Содержание:

Введение

Информационная безопасность – сравнительно молодая, быстро развивающаяся область информационных технологий. Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

С методологической точки зрения правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Информационная безопасность – многогранная область деятельности, в которой успех может принести только систематический, комплексный подход. Для решения данной проблемы рассматриваются меры законодательного, административного, процедурного и программно-технического уровня.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация. В законе РФ "Об информации, информатизации и защите информации" определено:

- "информационные ресурсы являются объектами собственности граждан, организаций, общественных объединений, государства";
- "информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений".

Информация имеет ряд особенностей:

- не материальна;
- хранится и передается с помощью материальных носителей;
- любой материальный объект содержит информацию о самом себе либо о другом объекте. Информации присущи следующие свойства:

Ценность информации определяется степенью ее полезности для владельца. Законом РФ "Об информации, информатизации и защите информации" гарантируется право собственника информации на ее использование и защиту от доступа к ней других лиц (организаций). Если доступ к информации ограничен, то такая информация называется конфиденциальной. Конфиденциальная информация может содержать государственную или коммерческую тайну.

Достоверность информации определяется достаточной для владельца точностью отражать объекты и процессы окружающего мира в определенных временных и пространственных рамках. Информация, искаженно представляющая действительность, может нанести владельцу значительный материальный и моральный ущерб. Если информация искажена умышленно, то ее называют дезинформацией.

Своевременность информации, т.е. соответствие ценности и достоверности определенному временному периоду, может быть выражена формулой

$$C(t) = C_0 e^{-2,3t/\tau},$$

где C_0 – ценность информации в момент ее возникновения; t – время от момента возникновения информации до момента определения ее стоимости; τ – время от момента возникновения информации до момента ее устаревания.

Предметом защиты является информация, хранящаяся, обрабатываемая и передаваемая в компьютерных (информационных) системах. Особенностями данного вида информации являются:

- двоичное представление информации внутри системы, независимо от физической сущности носителей исходной информации;
- высокая степень автоматизации обработки и передачи информации;
- концентрация большого количества информации в КС.

1. Объект защиты информации

Объектом защиты информации является компьютерная (информационная) система или автоматизированная система обработки информации (АСОИ).

Информационная система – это организационно-упорядоченная совокупность информационных ресурсов, технических средств, технологий и персонала, реализующих информационные процессы в традиционном или автоматизированном режиме для удовлетворения информационных потребностей пользователей.

Информационная безопасность АСОИ – состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Информационная безопасность достигается проведением соответствующего уровня политики информационной безопасности.

Под политикой информационной безопасности понимают совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.

Система защиты информации – совокупность правовых норм, организационных мер и мероприятий, технических, программных и криптографических средств и методов, обеспечивающих защищенность информации в системе в соответствии с принятой политикой безопасности.

Что касается подходов к реализации защитных мероприятий по обеспечению безопасности информационных систем, то сложилась трехэтапная (трехстадийная) разработка таких мер. Первая стадия – выработка требований – включает:

- определение состава средств информационной системы;

- анализ уязвимых элементов ИС;
- оценка угроз (выявление проблем, возникающих при наличия уязвимых мест);
- анализ риска (прогноз возможных последствий, вызывающих эти проблемы).

Вторая стадия – определение способов защиты – включает ответы на следующие вопросы: Какие угрозы должны быть устранены и в какой мере? Какие ресурсы системы должны быть защищаемы и в какой степени? С помощью каких средств должна быть реализована защита?

Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз? Третья стадия – определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты.

Для защиты АС на основании руководящих документов Гостехкомиссии могут быть сформулированы следующие положения.

1. Информационная безопасность АС основывается на положениях требованиях существующих законов, стандартов и нормативно-методических документов.
2. Информационная безопасность АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
3. Информационная безопасность АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
4. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).
5. Неотъемлемой частью работ по ИБ является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.
6. Защита АС должна предусматривать контроль эффективности средств защиты. Этот контроль может быть периодическим либо инициироваться по мере необходимости пользователем АС или контролирующим органом.

Рассмотренные подходы могут быть реализованы при обеспечении следующих основных принципов: Принцип системности. Системный подход к защите информационных систем предполагает необходимость учета всех

взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- при всех видах информационного проявления и деятельности;
- во всех структурных элементах;
- при всех режимах функционирования;
- на всех этапах жизненного цикла;
- с учетом взаимодействия объекта защиты с внешней средой.

Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности. В распоряжении специалистов по компьютерной безопасности имеется широкий спектр мер, методов и средств защиты компьютерных систем (современные СВТ, ОС, инструментальные и прикладные программные средства, обладающие теми или иными встроенными элементами защиты). Комплексное их использование предполагает

согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Принцип непрерывности защиты. Защита информации – это не разовое мероприятие и даже не конкретная совокупность уже проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, позволит создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты мо-гут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

Разумная достаточность. Создать абсолютно непреодолимую систему защиты принципиально невозможно, при достаточных времени и средствах можно преодолеть любую защиту. Поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов ИС и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

Гибкость системы защиты. Часто приходится создавать систему защиты в условиях большой неопределенности. По-этому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда средства защиты необходимо устанавливать на работающую систему, нарушая процесс ее нормального функционирования.

Открытость алгоритмов и механизмов защиты. Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления. Но это вовсе не означает, что информация конкретной системы защиты должна быть общедоступна – необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

Принцип простоты применения средств защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании, применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных непонятных ему операций (ввод нескольких паролей и имен и т.д.).

В настоящее время выделяют 4 этапа развития концепций обеспечения безопасности данных.

1 этап 1960 – 1970 гг.

Попытки обеспечить безопасность данных чисто формальными механизмами, содержащими, главным образом, технические и программные средства. Сосредоточение программных средств в рамках операционных систем и систем управления базами данных.

2 этап 1970 – 1976 гг. Развитие формальных механизмов защиты данных. Выделение управляющего компонента защиты данных – ядра безопасности. Развитие неформальных средств защиты. Формирование основ системного подхода к обеспечению безопасности данных.

3 этап 1976 – 1990 гг.

Дальнейшее развитие механизмов второго этапа. Формирование взгляда на обеспечение безопасности данных как на непрерывный процесс. Развитие стандартов на средства защиты данных. Усиление тенденции аппаратной реализации средств защиты данных. Формирование вывода о взаимосвязи обеспечения безопасности данных, архитектуры ИВС и технологии ее функционирования. Формирование системного подхода к проблеме обеспечения безопасности данных.

4 этап 1990 г. – по настоящее

Время дальнейшее развитие механизмов третьего этапа. Формирование основ теории обеспечения безопасности данных в ИВС. Разработка моделей, методов и алгоритмов управления защитой данных в ИВС.

2. МЕХАНИЗМЫ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ

Операционная система есть специально организованная совокупность программ, которая управляет ресурсами системы (ЭВМ, вычислительной системы, других компонентов ИВС) с целью наиболее эффективного их использования и обеспечивает интерфейс пользователя с ресурсами.

Операционные системы, подобно аппаратуре ЭВМ, на пути своего развития прошли несколько поколений.

ОС первого поколения были направлены на ускорение и упрощение перехода с одной задачи пользователя на другую задачу (другого пользователя), что поставило проблему обеспечения безопасности данных, принадлежащих разным

задачам.

Второе поколение ОС характеризовалось наращиванием программных средств обеспечения операций ввода-вывода и стандартизацией обработки прерываний. Надежное обеспечение безопасности данных в целом осталось нерешенной проблемой.

К концу 60-х гг. XX в. начал осуществляться переход к мультипроцессорной организации средств ВТ, поэтому проблемы распределения ресурсов и их защиты стали более острыми и трудноразрешимыми. Решение этих проблем привело к соответствующей организации ОС и широкому применению аппаратных средств защиты (защита памяти, аппаратный контроль, диагностика и т.п.).

Основной тенденцией развития вычислительной техники была и остается идея максимальной доступности ее для пользователей, что входит в противоречие с требованием обеспечения безопасности данных.

Под механизмами защиты ОС будем понимать все средства и механизмы защиты данных, функционирующие в составе ОС. Операционные системы, в составе которых функционируют средства и механизмы защиты данных, часто называют защищенными системами.

Под безопасностью ОС будем понимать такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы. Укажем следующие особенности ОС, которые позволяют выделить вопросы обеспечения безопасности ОС в особую категорию:

- управление всеми ресурсами системы;
- наличие встроенных механизмов, которые прямо или косвенно влияют на безопасность программ и данных, работающих в среде ОС;
- обеспечение интерфейса пользователя с ресурсами системы;
- размеры и сложность ОС.

