программного продукта или информационной системы.

Задание по безопасности (Security Target, ST**)** содержит совокупность требований к конкретной разработке, их выполнение позволит решить поставленные задачи по обеспечению безопасности.

Стандарт Общие критерии также устанавливает ряд ***оценочных уровней доверия*** (Evaluation Assurance Levels, EAL), используемых при оценке продуктов. Сертификация на более высокий уровень EAL предполагает более высокую степень уверенности в том, что система защиты продукта работает правильно и эффективно. Сертификаты, полученные продуктами для уровней EAL1-EAL4, признаются всеми странами, поддерживающими стандарт Common Criteria. Сертификация для высших уровней EAL5-EAL7 проводится отдельно в каждой стране. При этом профили защиты могут разрабатываться независимо каждой страной, в том числе и с учетом национальных особенностей защиты государственных секретов. Поэтому EAL4 является высшим уровнем, которого могут достигнуть продукты, не создававшиеся изначально с учетом соответствия требованиям EAL5-EAL7.

Признание соответствия продукта по стандарту Общих критериев происходит лишь после прохождения им весьма строгой и длительной

процедуры проверки. Это не означает, что все продукты, сертифицированные на соответствие стандарту Общие критерии, не имеют уязвимых мест в системе безопасности (подобных продуктов просто не существует), однако наличие такой сертификации позволяет с большей степенью уверенности утверждать, что продукт обладает надежной защитой.

Ознакомление с ***Федеральным стандартом США FIPS 140-2 "Требования безопасности для криптографических модулей" (Security Requirements for Cryptographic Modules)*** позволит вникнуть в проблематику, связанную с вопросами криптографии. Данный стандарт описывает внешний интерфейс криптографического модуля, общие требования к подобным модулям и их окружению. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них. Алгоритмическую сторону криптографии можно рассмотреть, изучив технические спецификации.

3.5. Сведения о стандартах на территории России

Руководящие документы (РД) Гостехкомиссии России начали появляться несколько позже мировых стандартов, и уже после опубликования «Гармонизированных критериев», подтверждая разницу между автоматизированными системами (АС) и продуктами (средствами вычислительной техники, СВТ), но в общем и целом они долгое время следовали в фарватере «Оранжевой книги».

Первое примечательное отклонение от этого курса произошло в 1997 году, когда был принят РД по отдельному сервису безопасности – межсетевым экранам (МЭ). Его основная идея – классифицировать МЭ на основании осуществляющих фильтрацию потоков данных уровней эталонной семиуровневой модели – получила международное признание и продолжает оставаться актуальной.

В 2002 году Гостехкомиссия России приняла в качестве РД русский перевод международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий", что послужило толчком для кардинальной и весьма своевременной со всех точек зрения переориентации. Переход на рельсы Общих критериев является непростой, но главное разрешимой задачей.

Стандарт ISO 15408 является государственным стандартом России. С 1 января 2004 года введены в действие следующие государственные стандарты (названия см. в таблице 2):

- ГОСТ Р ИСО/МЭК 15408-1-2002;
- ГОСТ Р ИСО/МЭК 15408-2-2002;
- ГОСТ Р ИСО/МЭК 15408-3-2002.

Принятие государственного стандарта, соответствующего Общим критериям, пока не означает взаимного признания сертификатов. Сделав следующий шаг на этом пути и присоединившись к странам, взаимно признающим полученные в них сертификаты, Россия получит существенный импульс в развитии информационных технологий в стране, поскольку:

- потребители смогут сократить свои затраты на сертификацию продуктов;
- сертифицирующие органы смогут привлечь дополнительный поток заказов на сертификацию из-за рубежа;
- производители российских высокотехнологичных продуктов смогут получить международные сертификаты в России, что позволит им выйти на закрытые ранее зарубежные рынки;
- Россия сохранит свои национальные требования при сертификации продуктов на высшие уровни защиты информации, включая защиту государственной тайны.

Чтобы разобраться в вопросах применения российских стандартов, необходимо представить себе административно-правовую структуру информационной безопасности и понять, какое место они в ней занимают. Эта структура показана на рис. 4, откуда видно, что стандарты относятся к специальным нормативным документам по технической защите информации и находятся в определенном логическом соответствии с правовыми и организационно-распорядительными документами. Наименования стандартов приведены в таблице 4.

Рассмотрим более подробно содержание стандартов ИСО/МЭК 15408.

В части 1 (ГОСТ Р ИСО/МЭК 15408-1-2002. Введение и общая модель) устанавливается общий подход к формированию требований оценки безопасности, на их основе разрабатываются профили защиты и задания по безопасности, представленные в классах данного стандарта:

- Оценка профиля защиты APE.
- Оценка задания по безопасности ASE.
- Поддержка доверия AMA .

Часть 2 (ГОСТ Р ИСО/МЭК 15408-2-2002. Функциональные требования безопасности) представляет собой обширную библиотеку функциональных требований к безопасности, описывающую 11 классов, 66 семейств, 135 компонентов и содержащую сведения о том, какие цели безопасности могут быть достигнуты и каким образом.

Часть 3 (ГОСТ Р ИСО/МЭК 15408-3-2002. Требования доверия к безопасности) включает в себя оценочные уровни доверия (ОУД), образующие своего рода шкалу для измерения уровня доверия к объекту оцен-

ки. Под доверием понимается «...основа для уверенности в том, что продукт или система информационных технологий отвечает целям безопасности».

Интерпретируя содержимое этих частей стандарта, можно сказать: каркас безопасности, заложенный частью 1, заполняется содержимым из классов, семейств и компонентов в части 2, а часть 3 определяет, как оценить прочность всего «строения».

Рис. 4. Административно-правовая структура ИБ в России

ГЛАВА 4. ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ

Среди технических спецификаций на первое место, безусловно, следует поставить ***документ X.800 «Архитектура безопасности для взаимодействия открытых систем».*** Здесь выделены важнейшие сетевые сервисы безопасности:

- аутентификация;
- управление доступом;
- обеспечение конфиденциальности и/или целостности данных;
- невозможность отказаться от совершенных действий.

Для реализации сервисов предусмотрены следующие сетевые механизмы безопасности и их комбинации:

- шифрование;
- электронная цифровая подпись (ЭЦП);
- управление доступом;
- контроль целостности данных;
- аутентификация;
- дополнение трафика;
- управление маршрутизацией;
- нотаризация.

Выбраны уровни эталонной семиуровневой модели, на которых могут быть реализованы сервисы и механизмы безопасности. Наконец, детально рассмотрены вопросы администрирования средств безопасности для распределенных конфигураций.

Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)» относится к более частной, но весьма важной и актуальной проблеме – аутентификации в разнородной распределенной среде с поддержкой концепции единого входа в сеть. Сервер аутентификации Kerberos представляет собой доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. О весомости данной спецификации свидетельствует тот факт, что клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Спецификация «Обобщенный прикладной программный интерфейс службы безопасности» (Generic Security Service Application Program Interface, GSS-API) описывает интерфейс безопасности, предназначенный для защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Он создает условия для взаимной аутентификации общающихся партнеров, контролирует целост-

ность пересылаемых сообщений и служит гарантией их конфиденциальности. Пользователями интерфейса безопасности GSS-API являются коммуникационные протоколы (обычно прикладного уровня) или другие программные системы, самостоятельно выполняющие пересылку данных.

Таблица 4

Российские стандарты, регулирующие ИБ

№ п/п	Стандарт	Наименование
1	ГОСТ Р ИСО/МЭК 15408-1-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России
2	ГОСТ Р ИСО/МЭК 15408-2-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России
3	ГОСТ Р ИСО/МЭК 15408-3-2002	Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России
4	ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России
5	ГОСТ Р 50922-96	Защита информации. Основные термины и определения. Госстандарт России
6	ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России
7	ГОСТ Р 51275-99	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России
8	ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России
9	ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России

Технические спецификации IPsec [IPsec] имеют, без преувеличения, фундаментальное значение, описывая полный набор средств обеспечения конфиденциальности и целостности на сетевом уровне. Для доминирующего в настоящее время протокола IP версии 4 они носят факультативный характер; в версии IPv6 их реализация обязательна. На основе IPsec строятся защитные механизмы протоколов более высокого уровня, вплоть до прикладного, а также законченные средства безопасности, в том числе виртуальные частные сети. Разумеется, IPsec существенным образом опирается на криптографические механизмы и ключевую инфраструктуру.

Точно так же характеризуются и ***средства безопасности транспортного уровня (Transport Layer Security, TLS)***. Спецификация TLS развивает и уточняет популярный протокол Secure Socket Layer (SSL), используемый в большом числе программных продуктов самого разного назначения.

Также важны рекомендации ***X.500 «Служба каталогов: обзор концепций, моделей и сервисов» (The Directory: Overview of concepts, models and services) и X.509 «Служба каталогов: каркасы сертификатов открытых ключей и атрибутов» (The Directory: Public-key and attribute certificate frameworks)***. В рекомендациях X.509 описан формат сертификатов открытых ключей и атрибутов – базовых элементов инфраструктур открытых ключей и управления привилегиями.

Как известно, обеспечение информационной безопасности – проблема комплексная, требующая согласованного принятия мер на законодательном, административном, процедурном и программно-техническом уровнях. При разработке и реализации базового документа административного уровня – политики безопасности организации – отличным подспорьем может стать рекомендация ***Internet-сообщества «Руководство по информационной безопасности предприятия» (Site Security Handbook).*** В нем освещаются практические аспекты формирования политики и процедур безопасности, поясняются основные понятия административного и процедурного уровней, содержится мотивировка рекомендуемых действий, затрагиваются темы анализа рисков, реакции на нарушения ИБ и действий после ликвидации нарушения. Более подробно последние вопросы рассмотрены в ***рекомендации «Как реагировать на нарушения информационной безопасности» (Expectations for Computer Security Incident Response).*** В этом документе можно найти и ссылки на полезные информационные ресурсы, и практические советы процедурного уровня.

При развитии и реорганизации корпоративных информационных систем, несомненно, окажется ***полезной рекомендация «Как выбирать поставщика Internet-услуг» (Site Security Handbook Addendum for ISPs).*** В первую очередь ее положений необходимо придерживаться в ходе формирования организационной и архитектурной безопасности, на которой базируются прочие меры процедурного и программно-технического уровней.

ГЛАВА 5. ПОЛИТИКА БЕЗОПАСНОСТИ

Для того чтобы определить, от каких именно угроз и каким образом защищает информацию автоматизированная вычислительная система (АВС), необходимо сформулировать ее политику безопасности, т.е. создать документ, описывающий все возможные взаимодействия. Политика безопасности подразумевает наличие множества условий, при которых пользователи системы могут получить доступ к информации и ресурсам. С одной стороны, политика безопасности предписывает пользователям, как правильно эксплуатировать систему, с другой – политика безопасности определяет множество механизмов безопасности, которые должны существовать в конкретной реализации АВС. Политика безопасности АВС может быть выражена формальным и неформальным образом.

5.1. Формальная и неформальная политики безопасности

5.1.1. Неформальная политика безопасности

Для неформальной политики безопасности широкое распространение получило описание правил доступа субъектов к объектам в виде таблицы, наглядно представляющей правила доступа. Обычно такая таблица подразумевает, что субъекты, объекты и типы доступа определены. Это позволяет составить таблицу, содержащую колонку типов доступа и колонку соответствующего отношения, которое должно соблюдаться между субъектом и объектом для данного типа доступа (см. таблицу 5).

