ЛЕКЦИЯ №1

«Теоретические основы безопасности операционных систем»

по дисциплине

«Безопасность операционных систем»

Текст лекции рассмотрен и одобрен на заседании кафедры протокол № _____ от " " 201__ г.

(Слайд 1. Титульный слайд)

Уважаемые студенты! Сегодня вы начинаете изучение новой дисциплины профиля «Технологии обеспечения безопасности информационных систем». Дисциплина называется «Безопасность операционных систем». Лекция №1 «Теоретические основы безопасности операционных систем». Продолжительность лекции - 4 академических часа.

Слайд 2 (план проведения занятия)

Данная лекция состоит из 3-х логических частей. Первая часть — введение. Во введении вы узнаете о задачах и содержании настоящей дисциплины, программу дисциплины, вам будет рекомендована литература для изучения и закрепления материала.

Вторая часть — основная. В ней будет рассказано о текущем уровне и перспективах развития операционных систем. Дана классификация ОС, определены принципы построения защищенных ОС. Рассмотрены критерии оценки безопасности ОС в различных странах.

Третья часть — заключение. Будут даны рекомендации для самостоятельной работы студента, сделаны выводы по материалам лекции, выражены пожелания по индивидуальному развитию студентов как высококлассных IT-специалистов в области информационной безопасности.

Слайд 3 (объем дисциплины)

Объем дисциплины составляет 108 академических часов, из них 48 часов аудиторных занятий (32 часа лекции и 16 часов практические занятия), 42 часа - самостоятельная работа студента. По итогам дисциплины предусмотрена отчетность в виде дифференцированного зачета.

Слайд 4 (задача и содержание дисциплины)

Задача дисциплины - овладеть навыками обеспечения безопасности современных операционных систем, использования программных и технических средств защиты информации, эксплуатации защищенных ОС.

Курс дисциплины состоит из 11 тем , всего 108 часов – лекции 32 часа, практические занятия 16 часов, СРС 60 часов). В конце изучения дисциплины дифференцированный зачет.

Тема №1 «Теоретические основы безопасности операционных систем»
Тема №2 «Концептуальные основы операционных систем»
Тема №3 «Идентификация и аутентификация»
Тема №4 «Управление доступом»
Тема №5 «Протоколирование и аудит»
Тема №6 «Криптографическая защита в современных операционных системах»
Тема №7 «Контроль целостности данных и компонентов ОС»
Тема №8 «Экранирование в современных ОС»
Тема №9 «Обеспечение отказоустойчивости и безопасного восстановления в современных ОС»
Тема №10 «Безопасное управление ОС»
Тема №11 «Аудит безопасности ОС»

Слайд 8 (рекомендуемая литература)

Основные учебники:

а) основная литература

- Сетевые операционные системы:Доп. МО РФ в кач. учеб. пособия для вузов/В.Г.Олифер, Н.А.Олифер.-3-е изд.-СПб. :Питер,2016.-668 с.:ил.-(Учебник для вузов). Библиогр.: с. 650-651.
- Таненбаум Э. Современные операционные системы/Э.Таненбаум; Пер. с англ.-4-е изд.-СПб.:Питер,2015.-1115 с.:ил.-(Классика computer science). Библиогр.: с. 1115

б) дополнительная литература

- Семенов Ю.А. Телекоммуникационные технологии. М: ИТЭФ-МФТИ, 2014.

Раздать список литературы!!!

Итак, вводная часть лекции окончена, перейдем к основной тематике лекции.

Фундаментальные знания по архитектуре, возможностям и функционированию операционных систем были вами получены в рамках изучения дисциплины "Операционные системы" в 5 и 6 семестре (3 курс).

В рамках изучения данной дисциплины будет сделан упор на изучение вопросов обеспечения безопасности в современных ОС, эксплуатации защищенных ОС.

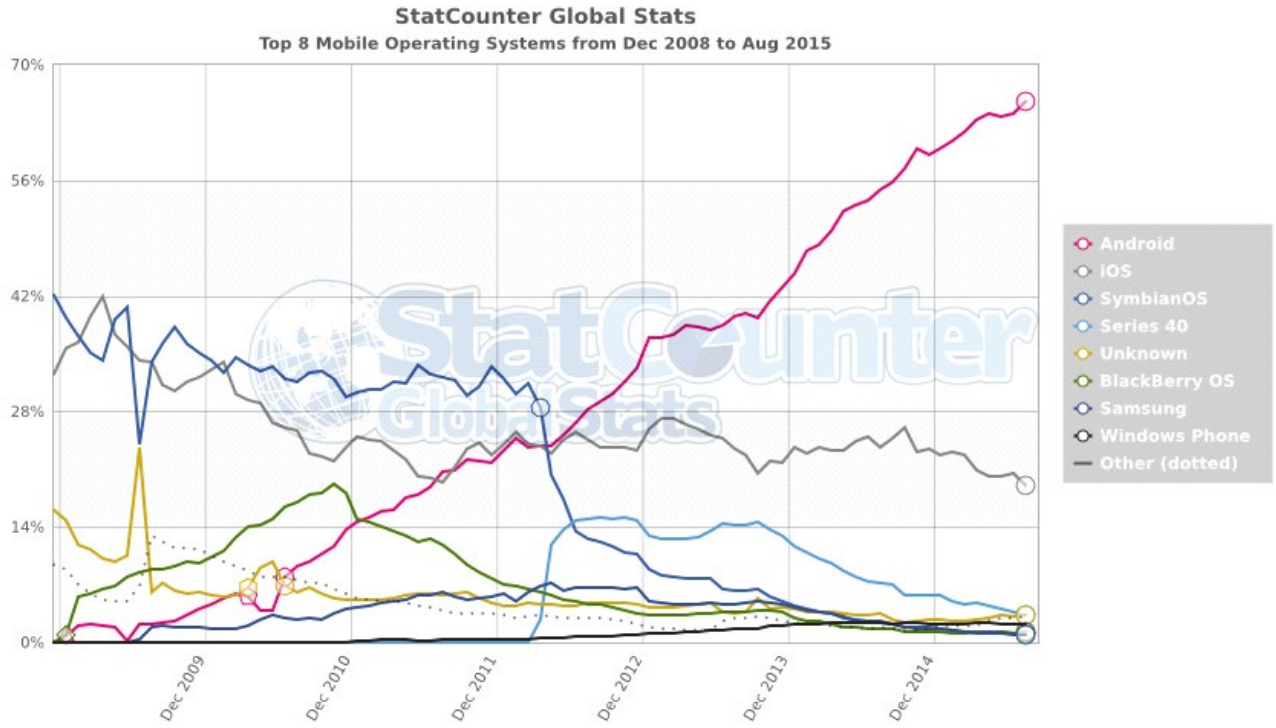
Слайд 9 (Текущее состояние развития ОС)

Операционная система, сокр. ОС (англ. operating system, OS) — комплекс взаимосвязанных программ, предназначенных для управления ресурсами вычислительного устройства и организации взаимодействия с пользователем.