Большинство ОС обладают дефектами с точки зрения обеспечения безопасности данных в системе, что обусловлено выполнением задачи обеспечения максимальной доступности системы для пользователя.

Рассмотрим типовые функциональные дефекты ОС, которые могут привести к созданию каналов утечки данных.

1. Идентификация. Каждому ресурсу в системе должно быть присвоено уникальное имя – идентификатор. Во многих системах пользователи не имеют возможности удостовериться в том, что используемые ими ресурсы действительно принадлежат системе.
2. Пароли. Большинство пользователей выбирают простейшие пароли, которые легко подобрать или угадать.
3. Список паролей. Хранение списка паролей в незашифрованном виде дает возможность его компрометации с после-дующим НСД к данным.
4. Пороговые значения. Для предотвращения попыток несанкционированного входа в систему с помощью подбора па-роля необходимо ограничить число таких попыток, что в некоторых ОС не предусмотрено.
5. Подразумеваемое доверие. Во многих случаях программы ОС считают, что другие программы работают правильно.
6. Общая память. При использовании общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП).
7. Разрыв связи. В случае разрыва связи ОС должна немедленно закончить сеанс работы с пользователем или повторно установить подлинность субъекта.
8. Передача параметров по ссылке, а не по значению (при передаче параметров по ссылке возможно сохранение параметров в ОП после проверки их корректности, нарушитель может изменить эти данные до их использования).
9. Система может содержать много элементов (например, программ), имеющих различные привилегии.

Основной проблемой обеспечения безопасности ОС является проблема создания механизмов контроля доступа к ресурсам системы. Процедура контроля доступа заключается в проверке соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Кроме того, ОС содержит вспомогательные средства защиты, такие как средства мониторинга, профилактического контроля и аудита. В совокупности механизмы контроля доступа и вспомогательные средства защиты образуют механизмы управления доступом.

Средства профилактического контроля необходимы для отстранения пользователя от непосредственного выполнения критичных с точки зрения безопасности данных операций и передачи этих операций под контроль ОС. Для обеспечения безопасности данных работа с ресурсами системы осуществляется с помощью специальных программ ОС, доступ к которым ограничен.

Средства мониторинга осуществляют постоянное ведение регистрационного журнала, в который заносятся записи о всех событиях в системе. В ОС могут

использоваться средства сигнализации о НСД, которые используются при обнаружении нарушения безопасности данных или попыток нарушения.

Контроль доступа к данным. При создании механизмов контроля доступа необходимо, прежде всего, определить множества субъектов и объектов доступа. Субъектами могут быть, например, пользователи, задания, процессы и процедуры. Объектами – файлы, программы, семафоры, директории, терминалы, каналы связи, устройства, блоки ОП и т.д. Субъекты могут одновременно рассматриваться и как объекты, поэтому у субъекта могут быть права на доступ к другому субъекту. В конкретном процессе в данный момент времени субъекты являются активными элементами, а объекты – пассивными.

Для осуществления доступа к объекту субъект должен обладать соответствующими полномочиями. Полномочие есть некий символ, обладание которым дает субъекту определенные права доступа по отношению к объекту, область защиты определяет права доступа некоторого субъекта ко множеству защищаемых объектов и представляет собой совокупность всех полномочий данного субъекта.

При функционировании системы необходимо иметь возможность создавать новые субъекты и объекты. При создании объекта одновременно создается и полномочие субъектов по использованию этого объекта. Субъект, создавший такое полномочие, может воспользоваться им для осуществления доступа к объекту или же может создать несколько копий полномочия для передачи их другим субъектам.

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь пойдет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций и контролировать выполнение установленного

порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, как показано в табл. 1.

Таблица 1. Фрагмент матрицы доступа

	Файл	Программа	Линия связи	Реляционная таблица
Пользователь 1	o r w с системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2	a			

О б о з н а ч е н и е : "o" – разрешение на передачу прав доступа другим пользователям, "r" – чтение, "w" – запись, "e" – выполнение, "a" – добавление информации.

Тема логического управления доступом – одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект – это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции

поиска, добавления, модификации и удаления данных, у других объектов. В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла).

Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной кон

фигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

Матрицу доступа, ввиду ее разреженности (большинство клеток – пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, т.е. для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администра-тору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа – исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления – гибкость. К сожалению, у "произвольного" под-хода есть ряд недостатков. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи. Следовательно, произвольность управления должна быть дополнена жестким контролем за реализацией избранной политики безопасности.

Второй недостаток, который представляется основным, состоит в том, что права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом. Подобная "разделенность" прав и данных существенно осложняет проведение несколькими системами согласованной политики безопасности и, главное, делает практически невозможным эффективный контроль согласованности.

Возвращаясь к вопросу представления матрицы доступа, укажем, что для этого можно использовать также функциональный способ, когда матрицу не хранят в явном виде, а каждый раз вычисляют содержимое соответствующих клеток. Например, при принудительном управлении доступом применяется сравнение меток безопасности субъекта и объекта.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

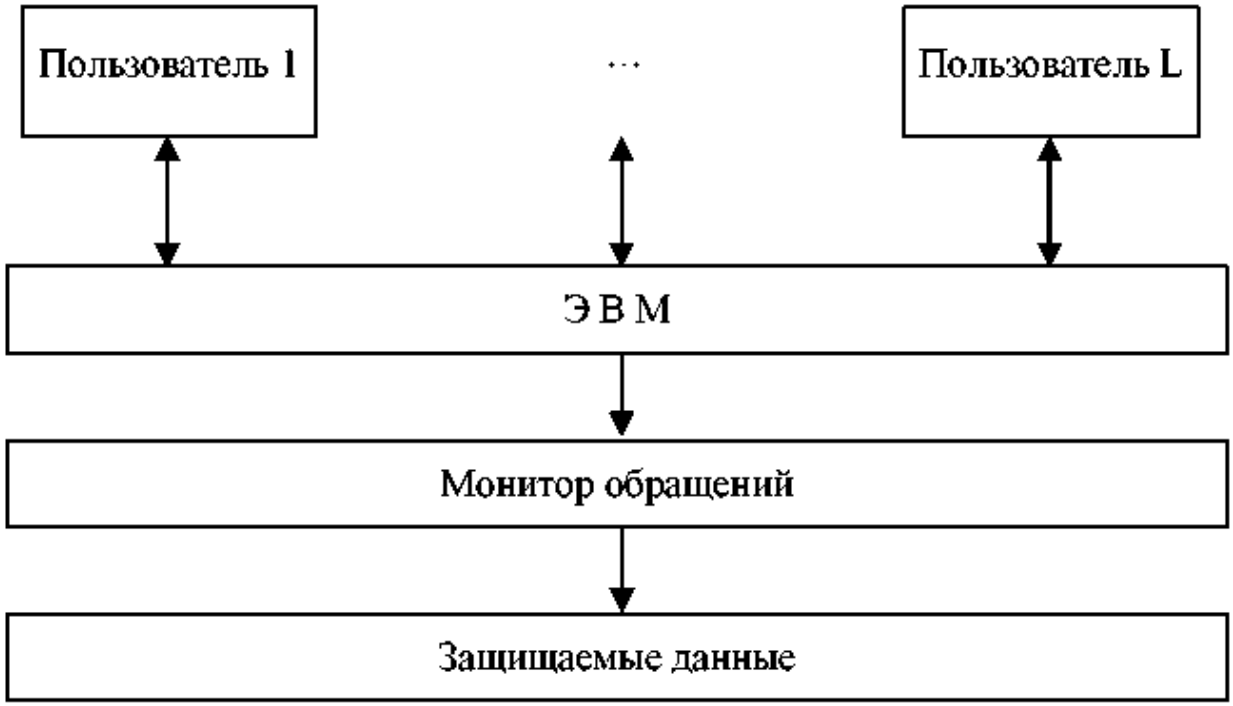

Рисунок 1. Схема модели Харрисона, Руззо и Ульмана

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

1. идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой произвольного (или дискреционного) управления доступом;
2. атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа мандатного управления доступом.

Непосредственное управление правами доступа осуществляется на основе одной из моделей доступа:

- матричной модели доступа (модель Харрисона-Руззо-Ульмана);
- многоуровневой модели доступа (модель Белла-Лападулы).

