Часть 3. Обзор стандартов защищенных операционных систем

Существует два способа построения защищенной системы – построение защищенной системы с нуля, и адоптация уже существующей операционной системы.

В случае построения защищенной системы с нуля, проблема обеспечения информационной безопасности является одной из целей разработчика каждого компонента создаваемой операционной системы. В этом случае методы обеспечения информационной безопасности являются неотъемлемой составной частью самой операционной системы. Такой подход чреват значительной трудоемкостью и доступен только крупным фирмам разработчикам операционных систем.

Доработка уже существующей операционной системы. Данный подход характеризуется значительно меньшими затратами. Но встраивание методов защиты в уже существующую операционную систему требует высокой степени документирования внутреннего мира операционной системы или открытости ее исходного текста. Такую информацию предоставляют единичные производители программного обеспечения. Недостаток информации о внутренних информационных процессах приводят к многочисленным случаям неуспешных попыток внедрения механизмов защиты в уже готовое ядро операционной системы.

Современный уровень развития системного программного обеспечения характеризуются значительным повышением роли компьютерной техники в нашей жизни. Появление виртуальных машин и языков интерпретаторов делает данные не отличимыми от исполнимых модулей.

Разрыв между теоретическими моделями безопасности и современными информационными технологиями. Практически все системы защиты информации в компьютерных системах основаны на информации об уже состоявшихся атаках, а не на анализе теоретико-множественных моделей систем. Таким образом, существующие системы обеспечения безопасности только противодействуют уже известным угрозам и методам атак, и не могут предсказывать все возможные действия нарушителя.

Модели информационной безопасности операционных систем закладываются в стандартах безопасности операционных систем.

Главная задача стандартов информационной безопасности – создать основу для взаимодействия между фирмами, производителями операционных систем, фирмами, выпускающими прикладное и системное программное обеспечение, а так же пользователями данных систем.

1. Критерии безопасности министерства обороны США – «Оранжевая книга»

Данные критерии безопасности были разработаны министерством обороны США в 1983 году.

В «Оранжевой книге» предложены три категории требований безопасности (политика безопасности, аудит, корректность) на основе которых сформулированы шесть базовых требований безопасности.

Политика безопасности

Требование 1. Политика безопасности

Система должна поддерживать заявленную политику безопасности, на основе которой должен осуществляется доступ к ресурсам всех пользователей работающих в системе.

Требование 2. Метки

С каждым объектом системы должны быть поставлена в соответствие метка, определяющая набор атрибутов доступа к этому объекту.

Аудит

Требование 3. Идентификация и аутентификация

Все субъекты должны иметь уникальные идентификаторы. Предоставление доступа к ресурсам системы должен осуществляться только после идентификации объекта и субъекта, подтверждения их подлинности. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа.

Требование 3. Регистрация и учет

Система должна предоставлять пользователю средства контроля над событиями в системе. Данный журнал должен быть надежно защищен от несанкционированного доступа.

Корректность

Требование 5. Контроль функционирования средств защиты

Подсистема защиты должна содержать полностью не зависимые от нее средства контроля функционирования данной подсистемы.

Требование 6. Непрерывность защиты

Должна обеспечивается защита от несанкционированного доступа или отключения системы защиты операционной системы.

Дане принципы и требования представлены на рис. 1.1.

Рис. 1.1. Классификация требований «Оранжевой книги»

Классы защиты систем с точки зрения «Оранжевой книги» приведены в табл. 1.1.

Табл. 1.1. Классы защиты

Класс	Требования
Группа D. Минимальная защита	
D1	Минимальная защита. В данную группу входят все системы, не отвечающие более высоким требованиям.
Группа C. Дискреционная защита	
C1	Дискреционная защита. Должно обеспечиваться разделение пользователей, защита информации одного пользователя от других пользователей системы, контроль и управление доступом. Данная группа предназначена для многопользовательских систем с одной группой секретности.
C2	Управление доступом. Дополнительно к требованиям класса C1, должно обеспечиваться возможности индивидуального контроля над действиями пользователей и управления доступом.
Группа B. Мандатная защита	

B1	Защита с применением меток безопасности. Дополнительно к требованиям класса C2, система должна поддерживать неформальную модель безопасности, маркировку данных, нормативное управление доступом.
B2	Структурированная защита. Ядро системы должно соответствовать четко документированной модели безопасности. Должно быть предусмотрено нормативное и произвольное управление доступом. Должны быть предоставлены средства обнаружения скрытых каналов утечки информации. Управление безопасностью должно осуществляется администраторами системы. Должны быть предусмотрены средства тестирования системы.
B3	Домены безопасности. Дополнительно к выше изложенным требованиям ядро системы должно поддерживать монитор взаимодействий, контролирующий все обращения к ресурсам системы. Средства аудита должны включать оповещение администратора при критичных событиях. Должны быть предусмотрены возможности тестирования системы на уровне архитектуры и реализации функций.
Группа A. Верификационная защита	
A1	Формальная верификация. Должны выполняться все требования класса B3. В ходе разработки должны выполняться формальные методы верификации функций защиты на основе разработанной модели безопасности.