Таблица 5

Выражение неформальной политики безопасности

Тип доступа	Отношение (субъект, объект)
Чтение	Больше
Выполнение	Больше
Запись	Равно

Исследуя таблицу, можно сделать заключение, что уровни безопасности субъектов должны быть выше уровней безопасности объектов для того, чтобы субъектам системы были разрешены операции чтения и выполнения. Подобным образом можно сделать заключение о том, что уровни субъекта и объекта должны быть одинаковыми для получения разрешения на выполнение операции записи.

Преимуществом такого способа представления политики безопасности является то, что она гораздо легче для понимания пользователями, чем формальное описание, так как для ее понимания не требуется специальных математических знаний, при этом снижается вероятность атак на вычислительную систему по причине ее некорректной эксплуатации. Основным недостатком неформального описания политики безопасности системы является то, что при такой форме представления правил доступа в системе гораздо легче допустить логические ошибки при проектировании системы и ее эксплуатации, особенно для нетривиальных систем, подобных многопользовательским операционным системам.

В результате разработчики безопасных АВС начали использовать формальные средства для описания политик безопасности. Преимуществом формального описания является отсутствие противоречий в политике безопасности и возможность теоретического доказательства безопасности системы при соблюдении всех условий политики безопасности. Требование формального описания систем характерно для систем, область применения которых критична. В частности, можно отметить тот факт, что для защищенных вычислительных систем высокой степени надежности необходимы формальное представление и формальный анализ системы.

5.1.2. Формальная политика безопасности

Для лучшего понимания принципов, используемых при создании формальных политик безопасности, рассмотрим основные математические методы, применяемые при формальном анализе вообще и формальном описании политик безопасности АВС в частности.

При анализе функционирования систем (не обязательно АВС), область применения которых является критичной, желательно рассмотреть все возможные поведения системы – ее реакции на все возможные входные данные.

Хотя количество всех возможных реакций системы слишком велико для исследования, существует два метода, позволяющих уменьшить количество реакций, которые необходимо рассмотреть за счет группировки «схожих» реакций системы. Получается, что для рассмотрения всех возможных реакций системы необходимо рассмотреть лишь небольшое количество входных воздействий.

К сожалению, эти методы анализа безопасности систем пригодны в основном для систем, основывающихся на механических, электрических и других компонентах, то есть компонентах, основанных на физических принципах действия. В системах, основанных на физических принципах, отношения между входными и выходными данными являются «непрерывными», то есть незначительные изменения во входных данных влекут

незначительные изменения в выходных данных. Это позволяет проанализировать (протестировать) поведение системы, основанной на физических законах конечным количеством тестов.

Первый метод заключается в доказательстве того, что система всегда «работает корректно», второй заключается в демонстрации того, что система никогда не выполняет неверных действий.

При использовании первого метода используется комбинация анализа и эмпирического тестирования для определения таких реакций системы, которые могут привести к серьезным сбоям – например, функционирование системы при граничных условиях или при условиях, не оговоренных в качестве возможных для компонентов системы. В качестве примера можно привести требование описания поведения системы в ответ на входное воздействие «выключение питания».

Второй метод выдвигает гипотезу о том, что система делает что-то некорректное, и на этой основе ведется анализ реакций системы с выявлением состояний, в которых возможно проявление данной некорректности. Доказательство корректности работы системы сводится к демонстрации того, что данные состояния недостижимы, то есть к доказательству от противного.

Подводя итог для этих методов непосредственного тестирования, нужно отметить, что они способны детектировать только примитивные ошибки в программном обеспечении вследствие сложности современных программных систем и вытекающего из этого многообразия реакций системы на входной поток данных, носят вероятностный характер.

Как уже отмечалось, сложность АВС определяется большим количеством дискретных решений, принимаемых системой при исполнении программ. Таким образом, при определении взаимоотношений между входом и выходом системы (входным и выходным потоками данных), в случае анализа АВС, реакцию системы на входное воздействие нельзя рассматривать как непрерывную функцию, так как она является дискретной: небольшие изменения во входных данных системы могут радикально изменить поведение всей системы в целом. Это является главным отличием современных АВС от систем, основанных на физических процессах.

Отклонение от непрерывности ведет к катастрофическому росту количества возможных реакций системы на изменения во входных данных. Поэтому в случае с АВС в области программного обеспечения используются понятия дискретной математики, такие как «множества», «графы», «частичный порядок», «машина конечных состояний» и т.д. «Вычисления» при описании данных систем базируются на методах формальной логики, а не на численном анализе. Это происходит потому, что результаты, интересующие при анализе системы, являются логическими свойствами. Математическая логика обеспечивает методы доказательства свойств

больших или бесконечных множеств связанных сущностей на конечный манер на основе методов, сходных с методом математической индукции. Другими словами под формальными методами при анализе АВС подразумевается применение математических моделей – моделей безопасности.

Выделяя ядро ТСВ системы и рассматривая его свойства (в частности свойство безопасности) при создании модели безопасности и учитывая его компактность, можно делать выводы о свойствах безопасности системы в целом. При этом можно строить доказательство двумя способами: либо показать, что система ведет себя корректно всегда, либо показать, что система никогда не выполняет некорректных действий (т.е. от методов исследования АВС перейти к методам исследования для физических систем).

Для автоматизации процесса доказательства свойств системы используются «доказатели теорем» – программное обеспечение, проводящее формальную дедукцию на основе комбинации эвристик и непосредственного поиска, с возможностью вмешиваться в процесс выбора последовательности шагов логического вывода о свойствах системы, при этом проверяющие корректность каждого шага.

Основным недостатком, присущим всем методам моделирования, является тот факт, что мы имеем дело не с самой системой, а с ее моделью. При этом модель может не отражать реальность или отражать ее некорректно, если учитывает не все факторы, оказывающие влияние на реальную систему, или излишне подробно описывает систему и ведет к неэффективности применения данного метода.

Таким образом, возникает задача корректного выбора уровня абстракции в описании модели безопасности. Под уровнем абстракции понимается множество требований к реальной системе, которые должны найти свое отражение в модели, для корректного отображения моделируемой системы.

К модели безопасности должны предъявляться требования, общие для всех моделей:

- адекватность;
- способность к предсказанию;
- общность.

ГЛАВА 6. МОДЕЛИ БЕЗОПАСНОСТИ

6.1. Основные понятия

Говоря о моделях безопасности системы, помним о том, что механизм, свойства которого должны уточняться в результате моделирования (монитор ссылок), отражает свойства механизмов безопасности всей системы. Если в начале проектирования безопасных систем данный монитор реализовывался в виде отдельного модуля, встроенного в операционную систему, то в настоящее время существует тенденция к реализации данной концепции в форме совместно работающего программного и аппаратного обеспечения, называемого TCB системы.

Немного о математической логике, которую будем использовать при рассмотрении моделей.

В логике существует понятие предикатов первого и второго порядка.

Логика первого порядка (исчисление предикатов) – формальное исчисление, допускающее высказывания относительно переменных, фиксированных функций, и предикатов. Расширяет логику высказываний. В свою очередь является частным случаем логики высшего порядка.

Логика высказываний (или пропозициональная логика) – это формальная теория, основным объектом которой служит понятие логического высказывания. С точки зрения выразительности, её можно охарактеризовать как классическую логику нулевого порядка. Логика высказываний является простейшей логикой, максимально близкой к человеческой логике неформальных рассуждений и известна ещё со времён античности.

Базовыми понятиями логики высказываний являются пропозициональная переменная – переменная, значением которой может быть логическое высказывание, – и (пропозициональная) формула, определяемая индуктивно следующим образом:

- Если P – пропозициональная переменная, то P – формула.
- Если A – формула, то $\neg A$ — формула.
- Если A и B – формулы, то $(A \to B)$— формула.
- Других соглашений нет.

Знаки $\neg, \wedge, \vee$ и $\to$ (отрицание, конъюнкция, дизъюнкция и импликация) называются пропозициональными связками. Подформулой называется часть формулы, сама являющаяся формулой. Собственной подформулой называется подформула, не совпадающая со всей формулой.

Язык логики первого порядка строится на основе сигнатуры, состоящей из множества функциональных символов $\mathcal{F}$и множества предикатных символов $\mathcal{P}$. С каждым функциональным и предикатным символом связана арность, то есть число возможных аргументов (А́рность пре-

диката, операции или функции в математике – количество их аргументов, или операндов. Слово образовалось из названий предикатов небольшой арности (унарный – один аргумент, бинарный – два, тернарный – три)). Кроме того используются следующие дополнительные символы

- Символы переменных (обычно x,y,z,x1,y1,z1,x2,y2,z2, и т. д.),
- Пропозициональные связки: $\vee, \wedge, \neg, \rightarrow$,
- Кванторы: всеобщности $\forall$и существования $\exists$,
- Служебные символы: скобки и запятая.

Перечисленные символы вместе с символами из $\mathcal{P}$ и $\mathcal{F}$ образуют Алфавит логики первого порядка. Более сложные конструкции определяются индуктивно:

Терм есть символ переменной, либо имеет вид $f(t_1, \ldots, t_n)$, где f – функциональный символ арности n, а $t_1, \ldots, t_n$ – термы.

Атом имеет вид $p(t_1, \ldots, t_n)$, где p – предикатный символ арности n, а $t_1, \ldots, t_n$ – термы.

Атом в математической логике – простейший случай формулы; формула, которую нельзя расчленить на подформулы.

Предика́т (n-местный, или n-арный) – это функция с множеством значений {0,1} (или «ложь» и «истина»), определённая на множестве $M = M_1 \times M_2 \times \ldots \times M_n$. Таким образом, каждый набор элементов множества M он характеризует либо как «истинный», либо как «ложный».

Предикат можно связать с математическим отношением: если n принадлежит отношению, то предикат будет возвращать на ней 1.

Предикат – один из элементов логики первого и высших порядков. Начиная с логики второго порядка, в формулах можно ставить кванторы по предикатам.

Предикат называют тождественно-истинным и пишут:
$P(x_1, ..., x_n) \equiv 1$,
если на любом наборе аргументов он принимает значение 1.

Предикат называют тождественно-ложным и пишут:
$P(x_1, ..., x_n) \equiv 0$,
если на любом наборе аргументов он принимает значение 0.

Предикат называют выполнимым, если хотя бы на одном наборе аргументов он принимает значение 1.

Так как предикаты принимают только два значения, то к ним применимы все операции булевой алгебры, например: отрицание, импликация, конъюнкция, дизъюнкция и т.д.

Формула – это либо атом, либо одна из следующих конструкций: $\neg F, F_1 \vee F_2, F_1 \wedge F_2, F_1 \rightarrow F_2, \forall x F, \exists x F$, где F, F1, F2 – формулы, а x – переменная.

Переменная x называется связанной в формуле F, если F имеет вид $\forall xG$либо $\exists xG$ или же представима в одной из форм $\neg H, F_1 \vee F_2, F_1 \wedge F_2, F_1 \rightarrow F_2$, причем x уже связанна в H, F1 и F2. Если x не связанна в F, ее называют свободной в F. Формулу без свободных переменных называют замкнутой формулой, или предложением. Теорией первого порядка называют любое множество предложений.

Логика второго порядка – расширяет логику первого порядка, позволяя проводить квантификацию общности и существования не только над атомами, но и над предикатами.

Логика второго порядка не упрощается к логике первого порядка.