Разработка и практическая реализация различных защищенных ОС привела Харрисона, Руззо и Ульмана к построению формальной модели защищенных систем. Схема модели Харрисона, Руззо и Ульмана (HRU-модели) приведена на рис. 1.

3. ЗАЩИТА В ОПЕРАЦИОННОЙ СИСТЕМЕ UNIX

Операционная система Unix относится к категории многопользовательских многопрограммных ОС, работающих в режиме разделения времени. Богатые возможности, заложенные в ОС Unix, сделали ее наиболее популярной в мире. ОС Unix поддерживается практически на всех типах ЭВМ.

Организация работ в ОС Unix основана на понятии последовательного процесса как единицы работы, управления и потребления ресурсов. Взаимодействие процессов внутри ядра (процесс вызывает ядро как подпрограмму) происходит по принципу сопрограмм. Последовательность вычислений внутри процесса строго выдерживается: процесс, в частности, не может активизировать ввод-вывод и продолжать вычисление параллельно с ним. В этом случае требуется создать параллельный процесс.

Ядро ОС Unix состоит из двух основных частей: управления процессами и управления устройствами. Управление процессами резервирует ресурсы, определяет последовательность выполнения процессов и принимает запросы на обслуживание. Управление устройствами контролирует передачу данных между

ОП и периферийными устройствами.

В любой момент времени выполняется либо программа пользователя (процесс), либо команда ОС. В каждый момент времени лишь один пользовательский процесс активен, а все остальные приостановлены. Ядро ОС Unix служит для удовлетворения потребностей процессов.

Процесс – это программа на этапе выполнения. В некоторый момент времени программе могут соответствовать один или несколько процессов, или не соответствовать ни одного. Считается, что процесс является объектом, учтенным в специальной таблице ядра системы. Наиболее важная информация о процессе хранится в двух местах: в таблице процессов и в таблице пользователя, называемой также контекстом процесса. Таблица процессов всегда находится в памяти и содержит на каждый процесс по одному элементу, в котором отражается состояние процесса: адрес в памяти или адрес свопинга, размер, идентификаторы процесса и запустившего его пользователя. Таблица пользователя существует для каждого активного процесса и к ней могут непосредственно адресоваться только программы ядра (ядро резервирует по одному контексту на каждый активный процесс). В этой таблице содержится информация, требуемая во время выполнения процесса: идентификационные номера пользователя и группы, предназначенные для определения привилегий доступа к файлам, ссылки на системную таблицу файлов для всех открытых процессом файлов, указатель на индексный дескриптор текущего каталога в таблице индексных дескрипторов и список реакций на различные ситуации. Если процесс приостанавливается, контекст становится недоступным и немодифицируемым.

Каталоги файловой системы ОС Unix "спрятаны" от пользователей и защищены механизмами ОС. Скрытой частью файловой организации в ОС Unix является индексный дескриптор файла, который описывает расположение файла, его длину, метод доступа к файлу, даты, связанные с историей создания файла, идентификатор владельца и т.д.

Работа с таблицами является привилегией ядра, что обеспечивает сохранность и безопасность системы.

При взаимодействии с ОС Unix пользователь может обращаться к большому числу информационных объектов или файлов, объединенных в каталоги. Файловая система ОС Unix имеет иерархическую структуру.

В ОС Unix используется четыре типа файлов: обычные, специальные, каталоги, а в некоторых версиях ОС и FIFO-файлы (First In – First Out). Обычные файлы содержат данные пользователей. Специальные файлы предназначены для организации взаимодействия с устройствами ввода-вывода. Доступ к любому устройству реализуется как обслуживание запроса к специальному (дисковому) файлу. Каталоги используются системой для поддержания файловой структуры. Особенность каталогов состоит в том, что пользователь может читать их содержимое, но выполнять записи в каталоги (изменять структуру каталогов) может только ОС. В ОС Unix, организуются именованные программные каналы, являющиеся соединительным средством между стандартным выводом одной программы и стандартным вводом другой.

Схема типичной файловой системы ОС Unix приведена на рис. 2. Рассмотрим основные механизмы защиты данных, реализованные в ОС Unix.