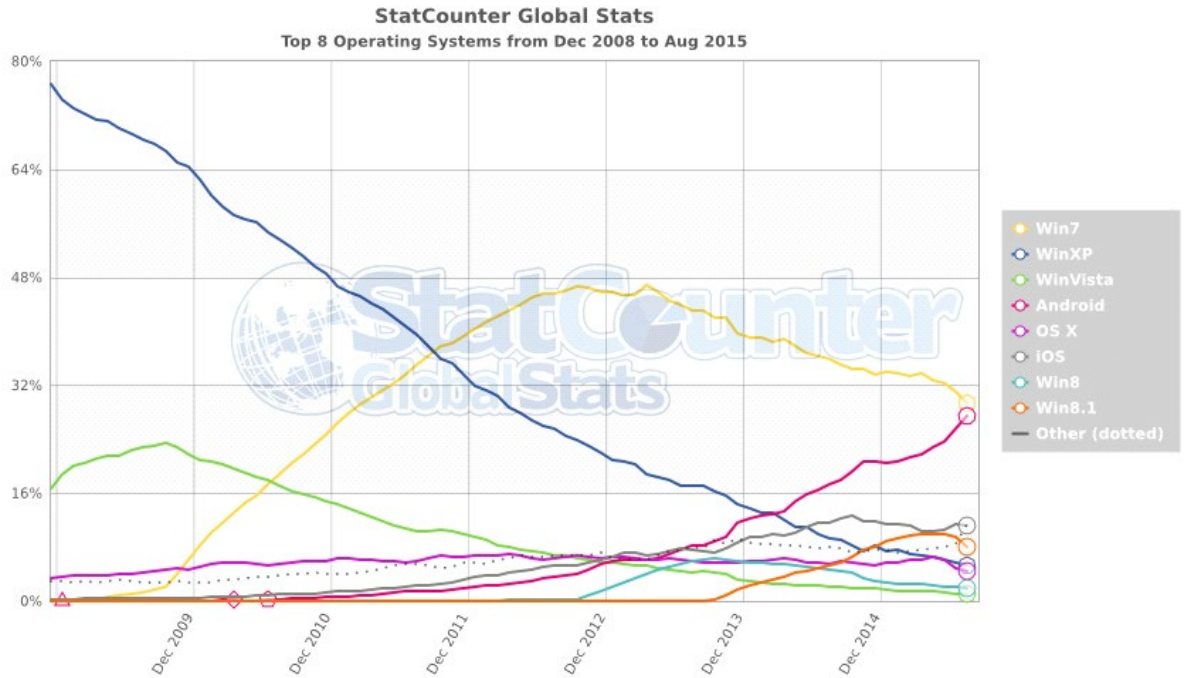
ОС является частью системного программного обеспечения.

Согласно сервиса Global Stats в период с декабря 2008 года по август 2015 статистика использования ОС на Desktop в мире является следующей:

ОС для мобильных платформ распределились следующим образом:



Общая статистика по ОС:



97% суперкомпьютеров из TOP500 в мире работает под управлением специализированного дистрибутива Linux, 37% серверов в сети Интернет управляется дистрибутивами Linux, 30% BSD и другими Unix-системами (HP-UX, Solaris, …), 33 % ОС семейства Windows.

Кроме операционных систем общего пользования широко развиваются операционные системы для сетевых устройств, встраиваемых устройств, специализированные ОС и др..

В настоящий момент в мире насчитываются тысячи ОС и их дистрибутивов, например, GNU/Linux, FreeBSD, NetBSD, OpenBSD, Windows XP, Windows 7, Windows 8.1, Android, iOS, IOS, SonicOS, JunOS, ScreenOS, PalmOS, AmigaOS, Solaris, OpenSolaris, OS X, QNX, BeOS, DOS, FreeDOS, Unix, Minix, HP-UX, Gaia, FlexOS, z/OS, AIX, LynxOS, Xbox, Mobilinux, Tizen, Bada, VxWorks, IRIX, ReactOS, Haiku, Timos, OpenVMS, OpenWRT, RouterOS, AirOS, ChromeOS, WebOS и др.

Тенденции развития современных ОС.

- Увеличение количества мобильных платформ, каналов доступа в сеть.
- Поддержка новых протоколов и сетевых стандартов, например, IPv6, HTML5.
- Развитие технологий виртуализации и облачных сервисов, например, Windows Azure.
- Поддержка многоядерных процессоров, распределенных и параллельных вычислений.
- Поддержка различных архитектур процессоров (x86/x64, ARM, MIPS, PowerPC).
- Развитие магазинов приложений и репозитариев программ.
- Развитие файловых систем.
- Унификация ОС для использования на мобильных и стационарных устройствах (Windows 8, Ubuntu Linux).
- Широкая интеграция и синхронизация между ОС на различных устройствах.
- Переход к использованию Web-приложений в качестве альтернативы ПО в ОС.
- Усиление роли механизмов безопасности и защиты.

Классификации ОС.

Операционные системы классифицируются по:

- количеству одновременно работающих пользователей: однопользовательские, многопользовательские;
- числу процессов, одновременно выполняемых под управлением системы: однозадачные, многозадачные;
- количеству поддерживаемых процессоров: однопроцессорные, многопроцессорные;
- разрядности кода ОС: 8-разрядные, 16-разрядные, 32-разрядные, 64-разрядные;
- типу интерфейса: командные (текстовые) и объектно-ориентированные (графические);
- типу доступа пользователя к ЭВМ: с пакетной обработкой, с разделением времени, реального времени;

- типу ядра: монолитные, гибридные, с микроядром;
- типу распространения: коммерческие, свободные;
- сфере использования: ПК, серверы, планшеты, смартфоны, суперкомпьютеры, игровые консоли, встраиваемые устройства, телевизоры, холодильники и другая бытовая техника, сетевые устройства и прочее;
- по семействам: Unix (Unix System V - Solaris, SCO Unix; Berkley Software Distribution Unix - FreeBSD, NetBSD, OpenBSD; Linux - RHEL, Debian, …), Windows (Windows XP, Windows 7, Windows Server), DEC (VAX/VMS, RT-11),
- типу использования ресурсов: сетевые, локальные.

Многопользовательские операционные системы, в отличие от однопользовательских, поддерживают одновременную работу на ЭВМ нескольких пользователей за различными терминалами.