Логика первого порядка подходит для описания рутинных свойств системы, то есть тех, ради которых АВС создается. Так как свойства безопасности системы являются дополнительным всеобъемлющим требованием, то необходимо применение логики второго порядка. Ядро безопасности АВС гарантирует безопасность системы вне зависимости от того, какие функции ядра и в какой последовательности задействованы. При этом свойства безопасности системы в целом могут быть описаны следующим выражением:

$$\forall \alpha \in pos: P(\alpha), \qquad (1)$$

где pos – множество всех возможных последовательностей вызовов функций, предоставляемых ядром безопасности системы;

P() – предикат, определяющий выходную реакцию в системе в зависимости от входного воздействия.

Выражение (1) является предикатом второго порядка и определяет следующее свойство: любая операция, выполняемая пользовательским программным обеспечением, преобразуется в последовательность вызовов функций ядра безопасности системы (функций в множестве pos = свойство полноты) и при условии защиты программного обеспечения ядра системы от модификации (= свойство изоляции), свойство P() является свойством системы в целом. Доказательство безопасности системы сводится к демонстрации инвариантности модели системы по отношению к некоторому свойству безопасности, определяемому предикатом P. Таким образом, для синтеза защищенной вычислительной системы необходимо выполнение следующих условий:

- свойства безопасности системы должны быть реализованы с помощью ядра безопасности системы;
- данные свойства должны быть выражены предикатом второго порядка (1).

В анализируемых далее моделях безопасности предикат P конкретизируется, а вместо исследования выражений, описываемых логикой второго порядка, изучаются модели состояний системы. Для модели системы необходимо доказать следующую теорему, называемую **основной теоремой безопасности**: «Если система начинает работу в безопасном состоянии и все переходы системы из состояния в состояние являются безопасными, то система является безопасной».

Таким образом, необходимо ввести понятия, пригодные для описания свойств состояния системы. Самыми естественными понятиями, с помощью которых можно описать состояние системы, являются понятия субъекта, объекта и доступа, которые и являются основой описания состояния моделей безопасности защищенных АВС.

Сущность – любая именованная составляющая компьютерной системы.

Объект – пассивная сущность, используемая для хранения и получения информации. Возможные примеры объекта:

- Записи;
- Сегменты;
- Файлы;
- Терминалы;
- Узлы сети;
- Биты;
- Байты…

Субъект – активная сущность. Она может инициировать запросы к ресурсам и использовать их для выполнения каких-либо вычислительных заданий. В процессе исполнения субъекты исполняют операции. Примеры субъектов:

- Пользователь;
- Процесс;
- Устройство…

Взаимодействие субъекта и объекта, в результате которого производится перенос информации между ними, называется **доступом**. Существует две фундаментальные операции, переносящие информацию между ними:

- **Операции чтения** – такая операция, результатом которой является перенос информации от объекта к субъекту;
- **Операция записи** – такая операция, результатом которой является перенос информации от субъекта к объекту.

Основной характеристикой субъекта является **уровень безопасности**.

Уровень безопасности – иерархический атрибут, который может быть ассоциирован с сущностью компьютерной системы для обозначения степени ее чувствительности по безопасности. Эта степень чувствительности может отражать степень ущерба от нарушений безопасности.

В связи с тем, что в системе существуют иерархические отношения, то нам необходимо знать этот набор уровней, т.е. ту иерархию, по которой мы классифицируем систему. Пример:

- Неклассифицированная информация;
- Конфиденциальная информация;
- Секретная информация;
- Совершенно секретная информация.

Для того, чтобы сопоставлять уровни безопасности, нужно внести математические обозначения.

Уровни безопасности – L.

Иерархические отношения – $>,<,\leq,\geq$.

Множество L –полностью упорядоченное множество – мы можем однозначно определить соотношения между двумя любыми элементами этого множества.

Доверие – атрибут, задающий чувствительность субъекта к свойству безопасности.

Секретность – атрибут, задающий чувствительность объекта к свойству безопасности.

Доверие и секретность мы можем определить как функции, одна из которых называется **Clearance,** вторая – **Classification.** Областью значений каждой из функций является множество L. Функция Clearance определена на множестве субъектов, а функция Classification – на множестве объектов.

Clearance: S → L;
Classification: O→ L.

6.2. Классификация моделей безопасности

Рассмотрим модели безопасности, которые были предложены различными авторами для построения политик безопасности. Эти модели стали классическими, хотя и появились в разное время. В них для моделирования защиты от угроз АВС используется математическая логика. Согласно классификации угроз по цели реализации, обозначим группы соответствующих моделей безопасности:

1. Модели, предотвращающие угрозу раскрытия информации.
2. Модели контроля целостности информации.
3. Модели, предотвращающие угрозу отказа служб.

6.2.1. Модели безопасности, предотвращающие угрозу раскрытия

Модели данной группы предотвращают угрозу раскрытия, и в свою очередь делятся на три подгруппы:

1. Модели разграничения доступа, построенные по принципу предоставления прав.
2. Модели разграничения доступа, построенные на основе принципов теории информации.
3. Модели разграничения доступа, использующие принципы теории вероятности.

6.2.2. Модели разграничения доступа, построенные по принципу предоставления прав

Эта подгруппа моделей является базовой для построения политик безопасности на основе разграничения доступа. Впервые данные модели описаны в середине 60-х годов прошлого века. Право доступа в них можно описать как билет, дающий доступ к объекту, описанному в этом билете. Основные типы моделей в этой части:

- Модели дискреционного доступа.
- Модели мандатного доступа.

Модели дискреционного доступа (DAC)

Модели данного класса необходимы для синтеза политик безопасности, не позволяющих неавторизованному пользователю получать доступ к информации.

Модель АДЕПТ-50

В данной модели представлены 4 типа объектов, относящихся к рассматриваемым вопросам безопасности:

- U – пользователи;
- J – задания;
- T – терминалы;
- F – файлы.

Каждый объект описывается 4-мерным кортежем (A, C, F, M). Расшифруем:

A – скаляр, элементы иерархически упорядоченных уровней безопасности: несекретно, конфиденциально, секретно, совершенно секретно.

C – дискретный набор рубрик, не зависящих от A.

F – группа пользователей, имеющих право на доступ к определенному объекту.

M – набор видов доступа, разрешенных к определенному объекту или осуществляемых объектом. Примеры: читать, присоединять и т.п.

Если U – множество всех пользователей, известных системе, а F(i) – набор всех пользователей, имеющих право использовать объект i, то для модели формулируются следующие правила:

- Пользователь u получает доступ к системе тогда и только тогда, когда этот пользователь принадлежит множеству пользователей.

$$\mathbf{u \in U}$$

- Пользователь u получает доступ к терминалу t тогда и только тогда, когда u имеет право использовать терминал t.

$$\mathbf{u \in F(t)}$$

- Пользователь u получает доступ к файлу j тогда и только тогда, когда привилегии выполняемого задания шире привилегий файла или равны им; а пользователь u является членом группы с определенными полномочиями.

$$\mathbf{A(j) >= A(f),\ C(j) >= C(f),\ M(j) >= M(f),\ u \in F(f).}$$

Задавая параметры A, C, F, M, можно сформировать матрицу определения параметров безопасности.

Объект	**A**	**C**	**F**	**M**
Пользователь u	Const	Const	{u}	const
Терминал T	Const	Const	{u(t,i)}	const
Задание j	Min (A(u), A(t))	C(u) ∩ C(t)	{u(j,i) }	M(u) ∩ M(t)
Существующий файл f(i)	Const	Const	{u(f,i) }	const
Новый файл f=g(f1,f2)	Max(A(f1), A(f2))	C(f1) ∪ C(f2)	{u(f,j) }	M(f1) ∪ M(f2)

где f1,f2 – старые файлы, f – новый файл как функция от f1 и f2

5-мерное пространство безопасности Хартстона

Существует 5 основных наборов:

- A – установленные полномочия;
- U – пользователи;
- E – операции;
- R – ресурсы;
- S – состояния.

A x U x E x R x S

Доступ рассматривается как ряд запросов, осуществляемых пользователями u для выполнения операции e над ресурсами R в то время, когда система находится в состоянии s. Например, запрос на доступ рассматривается в виде 4-мерного кортежа:

$$q=(u,e,R,s),$$

мы получаем проекцию пространства безопасности. Запросы получают право на доступ в том случае, когда они полностью заключены в соответствующие подпространства.

Процесс организации доступа к ресурсам будет состоять из следующих процедур:

I. Вызвать все вспомогательные программы, необходимые для предварительного принятия решения.
II. Определить из U те группы пользователей, к которым принадлежит u. Затем выбрать из A спецификации полномочий, которые соответствуют выбранной группе пользователей. Набор полномочий A(u) определяет привилегии пользователя u.
III. Определить из A набор A(e) полномочий, которые устанавливают e как основную операцию. Этот набор A(e) называется привилегией операции e.
IV. Определить из A набор A(R`) – набор полномочий, которые определяют поднабор ресурсов, называемых привилегией ресурсов R`.

Общие полномочия, появляющиеся в пунктах 2-4 (A(u), A(e), A(R`)) образуют домен D полномочий для запроса q, такой что $D(q)=A(u)\cap A(e)\cap A(R`)$

V. Удостовериться, что запрашиваемый ресурс R` полностью включается в домен D(q).
VI. Осуществить разбиение набора домена D(q) на эквивалентные классы так, чтобы 2 полномочия попадали в эквивалентный класс тогда и только тогда, когда они специфицируют одну единицу ресурса. Получается, что новый набор полномочий, один на каждую единицу ресурса, указанную в домене, является записью – A(u,q). Читается как «фактическая привилегия пользователя u по отношению к запросу q».
VII. Вычислить условия фактического доступа, соответствующего запросу q, осуществляя логическое «и» или логическое «или» над условиями A(u,q).
VIII. Оценить условия фактического доступа и принять решение о доступе.
IX. Произвести запись необходимых событий.
X. Вызвать все программы, необходимые для организации доступа после принятия решения.

XI. Выполнить все вспомогательные программы, вытекающие для каждого случая из условия VIII.
XII. Если решение о доступе было положительным – завершить физическую обработку.

Автор модели Хартстон говорит о том, что не всегда нужно выполнять все 12 шагов в полном объеме. Например, шаги 2 и 6 осуществляются при регистрации пользователей в системе, и т.д.

К достоинствам моделей дискреционного доступа можно отнести хорошую гранулированность защиты и относительно простую реализацию. В качестве примера реализаций данного типа моделей можно привести так называемую матрицу доступа, строки которой соответствуют субъектам системы, а столбцы – объектам; элементы матрицы характеризуют права доступа.

К недостаткам систем, построенных на основе DAC, следует отнести проблему троянских программ (троянских коней).

Модели мандатного доступа (MAC)

Мандатный доступ накладывает ограничение на передачу информации от одного пользователя другому, что решает проблему троянских коней.

Классическая MAC – модель Белла и Лападула (БЛМ)

Появление: Белл и Лападула следили за тем, как переносятся документы на бумажных носителях между людьми в государственных организациях.

Выводы:

1. В правительстве США все субъекты и объекты ассоциируются с уровнями безопасности (от низких, неклассифицированных до высоких, совершенно секретных); для предотвращения утечки информации, субъектам с низкими уровнями безопасности не позволяется читать информацию из объектов с высокими уровнями безопасности.

