

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 1 (56) / 1998

**Информационная безопасность в России:
опыт составления карты (стр. 4)**

**Общие критерии оценки безопасности
информационных технологий
и перспективы их использования (стр. 12)**

**Обновление семейства
Ultra-компьютеров (стр. 18)**

**ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ**



Аппаратно-программный комплекс “Межсетевой экран Застава-Джет” сертифицирован Гостехкомиссией России

12 января 1998 года Государственная техническая комиссия при Президенте Российской Федерации завершила сертификацию межсетевого экрана “Застава-Джет”, присвоив ему второй класс защищенности в

соответствии с Руководящим документом, утвержденным в июле 1997 года. Копия сертификата приведена на с. 3.

“Застава-Джет” — это современный комплексный межсетевого экран, разработанный

на основе продукта Gauntlet компании Trusted Information Systems.

Общая схема подключения межсетевого экрана “Застава-Джет” приведена на рис. 1.

В состав комплекса “Застава-Джет” входят следующие программные компоненты:

- фильтры сетевых пакетов;
- шлюзы прикладного уровня;
- средства идентификации и аутентификации;
- средства регистрации и учета;
- средства сигнализации о попытках несанкционированного доступа;
- средства контроля действий администратора межсетевого экрана;
- средства динамического контроля целостности программной информационной среды МЭ;
- средства резервного копирования и восстановления



Рис. 1. Общая схема подключения межсетевого экрана “Застава-Джет”.

и некоторые другие. Схема взаимодействия основных частей межсетевого экрана представлена на рис. 2.

Дополнительной особенностью МЭ «Застава» является обеспечение отказоустойчивости путем зеркалирования информации и ПО на файловых системах межсетевого экрана.

Применение “Застава-Джет” в комплексе с другими средствами информационной безопасности позволяет защитить информационные системы организаций, имеющие выход в открытые сети, такие как Интернет. Это значит, что можно пользоваться многочисленными информационными ресурсами и современными коммуникационными средствами, не подвергаясь опасности внешнего вторжения.

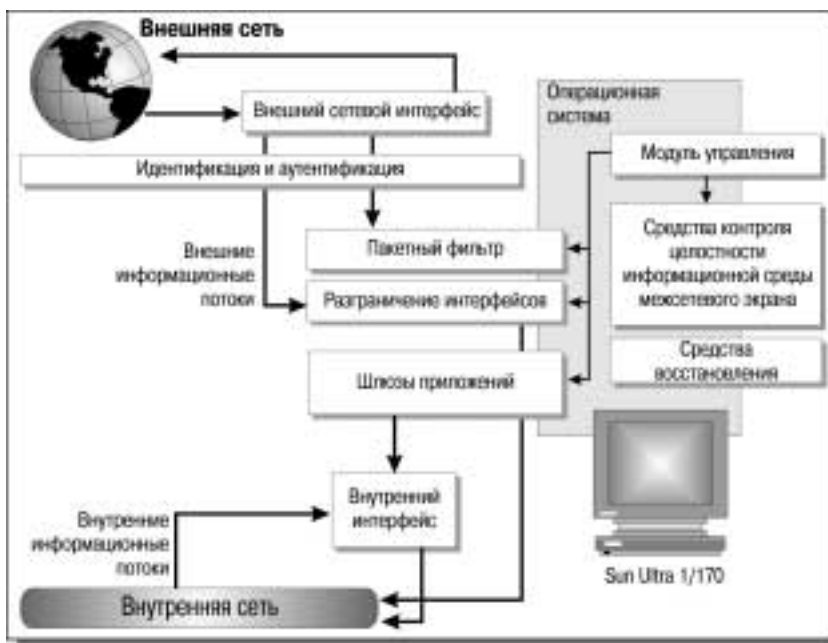


Рис. 2. Схема взаимодействия компонент межсетевого экрана “Застава-Джет”.

**ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU. 0001. 01БИ00**



СЕРТИФИКАТ

№ 146

Выдан 14 января 1998 г.
Действителен до 14 января 2001 г.

Настоящий Сертификат удостоверяет, что единичный экземпляр **аппаратно-программного комплекса «Межсетевой экран Застава-Джет»** (аппаратный комплекс - заводской номер 551F14D4, программный продукт - идентификационный номер МЭЗ 0001.97), разработанного АОЗТ «Инфосистемы ДЖЕТ» г.Москва (технические условия от 10.12.97 г. № 0197), функционирующий под управлением ОС Solaris 2.5.1, является программно-техническим средством защиты от несанкционированного доступа к информации и соответствует требованиям Руководящего документа Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 2 классу защищенности при выполнении «Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам» и аттестации по требованиям безопасности информации рабочих мест защищаемой локальной вычислительной сети.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией «Центр безопасности информации» (аттестат аккредитации от 23.05.97 г. № СЗИ RU.117.Б08.025), протокол испытаний от 25.12.97 г.

Заявитель – АОЗТ «Инфосистемы Джет»
Адрес - 103006, Москва, ул.Краснопролетарская, д.6
Тел. (095) 973-48-48

Инспекционный контроль соответствия аппаратно-программного комплекса «Межсетевой экран Застава-Джет» требованиям нормативных документов Гостехкомиссии России и техническим условиям осуществляется испытательной лабораторией «Центр безопасности информации».

**ПЕРВЫЙ ЗАМЕСТИТЕЛЬ
ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ**



Е.А.Беляев

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 14 января 1998 г.

Информационная безопасность в России: опыт составления карты

Владимир Бетелин, член-корреспондент РАН,
Владимир Галатенко



Содержание

1. Введение
2. Основные определения
3. Грани информационной безопасности
4. Доступность, целостность, конфиденциальность
5. Законодательный, административный, процедурный, программно-технический уровни
6. Заключение

1. Введение

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю — национальном, отраслевом, корпоративном или персональном. Для иллюстрации этого положения ограничимся одним примером.

Согласно распоряжению президента США Клинтона (15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических угроз, так и от атак, проводимых с помощью информационного оружия. В начале октября 1997 года, при завершении подготовки доклада президенту, Роберт Марш, глава вышеупомянутой комиссии, заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.

На наш взгляд, нет оснований предполагать, что Россия обладает большей защищенностью.

В данной работе мы попытаемся составить карту, характеризующую состояние основных аспектов информационной безопасности в России. Нас будут интересовать как уже освоенные области, так и "белые пятна", незаслуженно обойденные вниманием.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать ее специфику, состоящую в том, что информационная безопасность есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, регламенты, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

2. Основные определения

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Из этого довольно очевидного положения можно вывести два важных для нас следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты.
- Информационная безопасность не сводится исключительно к защите информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита информации стоит по важности отнюдь не на первом месте.

3. Грани информационной безопасности

Информационная безопасность — многогранная, можно сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход. В этом разделе мы укажем важнейшие на наш взгляд грани.

Спектр интересов субъектов, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

Эти категории будут рассмотрены в разделе 4.

Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного (законы, нормативные акты, стандарты и т.п.);
- административного (действия общего характера, предпринимаемые руководством организации);
- процедурного (конкретные меры безопасности, имеющие дело с людьми);
- программно-технического (конкретные технические меры).

Перечисленные уровни мы рассмотрим в разделе 5.

Таковы два основных, на наш взгляд, измерения, задающие систему координат в пространстве информационной безопасности. У информационной безопасности есть и другие грани, но, чтобы чрезмерно не усложнять карту, мы оставим ее двумерной.

4. Доступность, целостность, конфиденциальность

4.1. Доступность

Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления — производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей. Имеются в виду продажа железнодорожных и авиабилетов, банковские услуги и т.п.