Понятие многозадачности означает поддержку параллельного выполнения нескольких программ, существующих в рамках одной вычислительной системы, в один момент времени. Однозадачные ОС поддерживают режим выполнения только одной программы в отдельный момент времени.

Многопроцессорные ОС, в отличие от однопроцессорных, поддерживают режим распределения ресурсов нескольких процессоров для решения той или иной задачи.

По типу пользовательского интерфейса делятся на объектно-ориентированные (как правило, с графическим интерфейсом) и командные (с текстовым интерфейсом).

По типу доступа к ресурсам ЭВМ ОС делятся на ОС пакетной обработки, в которых из программ, подлежащих выполнению, формируется пакет (набор) заданий, вводимых в ЭВМ и выполняемых в порядке очередности с возможным учетом приоритетности; разделения времени (TSR), обеспечивающих одновременный диалоговый (интерактивный) режим доступа к ЭВМ нескольких пользователей на разных терминалах, которым по очереди выделяются ресурсы машины, что координируется операционной системой в соответствии с заданной дисциплиной обслуживания; реального времени, обеспечивающих определенное гарантированное время ответа машины на запрос пользователя с управлением им какими-либо внешними по отношению к ЭВМ событиями, процессами или объектами.

Отдельному рассмотрению подлежат защищенные ОС. Но перед этим определим основные угрозы безопасности и атаки, от которых им необходимо защищаться.

Классификация угроз безопасности ОС.

Определения:

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации.

Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.

Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.

Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Выделяют и другие категории модели безопасности:

Достоверность — свойство соответствия предусмотренному поведению или результату;

Аутентичность или подлинность — свойство, гарантирующее, что субъект или ресурс идентичен заявленным.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

Атака — реализация угрозы.

Риск — это вероятностная оценка величины возможного ущерба в результате успешно проведенной атаки.

Классификация угроз ОС

- По характеру воздействия: пассивное и активное.
- По цели воздействия: нарушение конфиденциальности информации или ресурсов, нарушение целостности информации, нарушение работоспособности (доступности) системы.
- По условию начала воздействия: безусловные, по запросу от атакуемой системы, атака по наступлению события.
- По расположению атакующего: локальная или удаленная.
- По типу ресурсов: локальные или сетевые.
- По принципу воздействия на операционную систему: через легальные каналы, через скрытые каналы, через новые каналы.
- По типу используемой уязвимости: ошибки и НДВ в ОС, ошибки конфигурирования, ранее внедренная программная или аппаратная закладка.

- По способу действий злоумышленника (нарушителя): в интерактивном режиме (вручную) или в пакетном режиме (с помощью специально написанной программы).
- По объекту атаки: операционная система в целом, объекты операционной системы (файлы, устройства и т.д.), субъекты операционной системы (пользователи, системные процессы и т.д.), каналы передачи данных.
- По используемым средствам атаки: штатные средства операционной системы без использования дополнительного программного обеспечения; программное обеспечение третьих фирм (компьютерные вирусы, exploits, отладчики, сетевые мониторы и сканеры и т.д.); специально разработанное программное обеспечение.
- По состоянию атакуемого объекта операционной системы на момент атаки: хранение; передача; обработка.
- и др.

По характеру воздействия:

Пассивным воздействием на распределенную вычислительную систему можно назвать воздействие, которое не оказывает непосредственного влияния на работу системы, но способно нарушать ее политику безопасности.

Под активным воздействием на ОС понимается воздействие, оказывающее непосредственное влияние на работу системы (изменение конфигурации ОС, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности.

По цели воздействия

Этот классификационный признак является прямой проекцией трех основных типов угроз: раскрытия, нарушения целостности и отказа в обслуживании.

Цель большинства атак - получить несанкционированный доступ к информации. Существуют две принципиальные возможности такого доступа: перехват и искажение. Перехват - это получение информации без возможности ее искажения. Примером перехвата может служить прослушивание канала в сети. Такая атака является пассивным воздействием и ведет к нарушению конфиденциальности информации.

Искажение информации означает полный контроль над информационным потоком между объектами системы или возможность передачи сообщений от имени другого объекта. Очевидно, что искажение информации ведет к нарушению ее целостности, то есть представляет собой активное воздействие.

Принципиально иной целью атаки является нарушение работоспособности системы. В этом случае основная цель атакующего -

добиться, чтобы операционная система на атакованном объекте вышла из строя и, следовательно, для всех остальных объектов системы доступ к ресурсам данного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая атака "отказ в обслуживании".

По условию начала осуществления воздействия

При безусловной атаке ее начало не зависит от состояния системы атакуемого объекта, то есть воздействие осуществляется немедленно.

При атаке по запросу от атакуемой системы атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия.

При атаке по событию атакующий осуществляет постоянное наблюдение за состоянием операционной системы объекта атаки и при возникновении определенного события в этой системе начинает воздействие.

По наличию обратной связи с атакуемым объектом

Инициатор удаленной атаки без обратной связи не реагирует ни на какие изменения, происходящие на атакуемом объекте. Воздействие данного вида обычно осуществляется передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны.

Если атакующему требуется получить ответ на некоторые запросы, переданные на объект воздействия, то данная атака будет являться атакой с обратной связью.

По принципу воздействия на операционную систему

- использование известных (легальных) каналов получения информации; например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно, т. е. разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;
- использование скрытых каналов получения информации; например угроза использования злоумышленником недокументированных возможностей ОС;
- создание новых каналов получения информации с помощью программных закладок.

Примеры типичных атак на ОС

Получение доступа к информации не легитимным пользователем

Атакующий сканирует файловую систему в надежде обнаружить файлы с некорректными правами доступа.

Поиск и сбор информации

Программный агент под правами пользователя получает доступ ко всем его файлам на ФС, осуществляет поиск и сбор интересующей информации.

Перехват сетевого трафика
Получение пользовательских паролей путем анализа открытых протоколов (Telnet, POP3, HTTP)

Модификация кода исполняемых программ
Внедрение программных агентов в исполняемые программы ОС или прикладное ПО.

Использование вычислительных ресурсов системы
Запуск жадных программ (fork-бомб) для исчерпания ресурсов системы или скрытное использование вычислительных ресурсов не легитимными программами (bitcoin-майнинг и др.)

Повышение привилегий/Превышение полномочий
Атакующий, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя.

Восстановление удаленных данных (сборка мусора)
Во многих ОС информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Атакующий восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты.

Подмена доверенного компонента ОС или внедрение ложного объекта
Примером является подмена файла, отвечающего за проверку авторизации или внедрение динамически загружаемой библиотеки с целью перехвата функций.