Отсюда следует ***первое правило БЛМ*** (простое свойство безопасности, «нет чтения вверх») – NRU (no read up) – субъект с уровнем безопасности Xs может читать информацию из объекта с уровнем безопасности Xo, только если Xs преобладает над Xo.

2. В правительстве США субъектам запрещено размещать или записывать информацию в объекты, имеющие более низкий уровень секретности (например, нельзя выбрасывать бумаги в мусорное ведро).

Второе правило БЛМ («нет записи вниз») – NRD (no write down) – субъект с уровнем безопасности Xs может писать информацию в объект с уровнем безопасности Xo, только если Xo преобладает над Xs.

Именно второе правило БЛМ решает проблему троянских коней: типичная ситуация для троянских коней, когда информация переносится с более высокого уровня на более низкий, невозможна.

Формализация БЛМ:

Если S – множество субъектов, O – множество объектов, L – решетка уровней безопасности, тогда можно определить функцию F, определяющую уровни безопасности своих аргументов в данном состоянии. Применяется к субъектам и объектам, записывается как:

$$F: S \cup O \text{—›} L.$$

V – множество состояний, которое составляется из упорядоченных пар (F, M). M – матрица доступа субъектов системы к объектам. Более того, система представляется начальным состоянием Vo, определенным множеством запросов к системе R и функцией переходов T: (V x R) —›V, то есть такой, что система переходит из состояния в состояние после исполнения запроса.

Определение 1

Состояние (F, M) безопасно по чтению тогда и только тогда, когда для любого «s» из множества субъектов и любого «o» из множества объектов для допустимого чтения, следует, что F(S) преобладает над F(O) –

$$\mathbf{M(S,O) \text{—›} F(S)>F(O).}$$

Определение 2

Состояние (F, M) безопасно по записи тогда и только тогда, когда для любого s из множества субъектов и любого o из множества объектов для допустимой записи M(S,O) означает, что F(O) преобладает над F(S) –

$$\mathbf{M(S,O) \text{—›} F(O)>F(S).}$$

Определение 3

Состояние безопасно тогда и только тогда, когда оно безопасно по чтению и записи.

Три определения необходимы для того, чтобы сформулировать и доказать **основную теорему безопасности**:

Система (Vo, R, T), описываемая начальным состоянием Vo, множеством запросов к системе R и функцией переходов T, безопасна тогда и только тогда, когда состояние Vo безопасно и T таково, что для любого состояния V, достижимого из Vo, после исполнения конечной последовательности запросов из R можно осуществить переход к состоянию V* [T(Vo,R)=V*], также принадлежащему множеству состояний.

Классическая модель БЛМ имеет недостатки:

1. Проблема в распределенных системах – удаленное чтение. Запросы от одного рабочего места к другому, между сервером и рабочей станции создают удаленные сеансы, при этом невозможно соблюдать правила NWD и NRU. Решение: БЛМ применять локально, а для создания сеансов удаленной работы применять другую модель.
2. Проблема доверенных субъектов. Должен ли администратор системы подчиняться правилам БЛМ? В любой системе, на которую распространяются правила БЛМ, нужно выделять доверенные субъекты и рассматривать их в отдельности. Решение: использовать модели невыводимости и невмешательства.
3. Проблема системы Z. Джон Маклин разработал и описал эту систему: система, удовлетворяющая правилам БЛМ может, иметь ряд проблем с секретностью. Ничто в БЛМ не предотвращает систему от деклассификации объекта от «совершенно секретного» до «секретного» по желанию совершенно секретного пользователя.

Допустим, есть субъект с высокой степенью доверия A, он читает информацию из объекта с уровнем классификации тоже A. Субъект решил понизить свою степень доверия до B (A>B). После понижения своей степени доверия он может записать информацию в файл с классификацией B. БЛМ на это отреагировать не может. Белл и Лападула предполагали такую возможность, и в их дальнейшей разработке БЛМ были введены дополнительные требования – требования сильного и слабого спокойствия.

Правило сильного спокойствия:
уровни безопасности субъектов и объектов никогда не меняются в ходе системной операции. За счет этого теряется некоторая гибкость в выполнении операций.

Правило слабого спокойствия:
уровни безопасности субъектов и объектов никогда не меняются в ходе системной операции таким образом, чтобы нарушить заданную политику безопасности (например, уровень безопасности не должен меняться, когда к нему обращается некоторый субъект).

Самая слабая модель – БЛМ в классической формулировке, самая сильная – модель с сильным спокойствием.

С одной стороны, требования БЛМ являются слишком строгими, с другой стороны, есть ряд упущений, которые были уже обозначены, более того, в БЛМ отсутствует поддержка многоуровневых объектов (в секретном документе есть несколько абзацев, которые являются несекретными). Логическим продолжением МАС БЛМ стало появление специализированных моделей, перекрывающих проблемы, существовавшие в БЛМ.

Специализированная модель MMS

С целью устранения обозначенных недостатков Лендвером и Мак-Лином в ***модели передачи военных сообщений (MMS*** – military message system) были предложены определения; сформулированы и доказаны формальная и неформальная модели MMS.

Определение 1

Классификация – обозначение, накладываемое на информацию, отражающее ущерб, который может быть причинен неавторизованным доступом, включающим уровни: Secret, Top secret, и метки Crypto, Nuclear и т.д. Множество классификаций и отношений между ними образуют решетки.

Определение 2

Степень доверия пользователю – уровень благонадежности персоны. Каждый пользователь имеет степень доверия, и операции, производимые системой для данного пользователя, могут проверить степень доверия пользователю и классификацию объекта, с которыми он оперирует.

Определение 3

Пользовательский идентификатор – строка символов, используемая для того, чтобы отметить пользователя системы. Чтобы использовать систему, пользователь должен предъявить ей пользовательский идентификатор, а система должна провести его аутентификацию. Данная процедура называется логин. Каждый пользователь должен иметь уникальный логин.

Пользователь – это персона, уполномоченная для использования системы.

Определение 4

Роль – это работа, исполняемая пользователем. Пользователь всегда ассоциирован как минимум с одной ролью в некоторый момент времени. Он может менять роль в течение сессии. Для действий в данной роли пользователь должен быть уполномочен. Некоторые роли могут быть связаны только с одним пользователем в данный момент времени.

Определение 5

Объект – это одноуровневый блок информации. Это минимальный блок информации в системе, который имеет классификацию, т.е. объект не содержит других объектов и он не многоуровневый.

Определение 6

Контейнер – многоуровневая информационная структура. Имеет классификацию и может содержать объекты, каждый со своей классификацией, и/или другие контейнеры. Пример контейнера – файл.

Определение 7

Сущность – это объект или контейнер.

Определение 8

Требования степени доверия контейнеров – атрибут некоторых контейнеров. Для некоторых контейнеров важно требовать минимум степени доверия, т.е. пользователь, не имеющий соответствующий уровень благонадежности, не может просматривать содержимое контейнера. Такие контейнеры помечаются соответствующим атрибутом – CCR. Если у нас есть пользователь со степенью доверия «confidential», то он не может просматривать параграф сообщения «confidential» из документа «top secret», если этот документ находится в CCR-контейнере. Если нужно это разрешить – документ необходимо извлечь из контейнера.

Определение 9

Идентификатор (ID) – имя сущности без ссылки на другие сущности. Пример – имя файла является идентификатором файла. Обычно все сущности имеют идентификатор.

Определение 10

Ссылка на сущность является прямой, если это идентификатор сущности.

Определение 11

Ссылка на сущность является косвенной, если это последовательность двух или более имен сущностей, из которых только первое – идентификатор.

Определение 12

Операция – функция, которая может быть применена к сущности. Она может позволять просматривать или модифицировать сущность. Некоторые операции могут использовать более одной сущности (например, копирование).

Определение 13

Множество доступа – множество троек (пользовательский идентификатор или роль, операция, индекс операнда), которые связаны с сущностью.

Определение 14

Сообщение – особый тип, реализуемый в данной модели. Является контейнером. Включает поля «куда», «откуда», «время», «предмет», «текст», «автор». Чертежные сообщения включают поле чертежа.

Неформальная модель MMS

Пользователь получает доступ к системе только после прохождения процедуры login. Для этого пользователь предоставляет системе пользовательский идентификатор, и система производит аутентификацию, используя пароли, отпечатки пальцев или другую адекватную технику. После успешного прохождения аутентификации пользователь запрашивает у системы операции для использования функций системы. Операции, которые пользователь может запросить у системы, зависят от его Id или роли, для которой он авторизован.

С использованием операций пользователь может просматривать или модифицировать объекты или контейнеры. При этом система реализует следующие ограничения:

1) **Предположение безопасности:**
   A1: офицер безопасности системы присваивает уровни доверия, производит классификацию устройств и создает множество ролей корректно;
   A2: пользователь вводит корректную классификацию, когда изменяет, объединяет и переклассифицирует информацию;
   A3: пользователь классифицирует сообщения и определяет множество доступа для сущностей, которые он создает так, что только пользователь с требуемой благонадежностью может просматривать информацию;
   A4: пользователь должным образом контролирует информацию объектов, требующих благонадежности;
2) **Ограничение безопасности (относятся к компьютерной системе):**
   B1: Авторизация. Пользователь может запрашивать операции над сущностями, только если пользовательский идентификатор или текущая роль присутствуют во множестве доступа сущности вместе с этой операцией и со значением индекса, соответствующим позиции операнда, в которой сущность относят к требуемой операции.
   B2: Классификационная иерархия. Классификация контейнера всегда больше или равна классификации сущностей, которые он содержит.
   B3: Изменение объектов. Информация, переносимая из объекта, всегда наследует классификацию данного объекта. Информация, вставляемая в объект, должна иметь классификацию ниже классификации этого объекта.
   B4: Просмотр. Пользователь может просматривать только сущности с классификацией меньше, чем классификация устройства вывода и степень доверия к пользователю.
   B5: Доступ к контейнерам, требующим степени доверия. Пользователь может получить доступ к косвенно адресованной сущности

внутри контейнера, требующего степени доверия, только если его степень доверия не ниже классификации контейнера.

B6: Преобразование косвенных ссылок. Пользовательский идентификатор признается законным для сущности, к которой он обратился косвенно, только если он авторизован для просмотра этой сущности через ссылку.

B7: Требование меток. Сущности, просмотренные пользователем, должны быть помечены его степенью доверия.

B8: Установка степеней доверия, ролей, классификации устройств. Только пользователь с ролью офицера безопасности системы может устанавливать данные значения. Текущее множество ролей пользователя может быть изменено офицером безопасности или самим пользователем.

B9: Понижение классификации информации. Никакая классифицированная информация не может быть понижена в уровне своей классификации, за исключением случая, когда эту операцию выполняет пользователь с ролью «пользователь, уменьшающий классификацию информации».

B10: Уничтожение информации. Эта операции проводится только пользователем с ролью «пользователь, уничтожающий информацию».

Формальная модель MMS

Разработаем формальную модель MMS, соответствующую неформальным спецификациям, данным выше.

Предполагая существование множества возможных пользователей и множества возможных сущностей, можно определить состояние системы, включая ее безопасное состояние. Далее определяется система и ее история, вводятся ограничения на переход из одного состояния в другое. Система, все переходы которой удовлетворяют данным ограничениям, безопасна для переходов. В заключение определяется безопасная история и безопасность системы.