Важность доступности как аспекта информационной безопасности находится в разительном противоречии с тем вниманием, которое уделяют данному аспекту потенциально заинтересованные стороны. Если вопросы защиты от несанкционированного доступа (то есть обеспечение конфиденциальности и целостности информации) курирует Гостехкомиссия России, а криптографические средства (что опять-таки связано с обеспечением конфиденциальности и целостности) — ФАПСИ, то доступностью на государственном уровне не занимается пока никто. На законодательном уровне вопросы доступности затрагиваются только в новой редакции Уголовного кодекса (раздел IX — «Преступления против общественной безопасности», глава 28 — «Преступления в сфере компьютерной информации», статья 274 — «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»).

Авторам не известны отечественные аппаратно-программные продукты общего назначения, повышающие доступность систем (равно как и организации, занимающиеся разработкой таких продуктов). Имеющиеся зарубежные решения не везде применимы и весьма дороги, что существенно сужает круг возможных российских покупателей.

4.2. Целостность

Целостности повезло больше, чем доступности. Как уже отмечалось, различные аспекты целостности курируют ФАПСИ и Гостехкомиссия. Вышеупомянутая глава 28 УК предусматрива-

ет наказания за нарушение целостности. Есть отечественные продукты, обеспечивающие или контролирующие целостность.

В то же время, положение дел с целостностью далеко от идеала. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Пример области применения средств контроля динамической целостности — анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

4.3. Конфиденциальность

Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Отечественные аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить полное представление о потенциальных рисках и степени их серьезности. Во-вторых, авторам не известны отечественные аппаратные реализации шифраторов с достаточным быстродействием, что накладывает ограничения на виды и объемы шифруемой информации. Программные разработки охватывают лишь часть распространенных компьютерных платформ.

5. Законодательный, административный, процедурный, программно-технический уровни

5.1. Законодательный уровень

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Мы будем различать на законодательном уровне две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушениям информационной безопасности;
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

К первой группе следует отнести в первую очередь главу 28 ("Преступления в сфере компьютерной информации") раздела IX новой редакции Уголовного кодекса. Эта глава достаточно полно охватывает основные угрозы информационным системам, однако обеспечение практической реализуемости соответствующих статей пока остается проблематичным.

Закон "Об информации, информатизации и защите информации" можно причислить к этой же группе. Правда, положения этого закона носят весьма общий характер, а основное содержание статей, посвященных информационной безопасности, сводится к необходимости использовать исключительно сертифицированные средства, что, в общем, правильно, но далеко не достаточно.

Насколько можно судить по планам Государственной Думы, готовятся законы "О праве на информацию", "О коммерческой тайне", "О персональных данных". Это, безусловно, шаги в правильном направлении, так как делается попытка охватить все категории субъектов информационных отношений.

К группе направляющих и координирующих законов и нормативных актов относится целая группа документов, регламентирующих процессы лицензирования и сертификации в области информационной безопасности. Главная роль здесь отведена Федеральному агентству правительственной связи и информации (ФАПСИ) и Государственной технической комиссии (Гостехкомиссии) при Президенте Российской Федерации.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи очень важны Руководящие документы Гостехкомиссии, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно выделим утвержденный в июле 1997 года Руководящий документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

Как уже указывалось, самое важное на законодательном уровне — создать механизм, позволяющий согласовать процесс разработки зако-

нов с реалиями и прогрессом информационных технологий. Конечно, законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности. Пока, пожалуй, только Гостехкомиссия России демонстрирует способность динамично развивать нормативную базу.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Мы хотели бы обратить особое внимание на желательность приведения российских стандартов и сертификационных нормативов в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть много причин, по которым это должно быть сделано. Одна из них — необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских организаций. Вторая (более существенная) — доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен получить реалистичное решение вопрос об отношении к таким изделиям. Здесь необходимо разделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь военных) в принципе может представлять угрозу национальной безопасности (в том числе информационной), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно является сложной, однако, как показывает опыт европейских стран, она может быть успешно решена. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо снижения национальной безопасности.

Главное же, чего, на наш взгляд, не хватает современному российскому законодательству (и что можно почерпнуть из зарубежного опыта), это позитивной (не карательной) направленности. Информационная безопасность — это новая область деятельности, здесь важно научить, разъяснить, помочь, а не запретить и наказать. Общество должно осознать важность данной проблематики, понять основные пути решения соответствующих задач, должны быть скоординированы научные, учебные и производственные планы. Государство может сделать это оптимальным образом. Здесь не нужно больших материальных затрат, требуются интеллектуальные вложения.

Пример позитивного законодательства — Британский стандарт BS 7799:1995, описывающий основные положения политики безопасности (в следующем разделе мы разъясним этот термин). Более 60% крупных организаций используют этот стандарт в своей практике, хотя закон, строго говоря, этого не требует. Еще один пример — Computer Security Act (США), возлагающий на конкретные государственные структуры ответственность за методическую поддержку работ в области информационной безопасности. Со времени вступления этого закона в силу (1988 год) действительно было разработано много важных и полезных документов.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- ориентация на созидательные, а не карательные законы;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

5.2. Административный уровень

Основной мер административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;

- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Административный уровень — белое пятно в отечественной практике информационной безопасности. Нет законов, обязывающих организации иметь политику безопасности. Ни одно из ведомств, курирующих информационную безопасность, не предлагает типовых разработок в данной области. Ни одно учебное заведение не готовит специалистов по составлению политики безопасности. Мало кто из руководителей знает, что такое политика безопасности, еще меньшее число организаций такую политику имеют. В то же время, без подобной основы прочие меры информационной безопасности повисают в воздухе, они не могут быть всеобъемлющими, систематическими и эффективными. Например, меры защиты от внешних хакеров и от собственных обиженных сотрудников должны быть совершенно разными, поэтому в первую очередь необходимо определиться, какие угрозы чреватые нанесением наибольшего ущерба. (Отметим в этой связи, что по статистике

наибольший ущерб происходит от случайных ошибок персонала, обусловленных неаккуратностью или некомпетентностью, поэтому в первую очередь важны не хитрые технические средства, а меры обучения, тренировка персонала и регламентирование его деятельности.)

Разработка политики безопасности требует учета специфики конкретных организаций. Бесмысленно переносить практику режимных государственных организаций на коммерческие структуры, учебные заведения или персональные компьютерные системы. В этой области целесообразно предложить, во-первых, основные принципы разработки политики безопасности, а, во-вторых, — готовые шаблоны для наиболее важных разновидностей организаций.

Анализ ситуации на административном уровне информационной безопасности еще раз показывает важность созидательного, а не карательного законодательства. Можно потребовать от руководителей наличия политики безопасности (и в перспективе это правильно), но сначала нужно разъяснить, научить, показать, для чего она нужна и как ее разрабатывать.

5.3. Процедурный уровень

К процедурному уровню относятся меры безопасности, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, и поэтому нуждаются в существенном пересмотре.

Можно выделить следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Управление персоналом в контексте информационной безопасности является в России белым пятном. Во-первых, для каждой должности должны существовать квалификационные требования по информационной безопасности. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и оттренировать выполнение этих мер практически (и проводить подобные тренировки дважды в год).

Без всякого преувеличения, нужна информационная гражданская оборона. Спокойно, без нагнетания страстей, нужно разъяснять обществу не только преимущества, но и опасности, вытекающие

из использования информационных технологий. Акцент, на наш взгляд, следует делать не на военной или криминальной стороне дела, а на чисто гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

Разумеется, разделы, касающиеся информационной безопасности, должны стать частью школьных и, тем более, ВУЗовских курсов информатики.