Нарушение работоспособности ОС или ее компонентов
Проведение DoS/DDoS атак на сетевые службы, удаление критичных компонентов ОС.

Нарушение работоспособности аппаратных компонентов
Выведение из строя аппаратных компонентов посредством износа или эксплуатации ошибок в драйверах или микрокоде.

Уничтожение или модификация информации
Удаление информации в следствии нелегальных действий легального пользователя или атакующего.

Получение данных авторизации и другой ключевой информации

Сбор файлов с паролями, получение хешей для дальнейшего перебора, сбор закрытых ключей и сертификатов, баз данных, содержащих данные авторизации.

Распространение вирусов и установка программных агентов
Вирусы распространяются зачастую посредством невнимательности пользователей или эксплуатации уязвимостей в ПО. Программные агенты устанавливаются для закрепления и эксплуатации доступа.

Перебор паролей/слабые пароли и ключи
Осуществление многочисленных попыток авторизации до успешного. Выделяют полный перебор (brute-force), перебор по словарю, перебор с использованием знаний о пользователе.

Получение удаленного доступа к ОС
Посредством эксплуатации программных закладок, использования некорректных настроек или ошибок в ПО, халатности пользователя.

При осуществлении APT-атак одновременно используются различные векторы.

Нарушители информационной безопасности в ОС.

Внутренние (пользователь в системе или в сети) и внешние нарушители.

Разработчики, администраторы, пользователи, сторонние лица.

Понятие защищенных ОС.

Операционную систему называют защищенной, если она предусматривает средства защиты от основных классов угроз.

Основным назначением операционной системы (ОС) является обеспечение корректного совместного использования разнообразных ресурсов вычислительной системы (ВС) несколькими прикладными задачами. Кроме того, ОС предоставляет высокоуровневый интерфейс доступа к разнообразным устройствам. В отличие от обычной ОС, ЗОС регулирует доступ к системным ресурсам исходя из соображений не только возможности их совместного использования конкурирующими приложениями, но и исходя из принятой в данной конкретной ЗОС политики безопасности (ПБ). ПБ оперирует абстрактными понятиями субъекта и объекта. Конкретные наборы правил, на основании которых делается вывод о предоставлении доступа субъекта к объекту, сведены в различные модели безопасности (МБ). Таким образом, основным отличием ЗОС от ОС является наличие в первой ПБ. А основной задачей при проектировании ЗОС является

задача внедрения абстрактной ПБ в конкретную ОС. При этом возникает две основные проблемы. Во-первых, необходимо адекватно отобразить множество субъектов и объектов ОС на множество субъектов и объектов ПБ. Во-вторых, необходимо обеспечить такой механизм взаимодействия всех компонент ВС друг с другом, чтобы он однозначно соответствовал правилам взаимодействия объектов и субъектов внедряемой ПБ.

Примеры защищенных ОС

Trusted Solaris — основанная на Solaris операционная система с гарантированной безопасностью компании Sun Microsystems.
Использует модель принудительного контроля доступа. В составе Trusted Solaris реализованы идентификация и аутентификация, контроль доступа, основанный на ролях, аудит.

Trusted Solaris 8 сертифицирована по Common Criteria по уровню EAL4+ в профилях защиты (protection profiles) CAPP, RBACPP и LSPP.

Проект TrustedBSD представляет набор расширений безопасности для операционной системы FreeBSD. Он был начат с целью реализации концепций Common Criteria for Information Technology Security Evaluation и Orange Book (Оранжевой книги). Проект TrustedBSD сфокусирован на аудите событий безопасности списков контроля доступа (ACL), расширении атрибутов файловой системы и мандатном управлении доступом (MAC).

ОС МСВС (Мобильная система Вооружённых Сил)— защищённая операционная система общего назначения. Предназначена для построения стационарных защищённых автоматизированных систем.
Разработчик ОС МСВС — Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В. В. Соломатина (ВНИИНС). Представляет собой дистрибутив GNU/Linux, являющийся многопользовательской многозадачной сетевой ОС. Функционирует на аппаратных платформах Intel, SPARC (Эльбрус−90микро), IBM System/390 и MIPS, поддерживает многопроцессорные конфигурации (SMP). Содержит средства мандатного управления доступом, списки контроля доступа, ролевую модель.
В качестве среды рабочего стола используется elk, основанный на QVWM.
Менеджер пакетов — RPM.

ОС сертифицирована по 2 классу защищенности информации от НСД согласно РД и по 1 уровню классификации контроля отсутствия не декларированных возможностей согласно РД. Возможна обработка информации до уровня "совершенно секретно" включительно.

Astra-Linux - операционная система специального назначения, созданная на базе ядра Linux. Базовый дистрибутив - Debian. Разработчик - ОАО НПО РусБитех. Имеет версию "общего назначения" - Орел, и версии специального назначения - для создания защищенных АС.

- Очистка оперативной и внешней памяти и гарантированное удаление файлов: ОС выполняет очистку неиспользуемых блоков файловой системы непосредственно при их освобождении.
- Маркировка документов: разработанный механизм маркировки позволяет серверу печати (CUPS) проставлять необходимые учётные данные в выводимых на печать документах. Мандатные атрибуты автоматически связываются с заданием для печати на основе мандатного контекста получаемого сетевого соединения. Вывод на печать документов без маркировки субъектами доступа, работающими в мандатном контексте с грифом выше «несекретно», невозможен.
- Регистрация событий: реализована оригинальная подсистема протоколирования, интегрированная во все компоненты операционной системы и осуществляющая надёжную регистрацию событий с использованием специального сервиса.
- Механизмы защиты информации в графической подсистеме: графическая подсистема включает в себя X-сервер Xorg, пользовательский рабочий стол Fly, а также ряд программных средств, предназначенных как для пользователей, так и для администраторов системы. Проведена работа по созданию и встраиванию в графическую подсистему необходимых механизмов защиты информации,

обеспечивающих выполнение мандатного разграничения доступа в графических приложениях.