Основной идеей проведения формализации является взгляд на компьютерную систему как на взаимоотношения между состояниями системы и самой системой. Предполагается, что состояние системы состоит из сущностей и их отношений, и система добавляет к данным отношениям пользователей и пользовательские операции над сущностями. Следовательно, все ограничения на свойства пользователей включены в определение безопасности системы. Данный взгляд разделяет состояние системы и саму систему в терминах статики в противоположность динамическим свойствам. Статические свойства – свойства, которые сохраняются для всех состояний системы, и, следовательно, могут быть проверены для изолированного состояния системы; динамические состояния – те, кото-

рые нуждаются в исследовании взаимоотношений между состояниями безопасности, и, следовательно, могут быть проверены только исследованием двух или более состояний. В определение безопасности состояния включены только статические свойства.

Принципиальной трудностью, возникающей при формализации модели, является интерпретация «копирования», «просмотра», «вывода системы» и «авторизованной операции». Информация считается копируемой не только тогда, когда она непосредственно переносится из одной сущности в другую, но и когда она дает потенциальный вклад в другую сущность. Например, если операция сканирует файл сообщений А и копирует сообщения, выбранные фильтром Ф в файл сообщений Б, то и А, и Ф являются потенциальным вкладом в модификацию Б (и, следовательно, субъектом для ограничений, вызванных безопасностью копирования и CCR безопасностью), даже если и А, и Ф – пусты. Семантика для просмотра – проста: сущность может быть просмотрена, если операция делает ее членом выходного контейнера.

В формализации вывод системы интерпретируется как множество контейнеров; другие сущности, части сущностей, ссылки и классификации, которые видны пользователю, интерпретируются как копирующиеся в контейнер выхода.

Семантика авторизованных операций неспецифицирована. Можно только сказать, что неавторизованные операции не должны изменять состояние системы, исключая сообщения об ошибке.

6.2.3. Достоинства и недостатки моделей предоставления прав

Достоинства:

1) Интуитивная понятность.
2) Возможность реализации с высокой степенью точности.

Недостатки:

1) Возможность образования скрытых каналов утечки информации.

Скрытые каналы утечки информации обнаружить несложно, но лишь в процессе эксплуатации системы, поэтому их сложно ликвидировать.

6.3. Информационные модели

Информационные модели определяют ограничения на предоставление ввода/вывода системы, которые достаточны для реализации системы.

Они накладывают ограничения на интерфейс программных модулей системы с целью достижения безопасной реализации. При этом подробности реализации определяются разработчиком системы. Данные модели являются результатом применения теории информации к проблеме безопасности систем.

Рассмотрим две информационные модели:

- Модель невмешательства.
- Модель невыводимости.

Достоинством данных моделей является:

1) Отсутствие скрытых каналов утечки.
2) Естественность их использования для реализации сетевых защищенных АВС.

6.3.1. Модель невмешательства

Невмешательство – это ограничение, при котором ввод высокоуровневого пользователя не может смешиваться с выводом низкоуровневого пользователя. Модель невмешательства рассматривает систему, состоящую из 4-х объектов:

- Высокий ввод (High In).
- Низкий ввод (Low In).
- Высокий вывод (High Out).
- Низкий вывод (Low Out).

Рассмотрим систему, вывод которой пользователю *u* определён функцией *out*:

$$out\ (u,\ hist.read\ (u)),$$

где *hist.read (u)* – это история ввода системы (*traces*), чей последний ввод был *read (u)*, т.е. команда чтения, исполненная пользователем *u*.

Введем понятие – очищение (*purge*) истории ввода. Purge удаляет команды, исполненные пользователем, чей уровень безопасности не доминирует над уровнем безопасности u.

Используется также функция *clearance (u)*, которая определяет степень доверия к пользователю.

Система удовлетворяет требованиям невмешательства, если, и только если для всех пользователей *u*, всех историй *T* и всех команд вывода *c* выполняется следующее равенство:

$$out\ (u,\ T.c(u)) = out\ (u,\ purge\ (u,\ T).c(u))$$

С целью проверки системы на соответствие требованиям невмешательства разрабатывалось большое количество различных условий, выполнение которых было бы достаточно для поддержки невмешательства. Верификация модели невмешательства более сложная, чем верификация модели БЛМ. Достоинство в том, что при применении данной модели не остаётся скрытых каналов утечки информации, она более интуитивно понятна по сравнению с БЛМ.

Сравнение модели БЛМ и модели невмешательства:

1. БЛМ слабее, чем модель невмешательства, за счёт того, что последняя запрещает многие скрытые каналы, которые остаются при реализации БЛМ.
2. Модель невмешательства слабее, чем БЛМ, так как она разрешает низкоуровневым пользователям копировать один высокоуровневый файл в другой высокоуровневый файл, что запрещается в последней из-за нарушения безопасности по чтению.

6.3.2. Модель невыводимости

Так же как и предыдущая модель, модель невыводимости базируется на рассмотрении информационных потоков, выражается в терминах пользователей и информации, связанных с одним из двух возможных уровней секретности:

- Высокий.
- Низкий.

Система считается **невыводимо безопасной**, если пользователи с низким уровнем безопасности не могут получить информацию с высоким уровнем безопасности в результате любых действий пользователей с высоким уровнем безопасности.

Или другими словами: каждый пользователь связан с определенным взглядом на систему и может получить информацию, интерпретируя видимое ему поведение. Если система является невыводимо безопасной, то низкоуровневые пользователи не должны получить новой информации, если на вводе системы есть дополнительные высокоуровневые пользователи. Кроме этого, если низкоуровневые пользователи могут получить определенную информацию, основываясь на видимом ими поведении, то удаление высокоуровневых пользователей не должно изменить получаемой низкоуровневыми пользователями информации.

6.4. Вероятностные модели

Модели разграничения доступа, использующие принципы теории вероятности, исследуют вероятность преодоления системы защиты за определённое время t. К достоинствам модели данного типа можно отнести числовую оценку стойкости системы защиты. Недостатком является то, что изначально предполагается, что система может быть преодолена. Основная задача для таких моделей – это минимизация вероятности преодоления системы защиты.

6.4.1. Игровая модель

Первая из вероятностных моделей – это **игровая модель**. Игровая модель системы защиты строится по следующему принципу:

Разработчик создаёт первоначальный вариант системы защиты. После этого злоумышленник начинает его преодолевать. Если в момент времени T, в который злоумышленник преодолел систему защиты, и у разработчика нет нового варианта системы защиты, то считается, что система защиты преодолена. Если нет, то процесс продолжается.

Считается, что данная модель описывает процесс эволюции системы защиты в течение некоторого времени.

6.4.2. Модель с полным перекрытием

Вторая модель – это модель системы безопасности **с полным перекрытием**. В данном варианте модели декларируется то, что система, использующая данную модель, должна иметь, по крайней мере, одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему. В общих чертах её можно изобразить следующим образом (рис. 5):

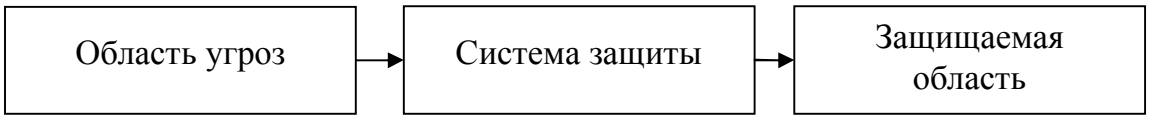

Рис. 5

В модели точно определяется каждая область, требующая защиты, оцениваются средства обеспечения безопасности с точки зрения эффективности, и их вклад в обеспечение безопасности во всей вычислительной системе. Считается, что несанкционированный доступ к каждому из набора защищаемых объектов *O* сопряжён с некоторой величиной ущерба, и этот ущерб может быть определён количественно. С каждым объектом, требующим защиты, связывается некоторое множество действий, к которому может прибегнуть злоумышленник для получения несанкционированного доступа к объекту. При этом можно попытаться перечислить все потенциально злоумышленные действия и, тем самым, сформировать набор угроз T, который направлен на выявление угроз безопасности. В этом случае основной характеристикой набора угроз является вероятность проведения каждого из злоумышленных действий. Естественно, что в жизни данные вычисления могут быть произведены с ограниченной степенью точности.

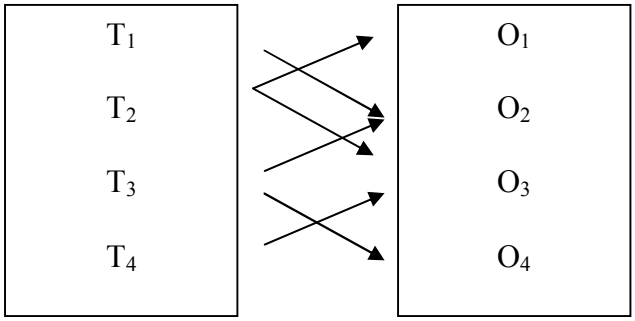

Рис. 6. Двудольный граф «Объект-угроза»

Одна угроза может действовать на несколько объектов. Цель защиты состоит в том, чтобы перекрыть каждое ребро графа. Получив такой граф, можно говорить о том, что существуют рёбра $<T_iO_j>$. Создадим третий набор, включающий средства безопасности M. Идеальным случаем является тот, когда для каждого M_k из множества M устраняется некоторое ребро $<T_iO_j>$ из данного графа. Получается, что набор M средств обеспечения безопасности преобразует двудольный граф в трёхдольный, и тогда существуют рёбра вида $<T_iM_k.><M_kO_j>$. если в системе остается ребро $<T_iO_j>$, то в ней существует незащищенный объект.

Нужно помнить о том, что одно и то же средство обеспечения безопасности может перекрывать более одной угрозы и/или защищать более одного объекта. Более того, отсутствие ребра $<T_iO_j>$ не гарантирует полного обеспечения безопасности.

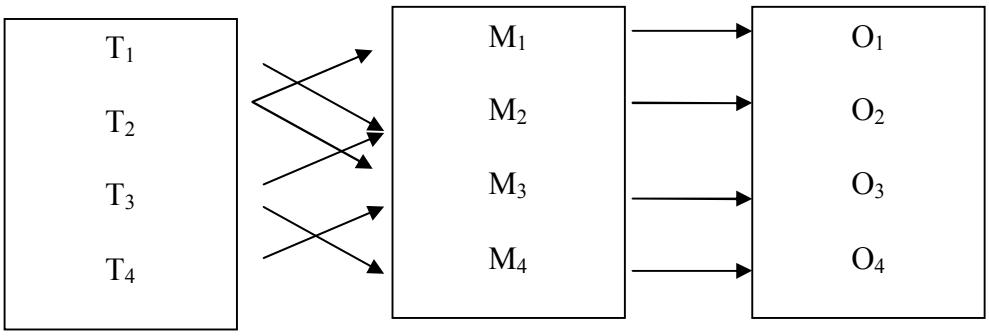

Рис. 7

По результатам рассмотрения вероятностных моделей, можно сказать следующее. Данные модели не специфицируют непосредственно механизмы защиты информации и могут использоваться только в сочетании с другими типами моделей системы защиты информации. Вероятностные модели позволяют численно получить оценку степени надёжности системы защиты информации. Более того, они могут численно оценить вероят-

ность преодоления системы безопасности, а также оценить степень ущерба при преодолении системы защиты.

К достоинствам данных моделей можно отнести то, что при их использовании можно минимизировать затраты на внедрение элементов системы защиты информации за счёт того, что можно оценить вероятность наступления той или иной угрозы и принять решение о применении того или иного средства защиты информации.