Меры физической защиты, известные с давних времен, нуждаются в доработке в связи с распространением сетевых технологий и миниатюризацией вычислительной техники. Прежде всего, следует защититься от утечки информации по техническим каналам. Этим занимается Гостехкомиссия России.

Поддержание работоспособности — еще одно белое пятно, образовавшееся сравнительно недавно. В эпоху господства больших ЭВМ удалось создать инфраструктуру, способную обеспечить по существу любой наперед заданный уровень работоспособности (доступности) на всем протяжении жизненного цикла информационной системы. Эта инфраструктура включала в себя как технические, так и процедурные регуляторы (обучение персонала и пользователей, проведение работ в соответствии с апробированными регламентами и т.п.). При переходе к персональным компьютерам и технологии клиент/сервер инфраструктура обеспечения доступности во многом оказалась утраченной, однако важность данной проблемы не только не уменьшилась, но, напротив, существенно возросла. Перед государственными и коммерческими организациями стоит задача соединения упорядоченности и регламентированности, присущих миру больших ЭВМ, с открытостью и гибкостью современных систем.

Реагирование на нарушения информационной безопасности — снова белое пятно. Допустим, пользователь или системный администратор понял, что имеет место нарушение. Что он должен делать? Попытаться проследить злоумышленника? Немедленно выключить оборудование? Позвонить в милицию? Проконсультироваться со специалистами ФАПСИ или Гостехкомиссии? Ни одно ведомство, причастное к информационной безопасности, не предложило регламента действий в подобной экстремальной ситуации или своей консультационной помощи. Необходимо организовать национальный центр информационной безопасности, в круг обязанностей которого входило бы, в частности, отслеживание современного состояния этой области знаний, информирование пользователей всех уровней о появлении новых угроз и мерах противодействия, оперативная помощь организациям в случае нарушения их информационной безопасности.

Планирование восстановительных работ и вся проблематика, связанная с восстановлением работоспособности после аварий, также является белым пятном. А ведь ни одна организация от таких нарушений не застрахована. Здесь необходимо отработать действия персонала во время и после аварий, заранее позаботиться об организации резервных производственных площадок, отработать процедуру переноса на эти площадки основных информационных ресурсов, а также процедуру возвращения и нормальному режиму работы. Подчеркнем, что подобный план нужен не только сверхважным военным организациям, но и обычным коммерческим компаниям, если они не хотят понести крупные финансовые потери.

5.4. Программно-технический уровень

Львиная доля активности в области информационной безопасности приходится на программно-технический уровень. Если иметь в виду зарубежные продукты, здесь существует полный спектр решений. Если ограничиться разработками, имеющими российские сертификаты по требованиям безопасности, картина получается существенно более разреженной.

Согласно современным воззрениям, в рамках информационных систем должны быть доступны по крайней мере следующие механизмы безопасности:

- идентификация и проверка подлинности (аутентификация) пользователей;
- управление доступом;
- протоколирование и аудит;
- криптография;
- (межсетевое) экранирование;
- обеспечение высокой доступности.

Кроме того, информационной системой в целом и механизмами безопасности в особенности необходимо управлять. И управление, и механизмы безопасности должны функционировать в разнородной, распределенной среде, построенной, как правило, в архитектуре клиент/сервер. Это означает, что упомянутые средства должны:

- опираться на общепринятые стандарты;
- быть устойчивыми к сетевым угрозам;
- учитывать специфику отдельных сервисов.

В соответствии с действующим в России порядком, за идентификацию/аутентификацию, управление доступом, протоколирование/аудит отвечает Гостехкомиссия России, за криптографию — ФАПСИ, межсетевое экранирование является спорной территорией, доступностью не занимается никто.

На сегодняшний день подавляющее большинство разработок ориентировано на платформы Intel/DOS/Windows. В то же время, наиболее значимая информация концентрируется на иных, серверных платформах. В защите нуждаются не отдельные персональные компьютеры, не только локальные сети на базе таких компьютеров, но, в первую очередь, существенно более продвинутые современные корпоративные системы. Пока для этого почти нет сертифицированных средств.

Рассмотрим типичную государственную организацию, имеющую несколько производственных площадок, на каждой из которых могут находиться критически важные серверы, в доступе к которым нуждаются работники, базирующиеся на других площадках, и мобильные пользователи. В число поддерживаемых информационных сервисов входят файловый и почтовый сервисы, системы управления базами данных (СУБД), Web-сервис и т.д. В локальных сетях и при межсетевом

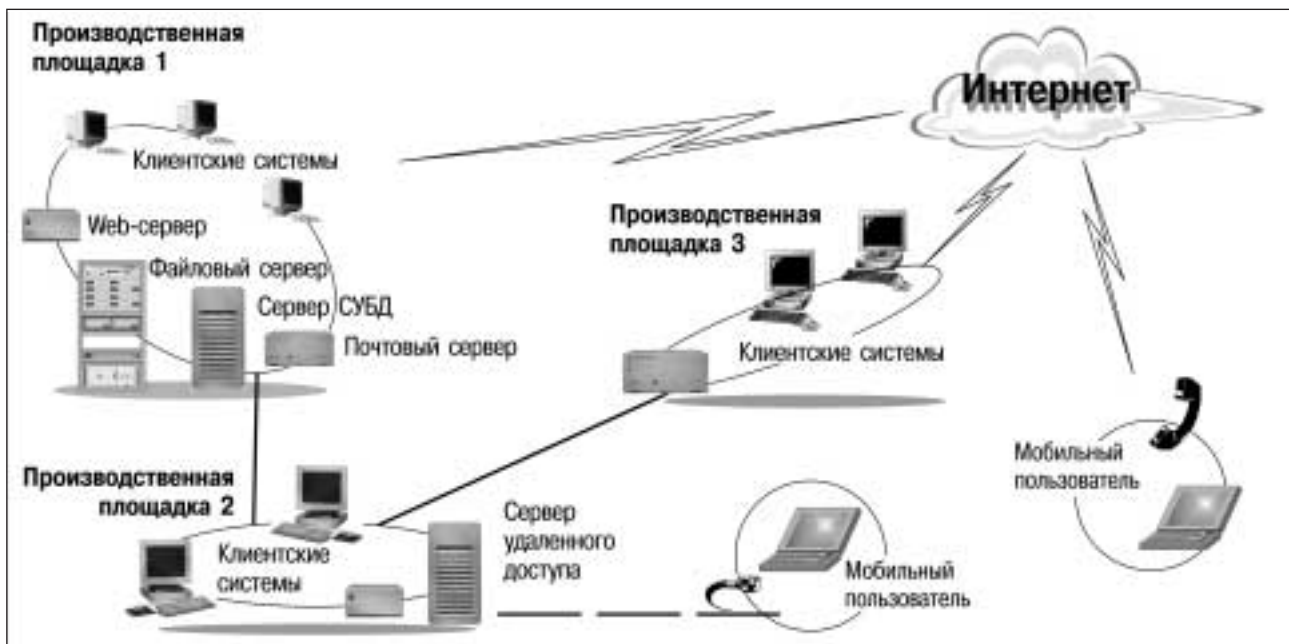


Рис. 1. Информационная система типичной государственной организации.

	Доступность	Целостность	Конфиденциальность
законодательный уровень	1	2	3
административный уровень	0	0	1
процедурный уровень	0	1	2
программно-технический уровень	0	1	2

Табл. 1. Оценка положения дел в информационной безопасности России.

доступе основным является протокол TCP/IP. Схематически информационная система такой организации представлена на рис. 1.