- Механизм контроля замкнутости программной среды: реализован механизм, обеспечивающий проверку неизменности и подлинности загружаемых исполняемых файлов в формате ELF.
- Проверка производится на основе проверки векторов аутентичности, рассчитанных в соответствии с ГОСТ Р 34.10-2001 и внедряемых в исполняемые файлы в процессе сборки.
- Контроль целостности: для решения задач контроля целостности применяется функция хэширования в соответствии с ГОСТ Р 34.11-94.1

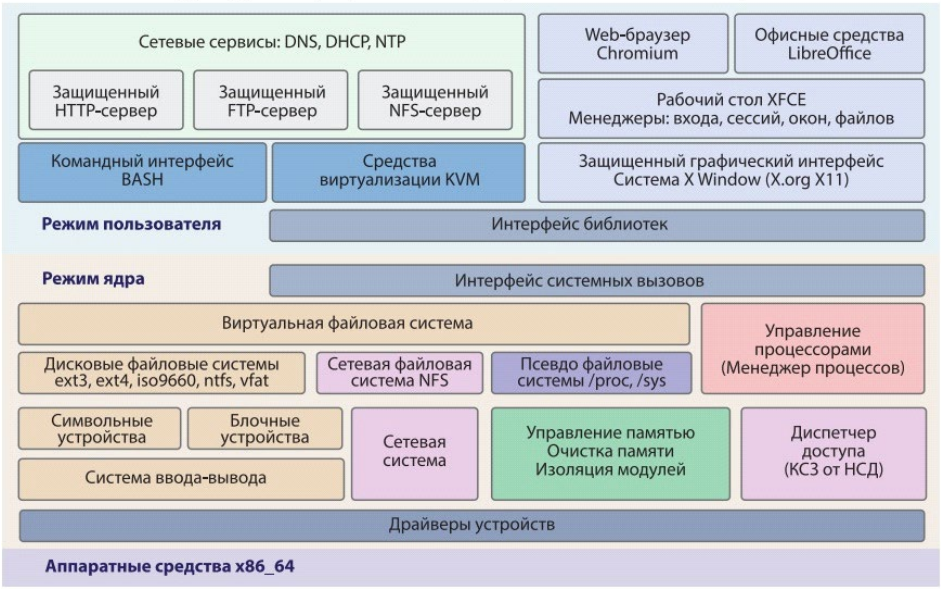
В операционной системе реализован механизм мандатного разграничения доступа. В Astra Linux Special Edition существует 8 мандатных уровней доступа (от 0 до 7). При работе на разных мандатных уровнях и категориях операционная система формально рассматривает одного и того же пользователя, но с различными мандатными уровнями, как разных пользователей и создает для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается.

ОС соответствует:

- требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 3 классу защищённости;
- требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссии России, 1999) - по 2 уровню контроля;
- реальным и декларируемым в документации функциональным возможностям.

ОС Заря, Заря-ЦОД, Заря РВ - семейство защищенных операционных систем военного назначения. Разработчик - ЦНИИ ЭИСУ. Системы созданы на основе ОС GNU/Linux. Могут использоваться для управления АРМ, серверами, сетевым оборудованием. Имеет сертификат МО РФ для работы со сведениями составляющими государственную тайну с грифом не выше "совершенно секретно". Имеет 2 класс защиты от НСД и 2 уровень контроля НДВ.

Структура защищенной операционной системы «Заря»



Принципы построения защищенных ОС.

Основу технологии создания защищенных систем составляют следующие принципы.

- *Принцип интегрированности* — средства защиты должны быть встроены в систему таким образом, чтобы все без исключения механизмы взаимодействия находились под их контролем. При разработке защищенной ОС следование этому принципу означает осуществление тотального контроля. Самый простой метод тотального контроля состоит в ограничении числа механизмов взаимодействия и интеграции средств защиты прямо в эти механизмы.
- *Принцип инвариантности* — средства защиты не должны зависеть от особенностей реализации приложений и не должны учитывать логику их функционирования, напротив они должны быть универсальны для всех типов взаимодействий и отображать их на отношениях между субъектами и объектами. Для ОС инвариантность средств защиты может быть достигнута путем применения строго регламентированной парадигмы функционирования приложений, ограничивающей способы взаимодействий.
- *Принцип унификации* — должно существовать однозначное соответствие между контролируемыми взаимодействиями субъектов и

объектов и операциями доступа, управление которыми описывается моделями безопасности. Это позволяет придать универсальность средствам защиты и использовать их без изменения как для реализации различных моделей безопасности, так и для контроля доступа к объектам различной природы. Следование этому принципу при разработке ОС приводит к необходимости создания универсального интерфейса доступа, объединяющего все способы взаимодействия между субъектами и объектами, все функции которого однозначным образом отображаются на множество операций, описываемых моделью безопасности.

- *Принцип адекватности* — для обеспечения реальной способности противостоять атакам необходимо устранить источники возникновения уязвимостей, на использовании которых основаны все механизмы реализации атак. Одной из основных причин появления уязвимостей является отсутствие последовательного подхода к контролю доступа. Существующие системы содержат привилегированные средства и службы, которые передают пользователям часть своих полномочий в обход средств контроля. Любая программная ошибка в таких средствах ведет к появлению уязвимости. Для операционной системы устранение причин появления уязвимостей означает обязательный контроль доступа на основе универсального интерфейса и единого механизма взаимодействия без каких-либо исключений, и минимизацию объема доверенного кода самих средств защиты с целью уменьшения вероятности появления в них ошибок.
- *Принцип корректности* — средства защиты должны реализовывать управление доступом в соответствии с формальными моделями. Наличие непротиворечивой модели безопасности позволяет формально обосновывать безопасность системы, предоставляет объективный критерий корректности ее работы, а также может служить основой для построения исчерпывающих тестов, проверяющих правильность работы средств защиты для всех ситуаций. Для защищенной ОС этот принцип предопределяет управление доступом на основе формальных моделей безопасности.

В РФ зачастую используется Linux с внесенными в него модификациями.

Специальных стандартов защищенности ОС не существует. Для оценки защищенности ОС используются стандарты, разработанные для компьютерных систем вообще. Как правило, сертификация ОС по некоторому классу защиты сопровождается составлением требований к адекватной политике безопасности, при безусловном выполнении которой защищенность конкретного экземпляра ОС будет соответствовать требованиям соответствующего класса защиты.

Существует ряд основополагающих документов, в которых регламентированы основные подходы к проблеме информационной безопасности:

- оранжевая (по цвету обложки) книга МО США
- гармонизированные критерии европейских стран
- руководящие документы Гостехкомиссии при Президенте РФ/ФСТЭК
- рекомендации X.800 по защите распределенных систем
- федеральный закон "Об информации, информатизации и защите информации".

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

Акты федерального законодательства:

- Международные договоры РФ;
- Конституция РФ;
- Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- Указы Президента РФ;
- Постановления Правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Методические документы государственных органов России:

- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ;
- Стандарты информационной безопасности.

Международные стандарты

BS 7799 Британский стандарт. Практические правила управления информационной безопасностью, построения СУИБ (системы управления информационной безопасностью).

ISO/IEC 17799:2005 — Международный стандарт, базирующийся на BS 7799-1:2005.