6.5. Модели контроля целостности

Рассмотрим модели безопасности, контролирующие целостность информации. В частности, модели Биба, использующиеся для синтеза механизмов контроля целостности информации в системе, а также модель Кларка – Вилсона (КВМ), которая является примером неформального выражения политики безопасности. Последняя модель сформулирована в виде набора неформальных правил, и хотя в литературе она названа моделью безопасности, ее скорее можно назвать политикой контроля целостности.

6.5.1. Модель Биба

Кен Биба в середине семидесятых годов прошлого века сделал два наблюдения. Они были последовательно внесены в модель безопасности, которая с тех пор называется моделью целостности Биба (или просто моделью Биба). В контексте разговора о моделях контроля целостности запись наверх может представлять угрозу в том случае, если субъект с низким уровнем безопасности искажает или уничтожает данные в объекте, лежащем на более высоком уровне. Поэтому, исходя из задач целостности, можно потребовать, чтобы такая запись была запрещена. Кроме того, можно рассматривать чтение снизу как поток информации, идущий из объекта нижнего уровня и нарушающий целостность субъекта высокого уровня. Поэтому весьма вероятно, что и такое чтение необходимо запретить.

Биба выразил свою модель таким же способом, каким была выражена БЛМ, за тем исключением, что правила его модели являются полной противоположностью правилам БЛМ. Возможны три вариации модели Биба: мандатная модель целостности, модель понижения уровня субъекта и модель понижения уровня объекта. Фактически, общий термин «модель Биба» используется для обозначения любой или сразу всех трех моделей.

6.5.1.1. Мандатная модель целостности Биба

Ее часто называют инверсией БЛМ. Это довольно точное название, поскольку основные правила этой модели просто переворачивают правила БЛМ. Мы будем ссылаться на эти правила как «нет чтения снизу» (NRD) и «нет записи наверх» (NWU) и определим их в терминах субъектов, объектов и нового типа уровней безопасности – уровней целостности, над которыми может быть введено отношение преобладания.

Правило NRD мандатной модели целостности Биба определяется как запрет субъектам на чтение информации из объекта с более низким уровнем целостности. Правило NWU мандатной модели целостности Биба определяется как запрет субъектам на запись информации в объект с более высоким уровнем целостности.

Одним из преимуществ этой модели является то, что она унаследовала многие важные характеристики БЛМ, включая ее простоту и интуитивность. Это значит, что проектировщики реальных систем могут легко понять суть этих правил и использовать их для принятия решений при проектировании. Кроме того, поскольку мандатная модель целостности Биба, подобно БЛМ, основана на простой иерархии, ее легко объяснить и изобразить пользователям системы.

С другой стороны, модель представляет собой очевидное противоречие с правилами NRU и NWD. Это значит, что если необходимо построить систему, которая предотвращает угрозы как секретности, так и целостности, то одновременное использование правил моделей БЛМ и Биба может привести к ситуации, в которой уровни безопасности и целостности будут использоваться противоположными способами.

Рассмотрим формальное описание модели Биба. Для этого опишем простые математические конструкции, которые помогут описать различные правила, составляющие мандатную модель целостности Биба.

Начнем с представления множества субъектов и объектов. Уровни целостности субъекта или объекта x обозначаются как уровень (x), и для них введено отношение преобладания. Используя эти определения, сформулируем правила NRD и NWU мандатной модели целостности Биба в терминах булевой функции разрешить:

NRD: $\forall s \in S, o \in O$: разрешить (s, o, чтение) $\Leftrightarrow$ уровень (o) > уровень (s).

Данный тип определения предусматривает условия, при которых функция разрешить принимает значение истинно. Определение утверждает, что для всех определенных субъектов и объектов операция чтения разрешена только в том случае, если выполняется условие преобладания. Правило NWU просто переворачивает использование отношения преобладания, как показано в следующем определении:

NWU: $\forall s \in S, o \in O$: разрешить (s, o, запись) $\Leftrightarrow$ уровень(s) > уровень(o).

Это определение утверждает, что для всех субъектов и объектов операция записи разрешается только в том случае, если выполняется условие преобладания. Подобие определения этих двух правил правилам модели БЛМ может предоставить удобный способ для проектировщиков системы предусмотреть возможность переконфигурирования правил БЛМ таким образом, чтобы поддерживать мандатную модель целостности Биба.

6.5.2. Модель понижения уровня субъекта

Вторая модель Биба заключается в небольшом ослаблении правила чтения снизу. Мандатная модель целостности не позволяет субъектам с высокой целостностью читать информацию из объектов с более низкой целостностью. Это правило гарантирует, что информация из объекта с низкой целостностью не нарушит целостности субъекта. Однако в модели понижения уровня субъекта ему разрешается осуществлять чтение снизу, но в результате такого чтения уровень целостности субъекта понижается до уровня целостности объекта.

Мотивом для введения такого правила может являться то, что субъекты с высокой целостностью рассматриваются как «чистые». Когда к чистому субъекту попадает информация из менее чистого источника, субъект «портится», и его уровень целостности должен быть соответственно изменен.

Одной из характеристик этой модели является то, что она не накладывает никаких ограничений на то, что субъект может прочитать. Если, например, субъект не должен никогда переходить на более низкий уровень целостности, то не следует использовать эту модель, поскольку она может привести к такому нарушению. Если все же эта модель реализована в реальной системе, то необходимо создание некоторых дополнительных мер, предупреждающих субъекта о возможных последствиях выполнения таких операций чтения перед тем, как они будут выполнены.

Следует также заметить, что модель подразумевает монотонное изменение уровней целостности субъектов. То есть, уровни целостности субъектов или остаются неизменными, или снижаются. Иными словами, целостность субъекта может остаться прежней или ухудшиться, поскольку модель не предусматривает механизмов повышения уровня целостности субъекта.

6.5.3. Модель понижения уровня объекта

Последний тип модели Биба представляет собой ослабление правила для записи наверх, то есть вместо полного запрета на запись наверх эта модель разрешает такую запись, но снижает уровень целостности объекта

до уровня целостности субъекта, осуществлявшего запись. Мотивы для такого правила те же, что и в модели понижения уровня субъекта.

Данная модель, подобно предыдущей, не накладывает никаких ограничений на то, что субъект может читать или писать. Поэтому в ситуациях, когда искажения объекта и понижение его уровня целостности могут вызвать серьезные последствия, использование этой модели не допускаются. Например, критическая база данных, включающая данные, целостность которых имеет предельно высокое значение, не может быть реализована на основании этой модели. Если данная модель используется в реальной системе, то необходимо возложить на субъекты ответственность за деградацию объектов с высокой целостностью. Для реализации этого потребуется использование дополнительных средств обработки.

Модель проста и интуитивно понятна, может быть выражена простыми правилами (NRD и NWU). Модель Биба также обладает многими проблемами, присущими БЛМ. Так, использование модели Биба в распределенных системах может привести к двунаправленному потоку информации при удаленном чтении, т.е. возникает эффект системы Z, описанный ранее. В практическом применении модель Биба слишком сильно полагается на понятие доверенных процессов, то есть проблема необходимости создания доверенных процессов для повышения или понижения целостности субъектов или объектов является весьма существенной. Эта критика последовала за критикой доверенных процессов в БЛМ.

В качестве дополнительной критики модели Биба можно упомянуть то, что она не предусматривает механизмов повышения целостности, что ведет к монотонному снижению целостности системы.

6.6. Модель Кларка-Вилсона

В 1987 году Дэвид Кларк и Дэвид Уилсон представили модель целостности, которая существенно отличалась от уровне-ориентированных моделей безопасности БЛМ и Биба. Созданию этой модели, которая известна как модель Кларка-Вилсона (МКВ), способствовал анализ методов управления целостностью бумажных ресурсов в неавтоматизированном офисе коммерческими организациями. Получившаяся модель целостности представляет собой руководство для разработчиков и проектировщиков компьютерных систем по обеспечению целостности определенных вычислительных ресурсов.

Модель МКВ выражается в терминах набора правил функционирования и обслуживания компьютерного окружения или приложения. Эти правила вырабатываются для обеспечения уровня защиты целостности для некоторого заданного подмножества данных в этом окружении или

приложении. Критическим понятием модели МКВ является то, что эти правила выражаются с использованием так называемых правильно сформированных транзакций, в которых субъект инициирует последовательность действий, которая выполняется управляемым и предсказуемым образом.

Представим модель МКВ с помощью строгого описания основных компонентов, включенных в модель. Модель Кларка-Вилсона выражается в терминах конечного множества. За D (для данных) обозначим все наборы данных в определенной компьютерной системе.

Чтобы различать данные, обладающие и не обладающие целостностью, создатели модели разделили D на два непересекающиеся подмножества, которые называются ограниченные элементы данных (CDI) и неограниченные элементы данных (UDI). Это можно изобразить следующими определениями:

$$D = CDI \cup UDI;\ CDI \cap UDI = 0.$$

Первое определение показывает, что D является объединением CDI и UDI, а второе определение показывает, что нет элементов, принадлежащих и CDI, и UDI. Набор D разделен таким образом, потому что мы хотим показать, как может меняться целостность данных. Другими словами, данные, не имеющие целостности и находящиеся поэтому в UDI, могут быть некоторым образом модернизированы, так чтобы иметь целостность и находиться соответственно в CDI.

Субъекты включены в модель как множество компонентов, которые могут инициировать так называемые процедуры преобразования. Процедура преобразования определяется как любая ненулевая последовательность элементарных действий. Элементарное действие, в свою очередь, определяется как переход состояния, который может вызвать изменение некоторых элементов данных. Например, субъекты могут устранять элементы данных, изменять информацию в элементах данных, копировать их и т.д. Каждая из этих операций называется процедурой преобразования, поскольку действительный способ, которым каждая из них выполняется, включает в себя последовательность элементарных действий (например, копирование A в B обычно состоит из таких операций, как чтение A, создание B, запись в B).

6.6.1. Правила модели МКВ

Используя вышеуказанные понятия, мы можем теперь рассмотреть основные правила, составляющие МКВ. В МКВ девять правил. Предполагается, что правила приняты все вместе, так что любое правило может ссылаться на любое другое правило без каких-либо ограничений.

Правило 1. В системе должны иметься процедуры утверждения целостности, утверждающие целостность любого CDI.

Простейшим примером такой процедуры утверждения является проверка контрольной суммы. При использовании этого подхода вычисляется контрольная сумма некоей хранимой информации, и копии этой информации сравниваются с оригиналом путем проверки соответствующих контрольных сумм. Различия в контрольных суммах сигнализируют о внесении изменений.

Правило 2. Применение любой процедуры преобразования к любому CDI должно сохранять целостность этого CDI.

Это правило можно рассматривать как свойство скрытия применения процедуры преобразования над CDI, то есть любое применение процедуры преобразования над CDI не приведет к нарушению целостности CDI.

Правило 3. Только процедура преобразования может вносить изменения в CDI.

Данное правило модели МКВ не позволяет субъектам с низкой целостностью, то есть не использующим процедуру преобразования, изменять объекты с высокой целостностью, то есть CDI. В этом плане модель Кларка-Вилсона подобна мандатной модели целостности Биба.

Правило 4. Субъекты могут инициировать только определенные процедуры преобразования над определенными CDI.