Для построения эшелонированной обороны подобной информационной системы необходимы по крайней мере следующие защитные средства программно-технического уровня:

- межсетевые экраны (разграничение межсетевого доступа);
- средства поддержки частных виртуальных сетей (реализация защищенных коммуникаций между производственными площадками по открытым каналам связи);
- средства идентификации/аутентификации, поддерживающие концепцию единого входа в сеть (пользователь один раз доказывает свою подлинность при входе в сеть организации, после чего получает доступ ко всем имеющимся сервисам в соответствии со своими полномочиями);
- средства протоколирования и аудита, отслеживающие активность на всех уровнях — от отдельных приложений до сети организации в целом, оперативно выявляющие подозрительную активность;
- комплекс средств централизованного администрирования информационной системы организации;
- средства защиты, входящие в состав приложений, сервисов и аппаратно-программных платформ.

На момент написания статьи из интересующего нас спектра продуктов были сертифицированы по требованиям безопасности для применения в госорганизациях ряд межсетевых экранов, операционных систем и реляционных СУБД. Даже если включить в этот перечень продукты, сертифицированные ФАПСИ для применения в коммерческих организациях (систему "ШИП", поддерживающую виртуальные частные сети, и средства криптографической защиты семейства "Верба"), большинство рубежей остается без защиты.

Таким образом, на сегодняшний день государственная организация не может получить современную информационную систему, защищенную сертифицированными средствами.

Коммерческие структуры, в отличие от госорганизаций, в определенной степени свободнее в своем выборе защитных средств. Тем не менее, в силу целого ряда обстоятельств (необходимость взаимодействия с госструктурами, расширительная трактовка понятия гостайны — "гостайна по совокупности", необходимость получения лицензии на эксплуатацию криптосредств, ограничения на импорт криптосредств) эта свобода не слишком велика. Практически на все категории субъектов информационных отношений перенесен подход, рассчитанный на госструктуры.

6. Заключение

В предыдущих разделах мы описали двумерное пространство информационной безопасности. Представим результаты наших рассуждений в наглядной форме, расставив оценки (от 0 до 5), показывающие степень освоенности различных областей в соответствии с современными требованиями и действующим законодательством (табл. 1).

Информационная безопасность в России развивается крайне неравномерно. Есть давно освоенные области (законодательство о лицензировании и сертификации, программно-технические меры обеспечения конфиденциальности и статической целостности), но большая часть областей, в том числе критически важных, остается белым пятном. Даже на освоенных областях пока не удалось достичь соответствия современным требованиям. Все это позволяет оценить ситуацию с информационной безопасностью в России как крайне тяжелую. Позитивные перемены происходят очень медленно, так что общее отставание от современного уровня продолжает накапливаться.

В то же время, при правильной организации дела положение можно кардинально улучшить в короткие сроки. Объективно все заинтересованные стороны выиграют от проведения комплексного, современного подхода. Необходима, однако, государственная программа самого высокого уровня, координирующая, направляющая и контролирующая ход работ в области информационной безопасности.

Общие критерии оценки безопасности информационных технологий и перспективы их использования

Марк Кобзарь, Игорь Калайда
Центр безопасности информации

Содержание

- | | |
|--|------------------------------------|
| 1. Введение | |
| 2. Общие положения | 5. Предопределенные профили защиты |
| 3. Требования к функциям безопасности | 6. Заключение |
| 4. Требования гарантированности безопасности | 7. Литература |



1. Введение

Обеспечение безопасности информационных технологий (ИТ) невозможно без разработки соответствующих законодательных актов и нормативно-технических документов. Критерии оценки безопасности ИТ занимают среди них особое место. Только стандартизированные критерии позволяют проводить сравнительный анализ и сопоставимую оценку продуктов ИТ.

В настоящее время в России единственными нормативными документами по критериям оценки защищенности средств вычислительной техники и автоматизированных систем являются Руководящие документы (РД) Гостехкомиссии РФ [1-5], разработанные с учетом предшествующих основополагающих документов [10, 13].

Появление проекта международного стандарта "Общие критерии оценки безопасности информационных технологий" [16] является качественно новым этапом в развитии нормативной базы оценки безопасности ИТ.

Общие критерии (ОК) обобщили содержание и опыт использования Оранжевой книги [10], развили Европейские критерии [13], воплотили в реальные структуры концепцию типовых профилей защиты Федеральных критериев США [15].

В Общих критериях проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства Общих критериев — полнота и систематизация требований безопасности, гибкость в применении и открытость для последующего развития.

В разработке Общих критериев участвовали Национальный институт стандартов и технологий и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Голландия), Органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция).

В январе 1996 года была выпущена версия 1.0 Общих критериев, в 1997 году появились дополнительные материалы, в мае 1998 года ожидается появление версии 2.0.

2. Общие положения

Общие критерии разработаны таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, оценщиков и пользователей объекта оценки. Под объектом оценки (ОО) понимается аппаратно-программный продукт или информационная система. К таким объектам относятся, например, операционные системы, вычислительные сети, распределенные системы, прикладные программы.

К рассматриваемым в ОК аспектам безопасности относятся: защита от несанкционированного доступа, модификации или потери доступа к информации при воздействии угроз, являющихся результатом случайных или преднамеренных действий. Защищенность от этих трех типов угроз обычно называют конфиденциальностью, целостностью и доступностью.

Некоторые аспекты безопасности ИТ находятся вне рамок ОК:

- ОК не охватывают оценку административных мер безопасности;
- в ОК не рассматривается оценка технических аспектов безопасности ИТ типа побочных электромагнитных излучений;
- ОК формулируют только критерии оценки и не содержат методик самой оценки;
- в ОК не входят критерии для оценки криптографических методов защиты информации.

Общие критерии предполагается использовать как при задании требований к продуктам и системам ИТ, так и при оценке их безопасности на всех этапах жизненного цикла.

ОК состоят из следующих частей:

- Часть 1. "Представление и общая модель". Определяются общая концепция, принципы и цели оценки безопасности ИТ. Приведены категории специалистов, для которых ОК представляют интерес.
- Часть 2. "Требования к функциям безопасности". Приведены требования к функциям безопасности и определен набор показателей для оценки безопасности информационных технологий. Каталоги части 2 содержат наборы требований, сгруппированные в семейства и классы.
- Часть 3. "Требования гарантированности безопасности". Приведены требования к гарантиям безопасности, сгруппированные в семейства, классы и уровни. Определены также критерии оценки для Профилей защиты изаданий по безопасности.
- Часть 4. "Предопределенные профили защиты". Приведены примеры профилей защиты, включающих функциональные требования и требования гарантированности. Ряд подобных требований присутствовал в предшествующих критериях (ITSEC, STCPEC, FC, TCSEC), другие впервые представлены в данном документе. Предполагается, что в конечном счете часть 4 станет каталогом профилей защиты, которые прошли процесс регистрации.
- Часть 5 (планируется). "Процедуры регистрации". Определит процедуры регистрации профилей защиты и их поддержки в международном регистре.

Общий объем материалов версии 1.0 Общих критериев (включая приложения) составляет около 800 страниц.

В соответствии с концепцией ОК, требования к безопасности объекта оценки разделяются на две категории:

- функциональные требования;
- требования гарантированности.

В функциональных требованиях описаны те функции объекта оценки, которые обеспечивают безопасность ИТ. Имеются в виду требования идентификации, установления подлинности (аутентификации) пользователей, протоколирования и др.

Требования гарантированности отражают качества объекта оценки, дающие основание для уверенности в том, что необходимые меры безопасности объекта эффективны и корректно реализованы. Оценка гарантированности получается на основе изучения назначения, структуры и функционирования объекта оценки. Требования гарантированности включают требования к организации процесса разработки, а также требования поиска, анализа и воздействия на потенциально уязвимые с точки зрения безопасности места.