ISO/IEC 27000xxx — Серия международных стандартов по управлению информационной безопасностью.

Государственные (национальные) стандарты РФ

ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.

ГОСТ Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

Оранжевая книга.

Критерии определения безопасности компьютерных систем (англ. Trusted Computer System Evaluation Criteria) — стандарт Министерства обороны США, устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе. Критерии используются для определения, классификации и выбора компьютерных систем, предназначенных для обработки, хранения и поиска важной или секретной информации.

Критерии, часто упоминающиеся как Оранжевая книга, занимают центральное место среди публикаций «Радужной серии» Министерства обороны США. Изначально выпущенные Центром национальной компьютерной безопасности США в качестве орудия для Агентства национальной безопасности в 1983 году и потом обновлённые в 1985.

Согласно TCSEC, для оценивания компьютерных систем выделено четыре основных группы безопасности, которые в свою очередь делятся на классы безопасности:

группа D - Minimal Protection (минимальная защита) - объединяет компьютерные системы, не удовлетворяющие требованиям безопасности высших классов. В данном случае группа и класс совпадают;

группа C - Discretionary Protection (избирательная защита) - объединяет системы, обеспечивающие набор средств защиты, применяемых пользователем, включая средства общего контроля и учета субъектов и их действий.

Эта группа имеет два класса:

1) класс C1 - Discretionary Security Protection (избирательная защита безопасности) - объединяет системы с разделением пользователей и данных;

2) класс C2 - Controlled Access Protection (защита контролируемого доступа) - объединяет системы, обеспечивающие более тонкие средства защиты по сравнению с системами класса C1, делающие пользователей индивидуально различимыми в их действиях посредством процедур контроля входа и контроля за событиями, затрагивающими безопасность системы и изоляцию данных. Примечание: Компьютерные системы, которые могут

быть использованы для нужд министерства обороны США, должны как минимум иметь рейтинг безопасности C2.

группа B - Mandatory Protection (полномочная защита) - имеет три класса:

1) класс B1 - Labeled Security Protection (меточная защита безопасности) - объединяет системы, удовлетворяющие всем требованиям класса C2, дополнительно реализующие заранее определенную модель безопасности, поддерживающие метки субъектов и объектов, полный контроль доступа. Вся выдаваемая информация регистрируется, все выявленные при тестировании недостатки должны быть устранены;

2) класс B2 - Structured Protection (структурированная защита) - объединяет системы, в которых реализована четко определенная и задокументированная формализованная модель обеспечения безопасности, а меточный механизм разделения и контроля доступа, реализованный в системах класса B1, распространен на всех пользователей, все данные и все виды доступа. По сравнению с классом B1 ужесточены требования по идентификации пользователей, контролю за исполнением команд управления, усилена поддержка администратора и операторов системы. Должны быть проанализированы и перекрыты все возможности обхода защиты. Системы класса B2 считаются "относительно неуязвимыми" для несанкционированного доступа;

3) класс B3 - Security Domains (области безопасности) - объединяет системы, имеющие специальные комплексы безопасности. В системах этого класса должен быть механизм регистрации всех видов доступа любого субъекта к любому объекту. Должна быть полностью исключена возможность несанкционированного доступа. Система безопасности должна иметь небольшой объем и приемлемую сложность для того, чтобы пользователь мог в любой момент протестировать механизм безопасности. Системы этого класса должны иметь средства поддержки администратора безопасности; механизм контроля должен быть распространен вплоть до сигнализации о всех событиях, затрагивающих безопасность; должны быть средства восстановления системы.

Системы этого класса считаются устойчивыми к несанкционированному доступу.

группа A - Verified Protection (проверяемая защита) - объединяет системы, характерные тем, что для проверки реализованных в системе средств защиты обрабатываемой или хранимой информации применяются формальные методы. Обязательным требованием является полная документированность всех аспектов проектирования, разработки и исполнения систем. Выделен единственный класс:

1) класс A1 - Verified Desing (проверяемая разработка) - объединяющий системы, функционально эквивалентные системам класса B3 и не требующие каких-либо дополнительных средств.

Отличительной чертой систем этого класса является анализ формальных спецификаций проекта системы и технологии исполнения,

дающий в результате высокую степень гарантированности корректного исполнения системы. Кроме этого, системы должны иметь мощные средства управления конфигурацией и средства поддержки администратора безопасности.

Требования	К л а с с ы					
	C1	C2	B1	B2	B3	A1
1 Требования к политике безопасности						
1.1 Произвольное управление доступом	+	+	=	=	+	=
1.2 Повторное использование объектов	–	+	=	=	=	=
1.3 Метки безопасности	–	–	+	+	=	=
1.4 Целостность меток безопасности	–	–	+	+	=	=
1.5 Принудительное управление доступом	–	–	+	+	=	=
2 Требования к подотчетности						
2.1 Идентификация и аутентификация	+	+	+	=	=	=
2.2 Предоставление надежного пути	–	–	–	+	+	=
2.3 Аудит	–	+	+	+	+	=

3 Требования к гарантированности						
3.1 Операционная гарантированность						
3.1.1 Архитектура системы	+	+	+	+	+	=
3.1.2 Целостность системы	+	=	=	=	=	=
3.1.3 Анализ тайных каналов передачи информации	–	–	–	+	+	+
3.1.4 Надежное администрирование	–	–	–	+	+	=
3.1.5 Надежное восстановление	–	–	–	–	+	=
3.2 Технологическая гарантированность						
3.2.1 Тестирование	+	+	+	+	+	+
3.2.2 Верификация спецификаций архитектуры	–	–	+	+	+	+
3.2.3 Конфигурационное управление	–	–	–	+	=	+
3.2.4 Надежное распространение	–	–	–	–	–	+

Системы общего пользования (Windows XP, дистрибутивы Linux, FreeBSD) относятся к классу С2.

4 Требования к документации						
4.1 Руководство пользователя по средствам безопасности	+	=	=	=	=	=
4.2 Руководство администратора по средствам безопасности	+	+	+	+	+	+
4.2 Тестовая документация	+	=	=	+	=	+
4.4 Описание архитектуры	+	=	+	+	+	+

Критерии ФСТЭК/Руководящие документы Гостехкомиссии.

В 1992 году ФСТЭК (Гостехкомиссия) опубликовала Руководящий документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

В документе устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Требования этих классов в основном соответствуют требованиям "Оранжевой книги". Класс 7 - D, класс 6 - C1, класс 1 - A1.

Наиболее существенные отличия:

- в 5 классе вводятся требования по целостности КСЗИ, которые усиливаются в 3 и 4 классе;
- в классе 5 требования к процедурам идентификации и аутентификации менее сильны, чем в "Оранжевой книге";
- начиная с класса 4 требования к запрету повторного использования информации более сильны, чем в "Оранжевой книге".