Это правило предполагает, что система должна определять и поддерживать некоторые отношения между субъектами процедуры преобразования и CDI, так называемые МКВ-тройки. Каждая такая тройка определяет возможность данного субъекта применить данную процедуру преобразования к данному CDI. Например, если (s, t, d) является элементом отношения, то субъекту s разрешается применить процедуру преобразования t к CDI d. Если же эта тройка не является элементом отношения, то такой тип применения процедуры преобразования будет запрещен. Это правило гарантирует, что всегда можно определить, кто может изменить CDI и как это изменение может произойти.

Правило 5. МКВ-тройки должны проводить некоторую соответствующую политику разделения обязанностей субъектов.

Это правило предусматривает, что компьютерная система определяет такую политику, чтобы не позволять субъектам изменять CDI без соответствующего вовлечения других субъектов. Это предотвращает субъектов от возможности наносить ущерб целостности CDI. Некоторые системы управления конфигурацией предоставляют уровень разделения обязанностей. Например, в некоторых системах разработчики ПО должны представить свои модули на просмотр менеджеру по разработке ПО перед тем, как они смогут включить их в конфигурацию. Этот подход защищает целостность конфигурации ПО.

Правило 6. Некоторые специальные процедуры преобразования могут превращать UDI в CDI.

Правило 7. Каждое применение процедуры преобразования должно регистрироваться в специальном CDI, в который может производиться только добавление информации, достаточной для восстановления картины о процессе работы этого CDI.

Это правило требует ведения специального регистрационного журнала, который хранится в определенном CDI.

Правило 8. Система должна распознавать субъекты, пытающиеся инициировать процедуру преобразования.

Это правило определяет механизмы предотвращения атак, при которых один субъект пытается выдать себя за другого.

Правило 9. Система должна разрешать производить изменения в списках авторизации только специальным субъектам (например, офицерам безопасности).

Можно сказать, что указанные выше девять правил определяют, как может быть проверена целостность, как и кем могут изменяться CDI и как UDI могут быть превращены в CDI.

Основным преимуществом модели МКВ является то, что она основана на проверенных временем методах обращения с бумажными ресурсами. Поэтому модель МКВ не следует рассматривать как академическое исследование, а скорее как комплекс существующих методов. Модель МКВ также предоставляет исследователям методы работы с целостностью, отличные от традиционных уровне-ориентированных подходов, таких как модели БЛМ и Биба.

Основным недостатком модели является то, что процедуру утверждения целостности и методы предотвращения CDI от искажения целостности нелегко реализовать в реальных компьютерных системах.

Все недостатки данной модели вытекают из-за ее неформализованности. Ее можно применять при проектировании систем для спецификации пользовательских приложений и использовать на соответствующем уровне иерархии рассмотрения защищенной вычислительной системы.

6.7. Модели, предотвращающие угрозу отказа служб

Рассмотренные ранее исследования компьютерной безопасности были связаны с угрозами раскрытия и нарушением целостности. Одной из причин такой очередности долгое время являлось то, что различные международные организации по защите определяли раскрытие и целостность как основные угрозы. В результате, большая часть работы велась именно в этих направлениях.

Однако в области моделей, противодействующих отказу в обслуживании, были сделаны некоторые шаги. Рассмотрим понятия, связанные с описанием и предотвращением угрозы отказа в обслуживании (ОВО). В частности, определим ряд терминов, среди которых важное место занимает понятие максимального времени ожидания, впервые введенное Вирджилом Глигором.

6.7.1. Основные понятия ОВО

Безопасные вычислительные системы служат промежуточным звеном при запросе тех или иных услуг пользователями за счет монитора ссылок. Такой промежуточный монитор ссылок позволяет рассмотреть запросы услуг в терминах простой модели, в которой пользователи являются зарегистрированными либо незарегистрированными, и обеспечиваются запрашиваемой услугой либо получают отказ. В случаях, когда зарегистрированным пользователям не предоставляется запрашиваемая услуга, говорят, что имеет место отказ в обслуживании.

Глигор первым отметил, что в понятия предоставления или отказа в обслуживании должно быть включено время. Каждая услуга должна быть связана с некоторым периодом времени, называем максимальным временем ожидания (MWT). Для некоторой услуги MWT определяется как длина промежутка времени после запроса услуги, в течение которого считается приемлемым предоставление этой услуги.

Можно трактовать приведенное выше определение по-другому. А именно, рассматривать MWT как период времени, в течение которого запрашиваемая услуга не устаревает. Иными словами, если после запроса услуга обеспечивается в течение слишком долгого времени, то может случиться так, что ее нельзя будет больше использовать. Заметим, что хотя приведенное выше определение и не выражено в терминах пользователей, запрашивающих услуги, может оказаться, что для данной услуги MWT будет различным для различных пользователей.

Дав определение MWT, мы можем теперь ввести точное определение угрозы ОВО, а именно, будем говорить, что имеет место угроза ОВО всякий раз, когда услуга с соответствующим максимальным временем ожидания (MWT) запрашивается зарегистрированным пользователем в момент времени t и не предоставляется этому пользователю к моменту времени (t + MWT).

При более тщательном рассмотрении угрозы ОВО и предложенного понятия MWT возникают некоторые вопросы. Например, угрозы ОВО можно полностью избежать, если определить MWT для всех услуг равным бесконечности. Однако этот подход не годится для тех случаев, когда величина MWT определяется некоторой значимой операционной характери-

стикой. Кроме того, значение MWT можно определить только для конкретного набора услуг, для которых оно необходимо, то есть можно определить некоторое подмножество активов системы как особенно критическое; тогда значения MWT будут соответствовать услугам, связанным с этими критическими активами.

6.7.2. Мандатная модель ОВО

Теперь опишем в общих чертах мандатную модель ОВО, включающую в себя некоторые характеристики моделей БЛМ и Биба. Система услуг, которая будет использоваться для представления этой модели ОВО, выражается в знакомых терминах субъектов и объектов, которые использовались для описания моделей БЛМ и Биба.

Субъектам системы соответствуют приоритеты, которые могут быть одинаковы, ниже или выше по сравнению с приоритетом любого другого субъекта. Объектам соответствуют степени критичности, имеющие аналогичную иерархическую структуру. Субъект может требовать услугу у вычислительной системы, запрашивая доступ к объектам системы. Говорят, что субъект получает отказ в обслуживании, если его запрос зарегистрирован, но не удовлетворен в течение соответствующего MWT.

При описании модели необходимо рассмотреть условия, при которых один субъект может отказать в обслуживании другому субъекту. Такой отказ может быть вполне приемлем для одних случаев и совершенно не допустим для других. Например, администратор может иметь вполне подходящее оправдание, отказывая зарегистрированному пользователю в обслуживании, а нарушитель, как правило, не должен иметь такого оправдания. Правила, составляющие модель, нацелены на то, чтобы определить условия, при которых отказ в обслуживании был бы недопустим.

Рассмотрим правила, описывающие мандатную модель ОВО. Эти правила описывают взаимоотношения субъектов, аналогичные отношениям между субъектами и объектами в моделях БЛМ и Биба.

Первое правило – «никаких отказов вверх» (NDU) – основано на том наблюдении, что никаким объектам с более низким приоритетом не позволено отказывать в обслуживании субъектам с более высокими приоритетами. Однако некоторым субъектам с более высоким приоритетом (например, администраторам системы) должна предоставляться возможность отказывать в обслуживании объектам с более низким приоритетом, если первые того желают.

Второе правило представляет собой альтернативу, которую можно использовать в тех приложениях, для которых защищенным от угроз отказа в обслуживании должно быть лишь некоторое подмножество объектов. Таким образом, это правило учитывает то, что проблема отказа в обслу-

живании может стоять только для объектов из некоторого конкретно определенного множества.

Это более общее правило требует, чтобы субъекты с более низкими приоритетами не препятствовали запросам услуг субъектов с более высокими приоритетами, производимыми через объекты из некоторого конкретно определенного множества. Это множество, которое мы обозначим через С, обычно содержит те объекты, которые являются наиболее критическими и для которых предоставляемые услуги никогда не должны устаревать.

Второе правило NDU(C) утверждает, что ни один субъект не может отказать запросам, сделанным субъектом с более высоким приоритетом через объекты из множества С. Второе правило особенно полезно для вычислительных систем, в которых необходимо обеспечивать защиту ОВО только для выбранного множества критических услуг. Например, система, выполняющая некоторую определенную роль, может содержать лишь небольшое множество услуг, напрямую связанных с этой ролью. В результате защиту ОВО с использованием правила NDU(C) можно обеспечить только для этих критических услуг. Это значительно сократит стоимость и трудность реализации стратегии ОВО.

Главным преимуществом двух представленных правил ОВО является то, что они дают средство для предотвращения отказа в обслуживании на основе понятия приоритета, предположительно уже существующего для данной системы. Например, для большинства операционных систем существует понятие приоритета процессов. Данные правила также являются гибкими в том смысле, что их легко можно приспособить к данной системе.

Недостаток этих правил заключается в том, что они имеют смысл только для систем, в которых можно определить несколько приоритетов. Если это не так, тогда должны быть определены подходящие аналогичные правила внутри уровня с одним приоритетом.

Данную модель, также как и модель КВМ, сложно реализовать для реальных систем.

ВОПРОСЫ К ЧАСТИ 1

1. Какие исторические события можно связать с понятием «нарушение информационной безопасности»?
2. Перечислите виды компьютерных преступлений.
3. Какие руководящие документы существуют в области информационной безопасности?
4. Какие стандарты и спецификации информационной безопасности вы знаете?
5. Перечислите принципы, используемые в законе РФ «О государственной тайне».
6. Приведите список угроз безопасности информационной системы.
7. Приведите список мер противодействия угрозам информационной безопасности.
8. Выделите основную структуру требований Оранжевой книги.
9. В чем заключается различие классов безопасности по Оранжевой книге?
10. Сколько классов безопасности выделяется в Оранжевой книге?
11. Что является целью информационной безопасности согласно стандарта BS 7799?
12. Что является основой процесса управления согласно стандарта BS 7799-2?
13. По каким параметрам происходит выделение классов в Гармонизированных критериях?
14. В чем суть Общих критериев?
15. Перечислите стандарты информационной безопасности, действующие на территории РФ.
16. Перечислите известные вам технические спецификации.
17. Какие требования предъявляются к моделям безопасности?
18. Приведите классификацию моделей безопасности.
19. В чем заключается смысл правил модели БЛМ?
20. Перечислите достоинства и недостатки моделей предоставления прав.
21. Какие модели, построенные на основе принципов теории информации, вам известны?
22. В чем заключается принцип действия, заложенный в вероятностную модель с полным перекрытием?
23. Перечислите правила модели целостности Биба.
24. Перечислите виды моделей целостности Биба.
25. Какие понятия использует модель ОВО?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Алешин И.В. Информационно-безопасные системы. Анализ проблемы. – СПб.: Изд-во СПбГТУ, 1996.

2. Гаухман Л.Д., Максимов С.В. Уголовно-правовая охрана финансовой среды: новые виды преступлений и их классификация: Научно-практическое пособие. – М.: ЮрИнфоР, 1995.

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

4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия. – Телеком, 2000. – 452 с.

5. Панфилова Е.П. Компьютерные преступления / Под общ. ред. Б.В. Волжеккина. – М., 1999.

6. Поляк-Брагинский А.В. Сеть своими руками. – СПб.: BHV-Петербург, 2002.