В ОК функциональные требования и требования гарантированности представлены в едином стиле.

Термин "класс" используется для наиболее общей группировки требований безопасности.

Члены класса названы семействами. В семейства группируются наборы требований, которые обеспечивают выполнение определенной части целей безопасности и могут отличаться по степени жесткости.

Члены семейства называются компонентами. Компонент описывает минимальный набор требований безопасности для включения в структуры, определенные в ОК.

Компоненты построены из элементов. Элемент — самый нижний, неделимый уровень требований безопасности.

Организация требований безопасности в ОК по иерархии класс — семейство — компонент — элемент помогает определить нужные компоненты после идентификации угроз безопасности объекта оценки.

Между компонентами могут существовать зависимости. Они возникают, когда компонент недостаточен для выполнения цели безопасности и необходимо наличие другого компонента. Зависимости могут существовать как между функциональными компонентами, так и компонентами гарантированности.

Компоненты могут быть конкретизированы с помощью разрешенных действий для обеспечения выполнения определенной политики безопасности или противостояния определенной угрозе. К разрешенным действиям относятся назначение, выбор и обработка.

Назначение позволяет заполнить спецификацию идентифицированного параметра при использовании компонента. Параметр может быть признаком или правилом, которое конкретизирует требование к определенной величине или диапазону величин. Например, элемент функционального компонента может требовать, чтобы данное действие выполнялось неоднократно. В этом случае назначение обеспечивает число или диапазон чисел, которые должны использоваться в параметре.

Выбор — это выбор одного или большего количества пунктов из списка с целью конкретизации возможностей элемента.

Обработка позволяет включить дополнительные детали в элемент и предполагает интерпретацию требования, правила, константы или условия, основанную на целях безопасности. Обработка должна только ограничить набор возможных приемлемых функций или механизмов, чтобы осуществить требования, но не увеличивать их. Обработка не позволяет создавать новые

требования или удалять существующие и не влияет на список зависимостей, связанных с компонентом.

ОК определяют также набор структур, которые объединяют компоненты требований безопасности.

Промежуточная комбинация компонентов названа пакетом. Пакет включает набор требований, которые обеспечивают выполнение многократно используемого поднабора целей безопасности.

Уровни гарантированности оценки — это predetermined пакеты требований гарантированности.

Одной из основных структур ОК является Профиль защиты (ПЗ), определенный как набор требований, который состоит только из компонентов или пакетов функциональных требований и одного из уровней гарантированности. ПЗ специфицирует совокупность требований, которые являются необходимыми и достаточными для достижения поставленных целей безопасности.

Требования Профиля защиты могут быть конкретизированы и дополнены в другой структуре ОК — Задании по безопасности. Задание по безопасности (ЗБ) содержит набор требований, которые могут быть представлены одним из Профилей защиты или сформулированы в явном виде. ЗБ определяет набор требований для конкретного объекта оценки. Оно включает также спецификацию объекта оценки в виде функций безопасности (ФБ), которые должны обеспечить выполнение требований безопасности и мер гарантированности оценки.

Результатом оценки безопасности должен быть общий вывод, в котором описана степень ответственности объекта оценки функциональным требованиям и требованиям гарантированности.

3. Требования к функциям безопасности

Классы и семейства функциональных требований сгруппированы на основе определенной функции или цели безопасности. Всего в разделе "Требования к функциям безопасности" ОК представлены 9 классов, 76 семейств, 184 компонента и 380 элементов.

Класс FAU (аудит безопасности) состоит из 12 семейств, содержащих требования к распознаванию, регистрации, хранению и анализу информации, связанной с действиями, затрагивающими безопасность объекта оценки.

Класс FCO (связь) включает 2 семейства, связанные с аутентификацией сторон, участвующих в обмене данными.

Класс FDP (защита данных пользователя) подразделяется на 5 групп семейств, которые отно-

сятся к защите данных пользователя в пределах ОО в процессе ввода, вывода и хранения информации.

Класс FIA (идентификация и аутентификация) включает 9 семейств. Эффективность выполнения требований других классов зависит от правильной идентификации и аутентификации пользователей.

Класс FPR (секретность) включает 4 семейства и содержит требования к секретности, обеспечивающие защиту пользователя от раскрытия и неправомерного употребления его идентификационных данных другими пользователями.

Класс FPT (защита функций безопасности) включает 22 семейства функциональных требований, которые касаются целостности и контроля ФБ и механизмов, обеспечивающих ФБ.

Класс FRU (использование ресурса) включает 3 семейства, которые определяют готовность требуемых ресурсов к обработке и/или хранению информации.

Класс FTA (доступ к объекту оценки) включает 7 семейств, которые определяют функциональные требования, сверх требований идентификации и аутентификации, для управления сеансами работы пользователей.

Класс FTP (надежный маршрут/канал) включает 2 семейства, которые содержат требования к обеспечению надежного маршрута связи между пользователями и ФБ и надежного канала связи между ФБ.

4. Требования гарантированности безопасности

В этом разделе представлены 7 классов, 25 семейств, 72 компонента.

Класс АСМ (управление конфигурацией) состоит из трех семейств. Управление конфигурацией гарантирует готовность ОО и документации к распространению.

Класс АДО (поставка и эксплуатация) состоит из двух семейств и определяет требования к мерам, процедурам и стандартам, связанным с безопасной поставкой, установкой и эксплуатацией ОО.

Класс ADV (разработка) состоит из шести семейств и определяет требования для пошаговой проработки ФБ от общей спецификации ОО в ЗБ до реализации.

Класс AGD (руководства) состоит из двух семейств и определяет требования к полноте и завершенности эксплуатационной документации, представленной разработчиком. Эта документация, которая содержит два вида информации (для конечных пользователей и для администраторов), является важным фактором безопасной эксплуатации ОО.

Класс ALC (поддержка жизненного цикла) состоит из четырех семейств и определяет требования к модели жизненного цикла для всех этапов разработки ОО.

Класс ATE (тестирование) состоит из четырех семейств и формулирует требования для объема, глубины и вида испытаний, которые позволяют сделать вывод о выполнении функциональных требований безопасности.

Класс AVA (оценка уязвимости) состоит из четырех семейств и определяет требования, направленные на идентификацию уязвимых мест. Для некоторых функций безопасности предусмотрено требование к силе. Например, механизм пароля не может полностью предотвратить раскрытие, но его сила может быть увеличена путем увеличения длины пароля или уменьшения интервала изменений.

Сила функции оценивается как базовая, если анализ показывает, что функция обеспечивает адекватную защиту против нарушений безопасности нападавшими, обладающими низким потенциалом. Потенциал нападения определяется путем оценки возможностей, ресурсов и побуждений нападавшего.

Аналогично определяются средняя и высокая сила функции.

В ОК определено семь уровней гарантированности оценки (УГО). Увеличение гарантированности обеспечивается увеличением строгости и/или глубины оценки и включением компонентов из других семейств (то есть добавлением новых требований).

УГО1 – функционально проверенный проект. УГО1 предназначен для обнаружения очевидных ошибок при минимальных издержках. Компоненты УГО1 обеспечивают минимальный уровень гарантированности путем независимого анализа каждой функции безопасности с использованием функциональной и интерфейсной спецификации ОО.

УГО2 – структурно проверенный проект. Для получения гарантий служит анализ функций безопасности и проекта высокого уровня подсистем ОО, а также тестирование разработчиком и независимой группой.