Как видно из табл. 1.1. Классы защиты расположены от **D** до **A**. В класс **D** входят все системы. Класс **C** требует наличие системы управления доступом и регистрацией действий субъекта. Класс **B** требует поддержки политики безопасности, наличия в составе системы монитора, контролирующего события в системе. Класс **A** требует верификации исходного текста системы на соответствие модели безопасности, выполнение этих требований на практике представляется маловероятным.

Критерии безопасности, сформулированные в «Оранжевой книги» являлись первой попыткой создать стандарт безопасности, они послужили основой для создания многих других национальных стандартов информационной безопасности.

2. Европейские критерии безопасности информационных технологий

Европейские критерии информационной безопасности были созданы в 1991 году совместно Великобританией, Германией, Голландией и Францией.

Согласно данному документу, выделяются следующие задачи системы обеспечения информационной безопасности:

- защита информации от несанкционированного доступа;
- обеспечение целостности информации;
- обеспечение работоспособности системы.

Классы защиты систем представлены в табл. 1.2.

Табл. 1.2. Классы зашиты систем по европейским критериям безопасности информационных технологий

Класс	Требования
F–C1	Соответствует классу C1 «Оранжевой книги».
F–C2	Соответствует классу C2 «Оранжевой книги».
F–B1	Соответствует классу B1 «Оранжевой книги».
F–B2	Соответствует классу B2 «Оранжевой книги».
F–B3	Соответствует классу B3 «Оранжевой книги».
F–IN	Основное внимание уделяется обеспечению целостности данных. В основном данный класс ориентирован на базы данных.
F–AV	Повышенные требования к обеспечению работоспособности системы. Требуется обеспечить гарантированное время реакции системы на событие, дуплексирование и резервирование функций системы. Должны обеспечиваться функции работоспособности системы во время замены и модификации функций системы. Данный класс безопасности ориентирован на системы реального времени и системы управления технологическими процессами.
F–DI	Класс требований ориентирован на распределенные информационные системы. Требуется обеспечить идентификацию участников взаимодействия, обеспечить безопасность и целостность передаваемой по каналам связи информации.
F–DC	Класс требований ориентирован на распределенные информационные системы. Особое внимание уделяется требованиям к конфиденциальности передаваемой информации. Информация по каналам связи должна передаваться только в зашифрованном виде, ключи шифрования должны от несанкционированного доступа.
F–DX	Класс требований ориентирован на распределенные информационные системы. Должны выполняться требования целостности, передаваемой в зашифрованном виде информации по каналам связи. Фактически в классе F–DX объединяются требования классов F–DI и F–DC.

Кроме классов защиты европейские критерии безопасности предусматривают семь уровней адекватности систем.

Уровень E0 – минимальный уровень адекватности, соответствует классу D «Оранжевой книги».

Уровень E1 – анализу подвергается только общая архитектура системы, адекватность системы защиты подтверждается тестированием.

Уровень E3 – анализу подвергаются исходные тексты системы.

Уровень Е6 – самый высокий уровень адекватности систем, требующий соответствие формальной модели и выполнение требований политики безопасности.

Европейские критерии безопасности, созданные на основе «Оранжевой книги» являются следующим шагом в построении стандартов защиты информации.

3. Руководящие документы Гостехкомиссии России

Руководящие документы Гостехкомиссии были разработаны в 1992 году и включают в себя пять руководящих документов, главным из которых является «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации».

Согласно данных документов, все системы вычислительной техники распределяются на семь классов защищенности от несанкционированного доступа. Требования к классам приведены в табл. 1.3.