7. Ярочкин В.И., Халяпин Д.В. Основы защиты информации. Службы безопасности предприятия. ИПКИР. – М., 1993.

8. Доктрина информационной безопасности РФ // Российская газета. – 2000. – 28 сент.

9. О государственной тайне: Закон РФ от 21 июля 1993 г. // Закон. – 1999. – № 2.

10. О безопасности: Закон РФ от 5 марта 1992 г. // Ведомости съезда народных депутатов РФ и Верховного Совета РФ. – 1992. – № 15.

11. Об информации, информатизации и защите информации: Федеральный закон от 20 февраля 1995 г. // СЗ РФ. – 1995. – № 8.

12. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. // СЗ. – 1995. – № 33.

13. Об участии в международном информационном обмене: Федеральный закон от 4 июня 1996 г. // СЗ РФ. – 1996. – № 28.

14. О внесении изменений и дополнений в Закон РФ «О правовой охране программ для ЭВМ и баз данных»: Федеральный закон от 24 декабря 2002 г. // Российская газета. – 2002. – 28 дек.

15. О Перечне сведений, отнесенных к государственной тайне: Указ Президента РФ № 61 от 24 января 1998 г. // Российская газета. – 1998. – 3 февр.

16. О Перечне сведений конфиденциального характера: Указ Президента РФ № 188 от 6 марта 1997 г. // Закон. – 1998. – № 2.

17. О правовой охране программ для ЭВМ и баз данных: Закон РФ от 23 сентября 1992 г. // СЗ РФ. – 1992. – № 42.

18. Принципы безопасности банка и банковского бизнеса в России. – М.: Банковский Деловой Центр, 1997.

19. Уголовный кодекс РФ. – М., 2001.

20. Арсентьев М.В. К вопросу о понятии «информационная безопасность» // Информационное общество. – 1997. – № 4-6.

21. Дозорцев В.А. Информация как объект исключительного права // Дело и Право. – 1996. – № 4.

22. Статьев В.Ю., Тиньков В.А. Информационная безопасность распределенных информационных систем // Информационное общество. – 1997. – № 1.

23. Феоктистов Г.Г. Информационная безопасность общества // Социально-политический журнал. – 1996. – № 5.

24. Урсул А.Д. Информационная стратегия и безопасность в концепции устойчивого развития // Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 1996. – № 1.

ПРИЛОЖЕНИЯ

Приложение 1

Перечень книг радужной серии

Код книги	**Название**	**Дата выхода**	**Цвет**
5200.28-STD	*DoD Trusted Computer System Evaluation Criteria*	15 Aug 1983	Orange Book.
CSC-STD-002-85	*DoD Password Management Guideline*	12 Apr 1985	Green Book.
CSC-STS-003-85	*Guidance for applying TCSEC in Specific Environments*	25 Jun 1985	Yellow Book.
NCSC-TG-001	*A Guide to Understanding Audit in Trusted Systems*	1 Jun 1988	Tan Book.
NCSC-TG-002	*Trusted Product Security Evaluation Program*	22 Jun 1990	Bright Blue Book.
NCSC-TG-003	*Discretionary Access Control in Trusted Systems*	30 Sep 1987	Neon Orange Book
NCSC-TG-004	*Glossary of Computer Security Terms*	21 Oct 1988	Aqua Book
NCSC-TG-005	*Trusted Network Interpretation*	31 Jul 1987	Red Book
NCSC-TG-006	*Configuration Management in Trusted Systems*	28 Mar 1988	Amber Book

Продолжение прил. 1

Код книги	**Название**	**Дата выхода**	**Цвет**
NCSC-TG-007	*A Guide to Understanding Design Documentation in Trusted Systems*	6 Oct 1988	Burgundy Book
NCSC-TG-008	*A Guide to Understanding Trusted Distribution in Trusted Systems*	15 Dec 1988	Dark Lavender Book
NCSC-TG-009	*Computer Security Subsystem Interpretation of the TCSEC*	16 Sep 1988	Venice Blue Book
NCSC-TG-010	*A Guide to Understanding Security Modeling in Trusted Systems*	October 1992	Aqua Book
NCSC-TG-011	*Trusted Network Interpretation Environments Guideline (TNI)*	1 August 1990	Red Book
NCSC-TG-013 V2	*RAMP Program Document*	1 March 1995	Pink Book
NCSC-TG-014	*Guidelines for Formal Verification Systems*	1 Apr 1989	Purple Book
NCSC-TG-015	*Guide to Understanding Trusted Facility Management*	18 Oct 1989	Brown Book
NCSC-TG-016	*Guidelines for Writing Trusted Facility Manuals*	October 1992	Yellow-Green Book

Продолжение прил. 1

Код книги	**Название**	**Дата выхода**	**Цвет**
NCSC-TG-017	*Identification and Authentication in Trusted Systems*	September 1991	Light Blue Book
NCSC-TG-018	*Object Reuse in Trusted Systems*	July 1992	Light Blue Book
NCSC-TG-019	*Trusted Product Evaluation Questionnaire*	2 May 1992	Blue Book
NCSC-TG-020	*Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the UNIX System*	7 July 1989	(Silver Book)
NCSC-TG-021	*Trusted Database Management System Interpretation of the TCSEC (TDI)*	April 1991	(Purple Book)
NCSC-TG-022	*Trusted Recovery in Trusted Systems*	30 December 1991	(Yellow Book)
NCSC-TG-023	*Security Testing and Test Documentation in Trusted Systems*		(Bright Orange Book)
NCSC-TG-024 Vol. 1/4	*Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements*	December 1992	(Purple Book)

Окончание прил. 1

Код книги	**Название**	**Дата выхода**	**Цвет**
NCSC-TG-024 Vol. 2/4	*Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work*	30 June 1993	(Purple Book)
NCSC-TG-024 Vol. 3/4	*Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description*	28 February 1994	(Purple Book)
NCSC-TG-024 Vol. 4/4	*Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document*	Publication TBA	(Purple Book)
NCSC-TG-025	*Guide to Understanding Data Remanence in Automated Information Systems.*	September 1991	Forest Green Book
NCSC-TG-026	*Writing the Security Features User's Guide for Trusted Systems*	September 1991	(Hot Peach Book)
NCSC-TG-027	*Information System Security Officer Responsibilities for Automated Information Systems*	May 1992	(Turquoise Book)
NCSC-TG-028	*Assessing Controlled Access Protection*	25 May 1992	(Violet Book)
NCSC-TG-029	*Certification and Accreditation Concepts*	January 1994	(Blue Book)
NCSC-TG-030	*Covert Channel Analysis of Trusted Systems*	November 1993	Light Pink Book

Приложение 2

Базовые требования Оранжевой книги

Базовые требования «Оранжевой книги»	Классы защищенности					
	C1	C2	B1	B2	B3	A1
Политика безопасности						
1. Дискреционная политика безопасности	+	+	+	=	=	=
2. Мандатная политика безопасности	-	-	+	+	=	=
3. Метка секретности	-	-	+	+	=	=
4. Целостность меток	-	-	+	=	=	=
5. Рабочие метки	-	-	-	+	=	=
6. Повторение меток	-	-	+	=	=	=
7. Освобождение ресурсов при повторном использовании объектов	-	+	=	+	=	=
8. Изолирование модулей	-	+	=	=	=	=
9. Пометка устройств ввода/вывода	-	-	+	=	=	=
10. Пометка читаемого вывода	-	-	+	=	=	=
Подотчетность						
11. Идентификация и аутентификация	+	+	=	=	=	=
12. Аудит	-	+	+	+	+	=
13. Защищенный канал (доверенный путь)	-	-	-	+	=	=
Гарантии						
14. Проектная спецификация и верификация	-	-	+	+	+	+
15. Системная архитектура	+	=	=	+	+	=
16. Целостность системы	+	=	=	=	=	=
17. Тестирование системы безопасности	+	+	+	+	+	=
18. Доверенное восстановление после сбоев	-	-	-	-	+	=
19. Управление конфигурацией системы	-	-	-	+	+	+
20. Доверенное дооснащение системы	-	-	-	+	+	=
21. Доверенное распространение	-	-	-	-	+	=
22. Анализ скрытых каналов	-	-	-	+	+	+
Документация						
23. Руководство пользователя	+	=	=	=	=	=

Продолжение прил. 2

Базовые требования «Оранжевой книги»	Классы защищенности					
	C1	C2	B1	B2	B3	A1
24. Руководство по конфигурированию системы защиты	+	+	+	+	+	=
25. Документация по тестированию	+	=	=	=	=	+
26. Проектная документация	+	=	+	+	=	+
«-» – нет требований к данному классу «+» – новые или дополнительные требования «=» – требования совпадают с требованиями к СВТ предыдущего класса						

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

ГЛАВА 1. ПОНЯТИЕ И ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 6

ГЛАВА 2. ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 14

ГЛАВА 3. ОЦЕНОЧНЫЕ СТАНДАРТЫ 22
3.1. Критерии оценки доверенных компьютерных систем Министерства обороны США 22
3.2. Стандарт BS 7799-1 34
3.2.1. Регуляторы безопасности и реализуемые ими цели 33
3.2.1.1. Регуляторы общего характера 35
3.2.1.2. Регуляторы технического характера 37
3.2.1.3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия 40
3.3. Стандарт BS 7799-2. Четырехфазная модель процесса управления информационной безопасностью 43
3.4. Сведения о других международных стандартах 45
3.5. Сведения о стандартах на территории России 48

ГЛАВА 4. ТЕХНИЧЕСКИЕ СПЕЦИФИКАЦИИ 51

ГЛАВА 5. ПОЛИТИКА БЕЗОПАСНОСТИ 54
5.1. Формальная и неформальная политики безопасности 54
5.1.1. Неформальная политика безопасности 54
5.1.2. Формальная политика безопасности 55

ГЛАВА 6. МОДЕЛИ БЕЗОПАСНОСТИ. 58
6.1. Основные понятия 58
6.2. Классификация моделей безопасности 62
6.2.1. Модели безопасности, предотвращающие угрозу раскрытия 63
6.2.2. Модели разграничения доступа, построенные по принципу предоставления прав 63
6.2.3. Достоинства и недостатки моделей предоставления прав 73
6.3. Информационные модели 73
6.3.1. Модель невмешательства 74
6.3.2. Модель невыводимости 75
6.4. Вероятностные модели 75
6.4.1. Игровая модель 76

6.4.2. Модель с полным перекрытием 76
6.5. Модели контроля целостности 78
6.5.1. Модель Биба 78
6.5.1.1. Мандатная модель целостности Биба 77
6.5.2. Модель понижения уровня субъекта 80
6.5.3. Модель понижения уровня объекта 80
6.6. Модель Кларка-Вилсона 81
6.6.1. Правила модели МКВ 82
6.7. Модели, предотвращающие угрозу отказа служб 84
6.7.1. Основные понятия ОВО 85
6.7.2. Мандатная модель ОВО 86

ВОПРОСЫ К ЧАСТИ 1 88

БИБЛИОГРАФИЧЕСКИЙ СПИСОК 87

ПРИЛОЖЕНИЯ 89

Учебное издание

Блинов Алексей Михайлович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Часть 1

Редактор М.В. Манерова

Подписано в печать 17.09.10. Формат 60x84 1/16.
Усл. печ. л. 6,0. Тираж 150 экз. Заказ 427. РТП изд-ва СПбГУЭФ.

Издательство СПбГУЭФ. 191023, Санкт-Петербург, Садовая ул., д. 21.