УГО3 – методически проверенный и протестированный проект. УГО3 позволяет получить максимальную гарантию безопасности на стадии разработки проекта без существенного изменения обычных методов разработки. УГО3 обеспечивает дополнительную гарантированность путем включения средств контроля среды разработки и управления конфигурацией ОО.

УГО4 – методически проработанный и проверенный проект. УГО4 позволяет получать максимальную гарантию безопасности при проектировании, основанном на хороших коммер-

ческих методах разработки. УГО4 — самый высокий уровень, который, вероятно, будет экономически целесообразен. Компоненты УГО4 включают анализ функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и поднабора выполнения. Анализ поддержан независимым испытанием функций безопасности, актом испытаний разработчиком "серого ящика", независимым подтверждением выборочных результатов испытаний, свидетельством поиска разработчиком явных уязвимых мест и независимым поиском явных уязвимых мест.

УГО5 — полуформально разработанный и проверенный проект. Компоненты УГО5 обеспечивают гарантию путем анализа функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и всего процесса выполнения. Дополнительная гарантия получается за счет использования формальной модели и полуформального представления функциональной спецификации и проекта высокого уровня и полуформальной демонстрации соответствия между ними. Требуется также поиск тайных каналов передачи информации.

УГО6 — полуформально верифицированный и проверенный проект. Компоненты УГО6 обеспечивают гарантию путем анализа функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и структурированного представления процесса выполнения. Требуется также систематический поиск тайных каналов, структуризация процесса разработки, наличие средств контроля среды разработки и всестороннего управления конфигурацией ОО, включая полную автоматизацию.

УГО7 — формально верифицированный и проверенный проект. УГО7 применим при разработке специальных продуктов для эксплуатации в условиях чрезвычайно высокого риска.

5. Предопределенные профили защиты

Профиль защиты (ПЗ) включает следующие основные разделы:

- Безопасность окружения. Окружение описывается в терминах ожидаемых угроз, предписанной политики безопасности и условий использования ОО.
- Цели безопасности. Формулировка задачи обеспечения безопасности, являющаяся базисом для определения требований к ОО.
- Функциональные требования.
- Требуемый уровень гарантированности.

Профиль защиты ОК по сути является аналогом классов "Оранжевой книги" и классов защищенности РД Гостехкомиссии (ГТК) РФ, но

базируется на значительно более полной и систематизированной совокупности компонентов требований безопасности.

Часть 4 ОК содержит три профиля защиты. Два из них были созданы на основе более ранних критериев, еще один разработан для продуктов ИТ, которые являются относительно новыми для процесса оценки безопасности.

Профили "Коммерческая защита 1" (К31) и "Коммерческая защита 3" (К33) представляют собой развитие профилей Федеральных критериев [15], выполненное с использованием терминологии и конструкций ОК. Профиль К31 предназначен для замены профиля Федеральных критериев CS1 (и, следовательно, класса C2 TCSEC), но не идентичен этим наборам требований. Профиль К33 ОК предназначен для замены профиля Федеральных критериев CS3.

Профиль ОК "Межсетевой экран" (fire-wall) — первый член возможного семейства профилей, связанных с межсетевыми экранами*.

Количество стандартизованных Профилей защиты в ОК потенциально не ограничено, однако все они должны отвечать соответствующим требованиям и, прежде чем быть включенными в международный регистр, пройти процедуры регистрации, которые будут определены в ОК.

6. Заключение

Общие критерии основаны на ряде нормативных документов в области безопасности информационных технологий, принятых в шести странах Европы и Америки. Они учитывают накопленный в этом направлении опыт.

Новым в концепции ОК является гибкость и динамизм в подходе к формированию требований и оценке безопасности продуктов и систем ИТ. При сравнительном анализе всех основных стандартов безопасности ИТ по пяти показателям (универсальность, гибкость, гарантированность, реализуемость, актуальность) Общие критерии получили наивысшую оценку [9].

На наш взгляд, версия 1.0 Общих критериев имеет ряд недоработок: отсутствие предопределенных функциональных пакетов, отработанных профилей защиты, процедур регистрации новых профилей защиты, а также требований к криптографическим компонентам. Вероятно, эти недостатки будут устранены в последующих версиях.

Учитывая перспективность и международный характер Общих критериев, целесообразно использовать основные положения и конструкции ОК при разработке нормативных документов, методического и инструментального обеспе-

*Примечание. Подобное семейство профилей защищенности межсетевых экранов представлено в Руководящем документе Гостехкомиссии РФ [6].

чения оценки безопасности продуктов и систем ИТ в России. В частности, представляется необходимой разработка следующего комплекса стандартов (или Руководящих документов Гостехкомиссии России):

- Безопасность информационных технологий. Термины и определения.
- Концепция оценки безопасности информационных технологий.
- Общие критерии оценки безопасности информационных технологий. Функциональные требования и требования гарантированности оценки.
- Профиль защиты. Руководство по разработке и регистрации.
- Задание по безопасности. Руководство по разработке и оформлению.
- Руководство по проектированию и эксплуатации автоматизированных систем, отвечающих требованиям информационной безопасности.
- Руководство по сертификации продуктов и систем информационных технологий по требованиям безопасности.

Преимущество уже проведенных оценок безопасности продуктов и систем ИТ по действующим нормативным документам (РД ГТК России) может быть обеспечена путем разработки на основе концепции ОК типовых стандартизованных профилей защиты, соответствующих классам защищенности в Руководящих документах Гостехкомиссии России.

До принятия Общих критериев в качестве международного стандарта и появления соответствующих стандартов в России, целесообразно при формировании требований и оценке безопасности продуктов и систем ИТ руководствоваться не только требованиями действующих нормативных документов, но и дополнительными требованиями, сформированными на основе ОК с учетом специфики конкретного объекта оценки.

Целесообразно на основе материалов Общих критериев вести разработку профилей защиты и требований ТЗ по обеспечению безопасности для новых типов продуктов (систем) и новых информационных технологий.

7. Литература

1. Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. — Москва, 1992.
2. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. — Москва, 1992.
3. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. — Москва, 1992.
4. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — Москва, 1992.
5. Гостехкомиссия России. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. — Москва, 1992.
6. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — Москва, 1997.
7. И. Моисеенков. Американская классификация и принципы оценивания безопасности компьютерных систем. — КомпьютерПресс, 1992, 2.
8. В.А. Галатенко. Информационная безопасность — обзор основных положений. — Jet Info, 1996, 1-3.
9. Д.П. Зегжда, А.М. Ивашко. Как построить защищенную информационную систему. — НПО "Мир и семья — 95", Санкт-Петербург, 1997.
10. Trusted Computer System Evaluation Criteria (TCSEC). — US DoD 5200.28-STD, 1983.
11. National Computer Security Center. Trusted Network Interpretation. — NCSC-TG-005, 1987.
12. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800. — CCITT, Geneva, 1991.
13. Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France — Germany — the Netherlands — the United Kingdom. — Department of Trade and Industry, London, 1991.
14. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), Version 3.0. — Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993.
15. Federal Criteria for Information Technology Security (FC), Draft Version 1.0, (Volumes I and II). — National Institute of Standards and Technology, National Security Agency, US Government, 1993.
16. Common Criteria for Information Technology Security Evaluation (CCEB). Version 1.0. 96.01.31.

Обновление семейства Ultra-компьютеров

Леонид Черняк

13 января 1998 года компания Sun Microsystems представила полностью обновленное семейство рабочих станций Ultra. Оно включает:

- две младшие модели, Ultra 5 и Ultra 10, выполненные в рамках проекта Darwin;
- рабочую станцию средней производительности Ultra 30 (см. Jet Info, 1997, 16);
- высокопроизводительную рабочую станцию Ultra 60;
- известную станцию Ultra 2.