Где используется этот РД? Например при реализации автоматизированных систем. На него ссылается РД "Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации." При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

- не ниже 4 класса - для класса защищенности АС 1В;
- не ниже 3 класса - для класса защищенности АС 1Б;
- не ниже 2 класса - для класса защищенности АС 1А.

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

Общие критерии.

Общие критерии (Common Criteria, CC, или ОК). Международный стандарт (ISO/IEC 15408, последняя российская версия — 15408-3-2008) по компьютерной безопасности. Common Criteria не приводит списка требований по безопасности или списка особенностей, которые должен содержать продукт. Вместо этого он описывает инфраструктуру (framework), в которой потребители компьютерной системы могут описать требования, разработчики могут заявить о свойствах безопасности продуктов, а эксперты по безопасности определить, удовлетворяет ли продукт заявлениям. Таким образом, Common Criteria позволяет обеспечить условия, в которых процесс описания, разработки и проверки продукта будет произведён с необходимой скрупулёзностью.

На сайте ОК указан список всех продуктов по разделам, которые были сертифицированы по CC.

Среди них IBM z/OS Version 2 Release 1 with RACF - EAL5+, ALC_FLR.3, Windows 8 и Windows Server 2012 (подали заявку), IBM z/OS Version 2 Release 1 - EAL4+, ALC_FLR.3, Oracle Solaris 11.1 - EAL4+, ALS_FLR.3, SUSE Linux/RHEL 6.2 - EAL4+, ALC_FLR.3, Microsoft Windows Server 2008 R2 Hyper-V Release 6.1.7600 - EAL4+, ALC_FLR.3, Extreame Networks ExtreameXOS Network Operating System v12.3.6.2 - EAL3, ALC_FLR.2, Microsoft Windows Mobile 6.1 - EAL4+, ALC_FLR.1, Microsoft Windows Vista - EAL1.

В разработке Общих критериев участвовали Национальный институт стандартов и технологии 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).

ОБЩИЕ ПОЛОЖЕНИЯ

Общие критерии разработаны таким образом, чтобы удовлетворить потребности трех категорий пользователей: потребителей объекта оценки, разработчиков объекта оценки и оценщиков 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 преднамеренных или непреднамеренных действий. Защищенность от этих трех типов угроз обычно называют конфиденциальностью, целостностью и доступностью.

Вне рамок компетенции ОК находятся:

- оценка административных мер безопасности;
- оценка технических аспектов безопасности типа ПЭМИН;
- создание методик оценки;
- оценка криптографических методов и алгоритмов.

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.

Например,

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 и используют одну и ту же организацию и терминологию.

Одной из основных структур ОК является Профиль защиты (ПЗ), определенный как набор требований, который состоит из компонентов или пакетов функциональных требований ОК и одного из уровней гарантии, при необходимости усиленного дополнительными компонентами гарантии из ОК. Профиль защиты предназначен для многократного использования и определяет совокупность требований безопасности, 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. Задание по Безопасности определяет набор требований безопасности для конкретного объекта оценки. Оно включает также спецификацию объекта оценки в виде функций безопасности (ФБ), которые должны обеспечить выполнение требований безопасности и мер гарантии оценки.

Функциональный элемент - это функциональное требование безопасности, дальнейшее разделение которого не меняет значимо результат оценки; является наименьшим функциональным требованием безопасности, идентифицируемым и признаваемым в ОК.

Именование функционального элемента, например, FDP_IFF.4.2
F-функциональный элемент
DP - класс "Защита данных пользователя"
_IFF - семейство "Функции управления информационными потоками"
.4 - четвертый компонент "Частичное устранение неразрешимых информационных потоков"
.2 - второй элемент компонента.

Доверие к безопасности формируется через оценку.
Элемент доверия – требование безопасности, при дальнейшем разделении которого не изменяется значимый результат оценки. Он является наименьшим требованием безопасности, распознаваемым в ОК.

Именование элементов доверия, например, APE_ENV
A - элемент доверия (Assurance)
PE - класс "Оценка профиля защиты"
_ENV - семейство "Среда безопасности"

Оценочные уровни доверия (EAL).

Например, для оценки операционной системы Windows Server 2008 по CC был использован профиль "Операционные системы общего назначения" - GPOSPP.
Продукт проверяется на соответствие установленным требованиям профиля защиты. Степень соответствия ассоциируется с оценочным уровнем доверия.

Введено 7 оценочных уровня доверия:
EAL1 (ОУД) - функционально проверенный проект. ОУД1 - самый низкий уровень гарантии, для которого оценка является значащей и экономически оправданной. ОУД 1 предназначен для обнаружения очевидных ошибок при минимальных издержках. Компоненты ОУД 1 обеспечивают минимальный уровень гарантии путем анализа функциональной и интерфейсной спецификаций ОО и результатов независимого тестирования каждой из функций безопасности.
EAL2 - структурно проверенный проект. EAL2 применим, когда разработчики или пользователи требуют умеренно низкий уровень независимо гарантированной безопасности при отсутствии полного отчета о разработке. Компоненты EAL2 обеспечивают гарантию путем анализа функций безопасности и проекта высокого уровня подсистем ОО. Анализ поддержан независимым тестированием каждой из функций безопасности,

актом испытаний разработчиком "черного ящика" и свидетельством поиска разработчиком явных уязвимых мест.

EAL3 - методически проверенный и протестированный проект. EAL3 позволяет добросовестному разработчику получить максимальную гарантию безопасности на стадии разработки проекта без существенного изменения обычных методов разработки. Поэтому EAL3 применим, когда разработчики или пользователи требуют умеренного уровня независимо гарантированной безопасности и полного исследования продукта и процесса разработки без существенных технических затрат.

Компоненты EAL3 обеспечивают гарантию путем анализа функций безопасности и проекта высокого уровня подсистем ОО. Анализ поддержан независимым тестированием функций безопасности, актом испытаний разработчиком "серого ящика", независимым подтверждением выборочных результатов испытания разработчиком и свидетельством поиска разработчиком явных уязвимых мест. EAL3 обеспечивает также дополнительную гарантию путем включения средств контроля среды разработки и управления конфигурацией ОО.

EAL4 - методически проработанный и проверенный проект. EAL4 позволяет разработчику получить максимальную гарантию безопасности при проектировании, основанном на хороших коммерческих методах разработки. EAL4 - самый высокий уровень, который, вероятно, будет экономически целесообразен для ориентировки на существующие типы продуктов. Поэтому EAL4 применим, когда разработчики или пользователи требуют умеренно-высокий уровень независимо гарантированной безопасности в обычных продуктах ИТ и готовы нести определенные технические затраты для дополнительной безопасности.