Табл. 1.3. Классы защищенности средств вычислительной техники

Наименование показателя	Класс защищенности						
	7	6	5	4	3	2	1
Дискреционный принцип контроля доступа		+	+	+	=	+	=
Мандатный принцип контроля к доступу				+	=	=	=
Очистка памяти			+	+	+	=	=
Изоляция модулей				+	=	+	=
Маркировка документов				+	=	=	=
Защита ввода/вывода на внешние носители				+	=	=	=
Сопоставление пользователя и устройства				+	=	=	=
Идентификация и аутентификация		+	=	+	=	=	=
Гарантии проектирования			+	+	+	+	+
Регистрация			+	+	+	=	=
Взаимодействие пользователя с комплексом средств защиты					+	=	=
Функции восстановления					+	=	=
Контроль целостности комплекса средств защиты			+	+	+	=	=
Контроль модификации						+	=
Контроль дистрибуции						+	=
Гарантии архитектуры							+
Тестирование		+	+	+	+	+	=
Руководство пользователя		+	=	=	=	=	=
Руководство по комплексу средств защиты		+	+	=	+	+	=
Текстовая документация		+	+	+	+	+	=
Конструкторская документация		+	+	+	+	+	+

‘+’ – новые, дополнительные требования;

‘=’ – требования совпадают с предыдущим классом.

Кроме рассмотрения защиты средств вычислительной техники в документах Гостехкоммисси выделяется девять классов защищенности автоматизированных систем. Требования к классам защищенности приведены в табл. 1.4.

Табл. 1.4. Классы защищенности автоматизированных систем

Требования	Классы защищенности								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Контроль доступа: – в систему	+	+	+	+	+	+	+	+	+
– к узлам ЭВМ и каналам связи				+		+	+	+	+
– к программам				+		+	+	+	+
– к файловой системе, учетным записям				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
2. Подсистема регистрации и учета Регистрация и учет: – входа/выхода в систему	+	+	+	+	+	+	+	+	+
– печати		+		+		+	+	+	+
– запуска/завершения процессов				+		+	+	+	+
– доступ к защищенным файлам				+		+	+	+	+
– доступ из программ к ресурсам				+		+	+	+	+
– изменение прав							+	+	+
– создание защищенных объектов				+			+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка остаточной информации		+		+		+	+	+	+
2.4. Сигнализация нарушения защиты							+	+	+
3. Криптографическая подсистема – шифрование конфиденциальной информации				+				+	+
– шифрование информации пользователей собственными ключами									+
– аттестация криптографических систем				+				+	+
4. Подсистема обеспечения целостности – целостность программных средств	+	+	+	+	+	+	+	+	+
– охрана ЭВМ и носителей информации	+	+	+	+	+	+	+	+	+
– администратор службы защиты информации				+			+	+	+
– периодическое тестирование системы защиты информации	+	+	+	+	+	+	+	+	+
– наличие средств восстановления системы защиты информации	+	+	+	+	+	+	+	+	+
– использование сертифицированных средств защиты		+		+			+	+	+

Все классы защищенности разбиты на 3 группы. Высшей степени защищенности в каждой группе соответствует класс А.

Разработка документов Гостехкоммиссии явилось следствием бурного проникновения средств вычислительной техники и программных систем в нашу страну, с одной стороны и полного отсутствия национальной правовой базы для создания систем защиты.

Данные документы отличает недостаточно высокий уровень информационных технологий, однобокость подходов, значительный уклон в сторону секретности, вызванной спецификой разработавших их организаций. Фактически данные документы рассматриваю только одну угрозу – несанкционированный доступ.

4. Единые критерии безопасности информационных технологий

Единые критерии безопасности информационных технологий были приняты в 1996 году на основе объединения целого ряда национальных критериев безопасности: «Европейских критериев безопасности информационных технологий» (Великобритания, Германия, Голландия, Франция), «Федеральных критериев безопасности информационных технологий» (США), «Канадских критериев безопасности компьютерных систем». На сегодняшний день Единые критерии безопасности информационных технологий являются самым проработанным и новым документом в этой области.

Основе требования к безопасности определяется профилем защиты, на основании которого составляется проект защиты.

С точки зрения Единых критериев безопасности информационных технологий выделяется семь уровней адекватности систем. Для каждого уровня задается номер требований по каждой категории. Большее значение номера соответствует более жестким требованиям. Требования адекватности к уровням защиты приведено в табл. 1.5.