Одновременно было объявлено о начале производства нового графического ускорителя Elite3D.

Ultra 5 и Ultra 10

Станции Darwin - это прорыв Unix-рабочих станций в ценовой диапазон персональных компьютеров. Стоимость Ultra 5 в начальной конфигурации (процессор UltraSPARC-IIi 270 МГц, оперативная память 64 Мб, HDD 4.3 Гб, FDD 1.44 Мб, без монитора) составляет 2995 долларов. Ultra 5 дешевле и на 30% производительнее, чем Compaq PW 5100 или Hewlett-Packard Kayak XA на процессоре Pentium II 266 МГц в аналогичной конфигурации.

**Здесь и далее указаны цены для продажи в США.*

Более производительная станция Ultra 10 (процессор UltraSPARC-IIi 300 МГц, внешний кэш 512 Кб, оперативная память 64 Мб, HDD 4.3 Гб, FDD 1.44 Мб, без монитора) стоит 6395 долларов. Станция Ultra 10 с графическим ускорителем Elite3D m3 стоит 12 495 долларов и при этом более чем вдвое превосходит по производительности на графических тестах систему SGI Octane/MXI, продаваемую по цене 44495 долларов.

Архитектура

Две станции Darwin имеют близкую архитектуру. На Рис. 1. представлена архитектура станции Ultra 10, от станции Ultra 5 она отличается более высокой тактовой частотой процессора и наличием выделенного слота UPA (100 МГц) для подключения графических ускорителей Creator или Elite3D. Дополнительные отличия Ultra 10 по сравнению с Ultra 5 - конструктивное исполнение (минитауэр и настольное) и число слотов PCI (4 против 3).

Станции Darwin построены на 64-битном процессоре UltraSPARC-IIi. Он оптимизирован для использования в качестве основы однопроцессорных рабочих станций, в нем сочетаются высокая производительность и возможность подключения PCI-совместимых устройств напрямую на частоте 66 МГц или через мост PCI-PCI на частоте 33 МГц.

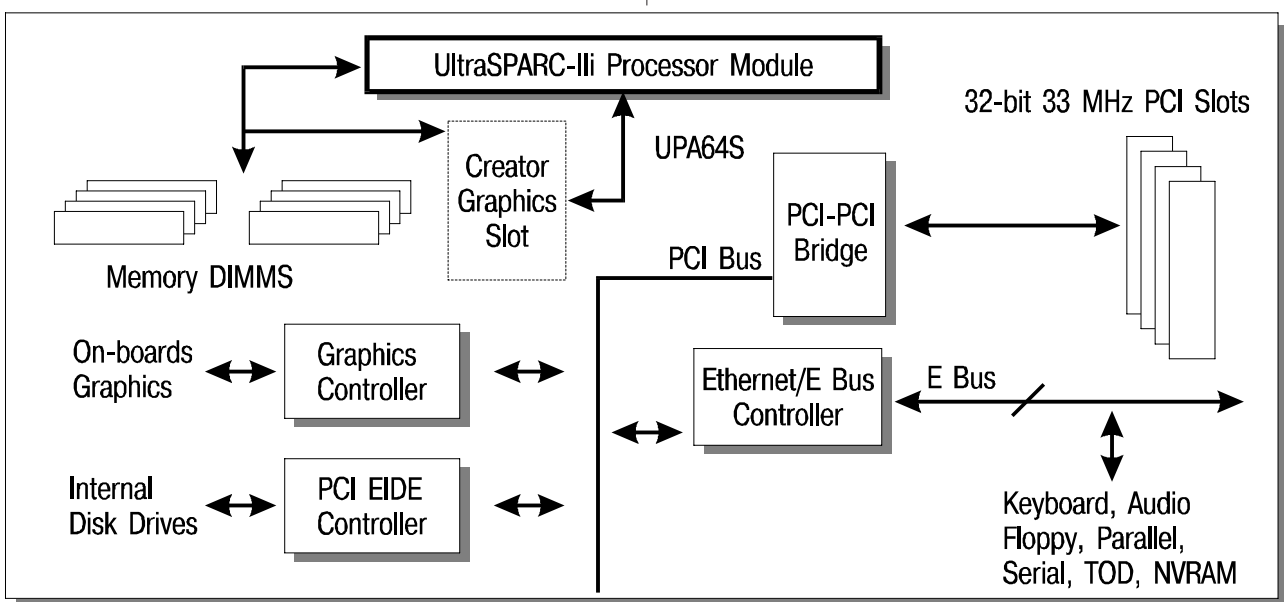


Рис. 1. Архитектура рабочей станции Ultra 10.

Области применения

Ultra 5 предназначена для тех приложений, где в рамках бюджетных ограничений необходимо сочетать высокую производительность вычислений и работу с двумерной графикой. Это разработка программного обеспечения, работа с документами, разработка встроенных систем.

Ultra 10 в большей степени ориентирована на трехмерные приложения, такие как анимация, геоинформационные системы, моделирование и анализ в науке и технике.

Отзывы тестировавших станции Darwin пользователей, в числе которых специалисты из крупнейших университетов и лабораторий, промышленных и медицинских компаний, можно посмотреть по адресу <http://www.sun.com/desktop/insight.html>. В качестве достоинств станций отмечается оптимальное соотношение производительность/цена и возможность использования PCI-периферии.

Ultra 60

О новой, самой производительной из рабочих станций Sun Microsystems также нельзя говорить вне ценового контекста. По словам президента SMCC (Sun Microsystems Computer Company) Эда Зандера, с появлением компьютера Ultra 60 рабочие станции стоимостью 50000 долларов и выше исчезают как класс. В начальной конфигурации Ultra 60 стоит 13 295 долларов. Полностью сконфигурированная система (два

процессора UltraSPARC-II 300 Мгц, графический ускоритель Elite3D m6, HDD 4 Гб, оперативная память 256 Гб и монитор 21 дюйм) стоит 27760 долларов.

Представитель IDC Кэрэн Сеймур сказал: "Цены на новую станцию Ultra 60 настолько агрессивны, что они могут стать стимулом к началу ценовой войны на рынке рабочих станций. Конкуренты обязаны найти ответ на присутствие Ultra 60 на рынке."

При меньшей стоимости Ultra 60 обладает более высокой производительностью, чем изделия конкурентов. Показательно сравнение по SPECint95 и SPECfp95.

	Sun Ultra 60	SGI Octane	HP J282
SPECint95	13.0	11.0	11.9
SPECfp95	23.5	22.7	19.3

Табл. 1. Сравнение производительности двухпроцессорных рабочих станций.

Новая рабочая станция обладает графическими возможностями, которые раньше ассоциировались преимущественно с продуктами компании Silicon Graphics. По производительности Ultra 60 Elite3D превосходит станции Silicon Graphics и Hewlett-Packard, находящиеся в ценовом диапазоне 50 - 85 тысяч долларов.