Компоненты EAL4 обеспечивает гарантию путем анализа функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и поднабора реализации. Анализ поддержан независимым тестированием функций безопасности, актом испытаний разработчиком "серого ящика", независимым подтверждением выборочных результатов испытания разработчиком, свидетельством поиска разработчиком явных уязвимых мест и независимым поиском явных уязвимых мест. EAL4 также обеспечивает гарантию путем использования средств контроля среды разработки и дополнительных средств управления конфигурацией ОО, включая средства автоматизации этого процесса.

EAL 5 - полуформально разработанный и проверенный проект.

EAL5 позволяет разработчику получить максимальную гарантию безопасности при проектировании, основанном на строгих коммерческих методах разработки, поддержанных умеренным использованием специальных технических методов обеспечения безопасности. Поэтому EAL5 применим, когда разработчики или пользователи требуют высокого уровня независимо гарантированной безопасности и строгого подхода к

разработке без существенных дополнительных затрат, относящихся к специалистам по техническим методам обеспечения безопасности. Компоненты EAL5 обеспечивают гарантию путем анализа функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и всей реализации. Дополнительная гарантия получена за счет формальной модели и полуформального представления функциональной спецификации и проекта высокого уровня и полуформальной демонстрации соответствия между ними. Анализ поддержан независимым тестированием функций безопасности, актом испытаний разработчиком "серого ящика", независимым подтверждением выборочных результатов испытания разработчиком, свидетельством поиска разработчиком явных уязвимых мест и независимым поиском уязвимых мест, гарантирующим относительное сопротивление нападению проникновения. Анализ также включает поиск тайных каналов и поддержан требованием модульной структуры проекта ОО. EAL5 также обеспечивает гарантию с помощью средств контроля среды разработки и всестороннего управления конфигурацией ОО, включая автоматизацию.

EAL 6 - полуформально верифицированный и проверенный проект. EAL6 позволяет разработчикам получать высокую гарантию за счет применения технических методов обеспечения безопасности в условиях сложного окружения. Поэтому EAL6 применим при разработке специальных изделий для использования в ситуациях высокого риска, где ценность защищаемых активов оправдывает дополнительные затраты. Компоненты EAL6 обеспечивают гарантию путем анализа функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и структурированного представления реализации. Дополнительная гарантия получается за счет формальной модели, полуформального представления функциональной спецификации, проекта высокого уровня и проекта низкого уровня, а также полуформальной демонстрации соответствия между ними. Анализ поддержан независимым тестированием функций безопасности, актом испытаний разработчиком "серого ящика", независимым подтверждением выборочных результатов испытания разработчиком, свидетельством поиска разработчиком явных уязвимых мест и независимым поиском уязвимых мест, гарантирующим высокое сопротивление нападению проникновения. Анализ также включает систематический поиск тайных каналов и поддержан требованием модульной и иерархической структуры проекта ОО. EAL6 также обеспечивает гарантию за счет структурированного процесса разработки, средств контроля среды разработки и всестороннего управления конфигурацией ОО, включая полную автоматизацию.

EAL 7 - формально верифицированный и проверенный проект. EAL7 представляет верхний достижимый предел гарантии оценки для фактически полезных продуктов и рассматривается только для экспериментального применения ко всем продуктам, кроме концептуально простых. Поэтому

EAL7 применим при разработке специальных продуктов для применения в ситуациях чрезвычайно высокого риска и/или где высокая ценность активов оправдывает более высокие затраты. Практическое применение EAL7 в настоящее время ограничено продуктами с сосредоточенными функциональными возможностями обеспечения безопасности, поддающимися формальному анализу. Компоненты EAL7 обеспечивают гарантию путем анализа функций безопасности, проекта высокого уровня подсистем, проекта низкого уровня модулей ОО и структурированного представления выполнения. Дополнительная гарантия обеспечивается за счет формальной модели, формального представления функциональной спецификации и проекта высокого уровня, полуформального представления проекта низкого уровня, формальной и полуформальной демонстрации соответствия между ними. Анализ поддержан независимым тестированием функций безопасности, актом испытаний разработчиком "белого ящика", независимым подтверждением всех результатов испытаний разработчиком, свидетельством поиска разработчиком явных уязвимостей и независимым поиском уязвимых мест, гарантирующим высокое сопротивление нападению проникновения. Анализ также включает систематический поиск тайных каналов и поддержан требованием модульной, иерархической и простой структуры проекта ОО. EAL7 также обеспечивает гарантию за счет структурированного процесса разработки, средств контроля среды разработки и всестороннего управления конфигурацией ОО, включая полную автоматизацию.

Класс доверия	**Семейство доверия**	**Краткое имя**
ACM – Управление конфигурацией	Автоматизация УК	ACM_AUT
	Возможности УК	ACM_CAP
	Область УК	ACM_SCP
ADO – Поставка и эксплуатация	Поставка	ADO_DEL
	Установка, генерация и запуск	ADO_IGS
ADV – Разработка	Функциональная спецификация	ADV_FSP
	Проект верхнего уровня	ADV_HLD
	Представление реализации	ADV_IMP
	Внутренняя структура ФБО	ADV_INT
	Проект нижнего уровня	ADV_LLD
	Соответствие представлений	ADV_RCR
	Моделирование политики безопасности	ADV_SPM
AGD – Руководства	Руководство администратора	AGD_ADM
	Руководство пользователя	AGD_USR
ALC – Поддержка жизненного цикла	Безопасность разработки	ALC_DVS
	Устранение недостатков	ALC_FLR
	Определение жизненного цикла	ALC_LCD
	Инструментальные средства и методы	ALC_TAT
ATE –Тестирование	Покрытие	ATE_COV
	Глубина	ATE_DPT
	Функциональное тестирование	ATE_FUN
	Независимое тестирование	ATE_IND
AVA – Оценка уязвимостей	Анализ скрытых каналов	AVA_CCA

	Неправильное применение	AVA_MSU
	Стойкость функций безопасности ОО	AVA_SOF
	Анализ уязвимостей	AVA_VLA

Профиль защиты представляет собой аналогию с классом безопасности в Оранжевой книге. Например, Labeled Security Protection Profile (LSPP) аналогичен классу B1.

Вывод

Для реализации защитных функций в ОС используются различные механизмы безопасности, такие как управление доступом, регистрация и учет, криптография, обеспечение целостности, экранирование, обеспечение отказоустойчивости и восстановления, безопасное управление и другие.

Все они будут подробно изучаться в рамках нашей дисциплины.