Табл. 1.5. Уровни адекватности защиты информации, согласно Единых критериев безопасности информационных технологий

Требования адекватности	Номера уровней						
	1	2	3	4	5	6	7
1. Управление конфигурацией – автоматическое управление конфигурацией				**1**	**1**	**2**	**2**
– управление конфигурацией	**1**	**1**	**2**	**3**	**3**	**4**	**4**
– ограничение управления конфигурацией			**1**	**2**	**3**	**3**	**3**
2. Дистрибуция – поставка							
– установка, настройка		**1**	**1**	**1**	**1**	**1**	**1**
3. Адекватность реализации – общие функциональные спецификации	**1**	**1**	**1**	**2**	**4**	**5**	**6**
– архитектура защиты		**1**	**2**	**2**	**3**	**4**	**5**
– форма реализации				**1**	**2**	**3**	**3**
– внутренняя структура средств защиты					**1**	**2**	**3**
– спецификация средств защиты				**1**	**1**	**2**	**2**
– соответствие архитектуры и спецификации требованиям безопасности	**1**	**1**	**1**	**1**	**2**	**2**	**3**
4. Документация – руководство администратора	**1**	**1**	**1**	**1**	**1**	**1**	**1**
– руководство пользователя	**1**	**1**	**1**	**1**	**1**	**1**	**1**
5. Процесс разработки – безопасность среды разработки			**1**	**1**	**1**	**2**	**2**
– исправление ошибок							
– технология разработки				**1**	**2**	**2**	**3**
– средства разработки				**1**	**2**	**2**	**3**
6. Тестирование – полнота тестирования		**1**	**2**	**2**	**2**	**3**	**3**
– глубина тестирования		**1**	**2**	**2**	**3**	**3**	**4**
– методика тестирования		**1**	**1**	**1**	**1**	**1**	**1**
– независимое тестирование	**1**	**1**	**2**	**2**	**2**	**2**	**3**
7. Оценка уязвимости – анализ скрытых каналов					**1**	**2**	**2**
– анализ не правильной работы защиты			**1**	**2**	**2**	**2**	**2**
– анализ преодоления средств защиты		**1**	**1**	**1**	**1**	**1**	**1**
– анализ наличия изъянов защиты		**1**	**1**	**2**	**3**	**4**	**4**

5. Изъяны защиты операционной системы UNIX

Операционная система UNIX рассмотренная в (2.6 – уточнить номер), является открытой системой, на базе которой создавалась целая серия операционных систем. Разработчики операционной системы ставили перед

собой цель создать операционную систему для межсетевого взаимодействия, предъявляющей минимальные требования к аппаратуре компьютера. При этом проблема обеспечения информационной безопасности, в начальный период существования операционной системы UNIX, уделялось сравнительно мало внимания. В тот период этим аспектом действительно зачастую пренебрегали, однако из операционных систем того времени, сейчас существует и развивается только операционная система UNIX. К сожалению, изъяны защиты, заложенные при проектировании этой операционной системы, остаются значительными лазейками для атаки на данную операционную систему.

В данном параграфе приведена информация об изъянах защиты операционной системы UNIX, приведенная в открытой печати и Internet.

Запуск системных утилит. Все пользователи регистрируются в файле /etc/passed. Все пользователи, кроме root имеют доступ к этому файлу только по чтению. Однако в ряде случаев пользователю приходится запускать программы, модифицирующие записи в файле /etc/passwd. Для этого требуется использовать атрибут SUID, который предоставляется многим пользователем. В этом случае выполняющий это процесс получает доступ к идентификатору и правам пользователя, которому принадлежит данная системная программа – как правило, это пользователь root имеющий полный доступ ко всем ресурсам системы.

Например, при создании нового каталога (mkdir) последовательно вызываются два системных процесса – mknot и chown, имеющие пава root. Если каталог создавался как фоновый процесс, то пользователь мог приостановить его после выполнения первого процесса и остаться с правами root.

Отправка сообщения пользователю root. Во многих версиях UNIX почтовая программа, после получения сообщения, назначает владельцем файла, в котором хранятся полученные сообщения адресата сообщения.

Посылка сообщения, содержащие исполнимый модуль. В некоторых версиях UNIX посылка сообщения с вложенным исполнимым модулем приводила к автоматическому запуску его на удаленном компьютере. Примером такой программы является червь Р.Мориса.

Удаленное выполнение команд. Утилита удаленного запуска программ uux, производит синтаксический анализ полученной команды, однако она не учитывает все многообразие возможностей формирования команды.

Переполнение буфера записи в файл /etc/passwd. В случае неконтролируемого переполнения буфера при записи в файл /etc/passwd, в нем может образоваться пустая строка, которая будет интерпретирована как пользователь пустым именем и паролем, обладающего правами root.

Переполнение стека. Адрес точки возврата при вызове процедуры может вследствие переполнения буфера, позволит заменить код точки возврата. Тем самым, передается управление, со всеми правами, которые принадлежат вызванной программе, на программу подставленную нарушителем.

Изъяны защиты UNIX оставляют большие возможности для нарушителей информационной безопасности. Эти проблемы характерны не только для операционной системы UNIX но и для многих других операционных систем.