Архитектура

На Рис. 2. представлена системная архитектура Ultra 60. Станция поставляется в одно- или двухпроцессорной комплектации (UltraSPARC-II,

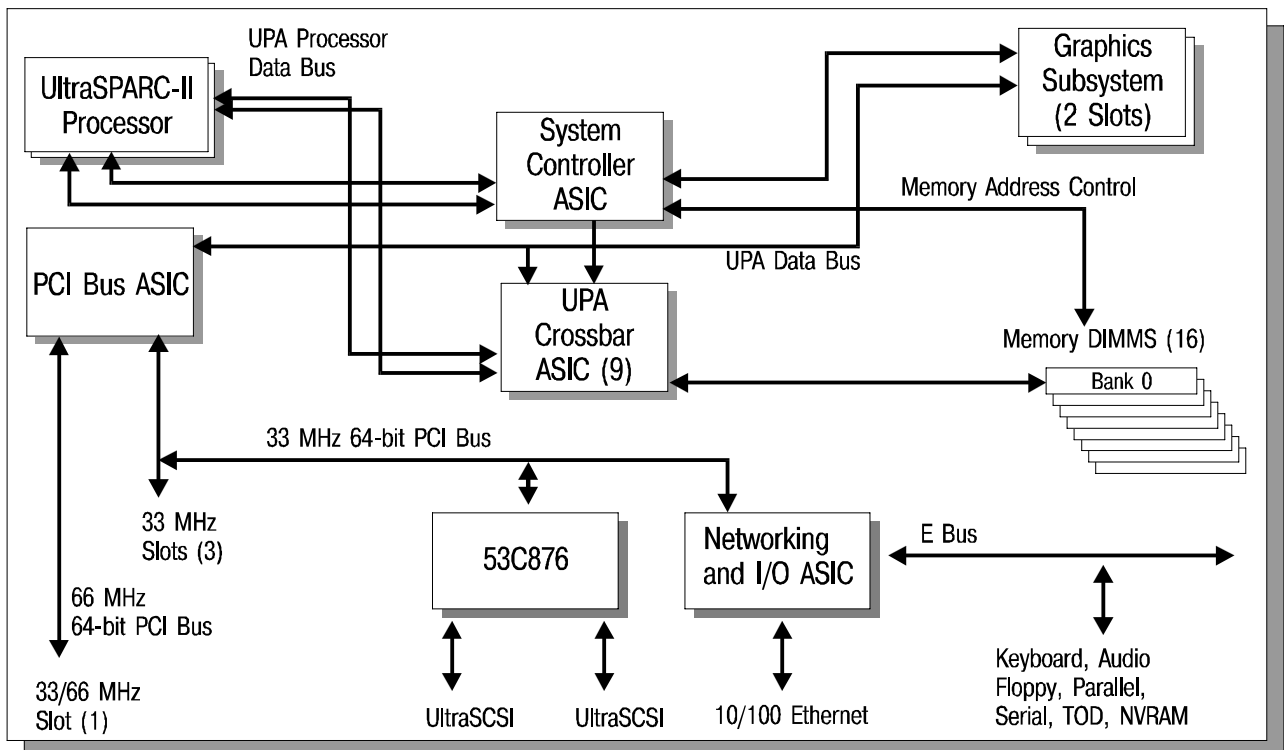


Рис. 2. Архитектура рабочей станции Ultra 60.

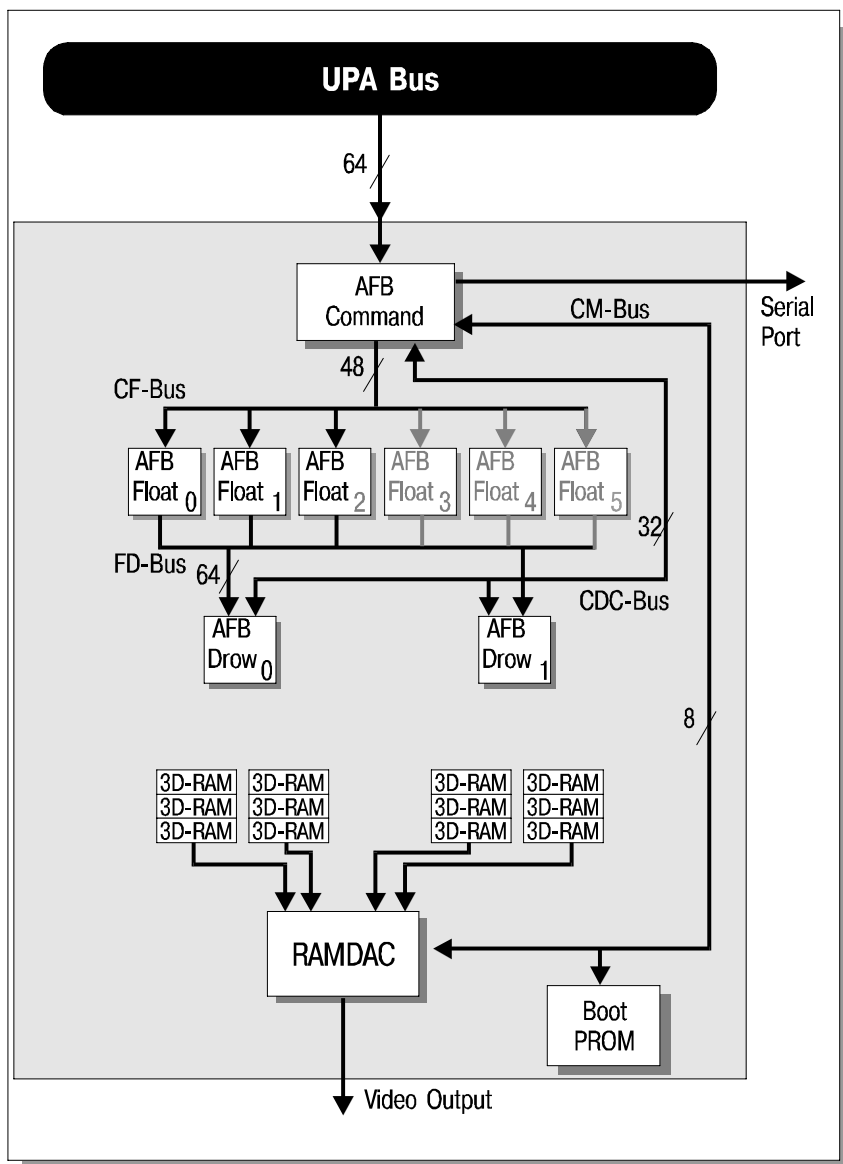


Рис. 3. Архитектура графических ускорителей Elite3D m3 и Elite3D m6.

300 МГц). От старших моделей серверов Sun она унаследовала коммутатор (структуру межсоединений) UPA. Характеристики процессора UltraSPARC и коммутатора UPA подробно описаны в статье А. Шадского "Семейство компьютеров Ultra компании Sun Microsystems" (см. Jet Info, 1997, 23-24). Как и в серверах Ultra Enterprise,

процессоры монтируются на отдельных конструктивных модулях вместе с внешней кэш-памятью, что позволяет модернизировать станцию при появлении новых поколений процессоров.

От станций семейства Darwin Ultra 60 отличается наличием внешней и внутренней шин UltraSCSI. Эти шины имеют про-

пускную способность 40 Мб/с, но сохраняют совместимость с FastSCSI и стандартным SCSI.

Графический ускоритель Elite3D

Графический ускоритель Elite3D сохраняет программную совместимость с ускорителем Creator Graphics, но при этом обладает некоторыми дополнительными функциональными возможностями. Он выпускается в двух версиях - Elite3D m3 и Elite3D m6.

Благодаря использованию трех графических процессоров с плавающей точкой, Elite3D m3 имеет на трехмерной графике вдвое более высокую производительность чем Creator3D series3. Elite3D m3 предназначен для станций Ultra 10, Ultra 30 и Ultra 60.

Шесть графических процессоров с плавающей точкой обеспечивают Elite3D m6 пятикратное повышение производительности по сравнению с Creator3D series 3. Elite3D m6 предназначен для станций Ultra 2, Ultra 30 и Ultra 60. Elite3D значительно ускоряет обработку пространственных покрытий и текстур.

На Рис. 3. представлена архитектура Elite3D m3 и Elite3D m6. Последний отличается удвоенным числом процессоров с плавающей точкой.