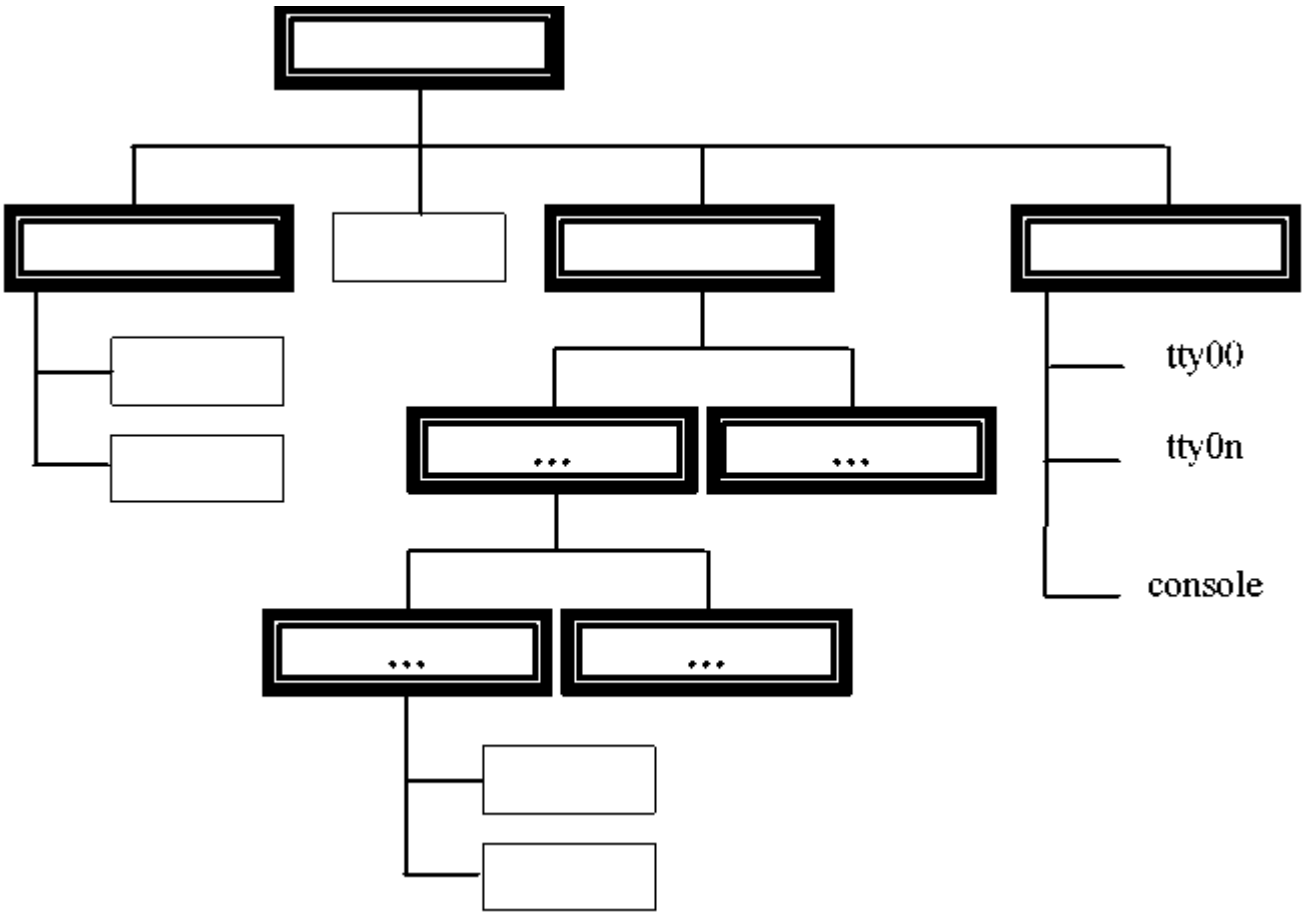

Рисунок 2. Схема файловой системы ОС Unix

Управление доступом к системе. При включении пользователя в число абонентов ему выдается регистрационное имя (идентификатор) для входа в систему и пароль,

который служит для подтверждения идентификатора пользователя. В отдельных версиях ОС Unix, помимо идентификатора и пароля, требуется ввод номера телефона, с которого выполняется подключение к системе. Администратор системы и пользователь могут изменить пароль командой passwd. При вводе этой команды ОС запрашивает ввод текущего пароля, а затем требует ввести новый пароль. Если предложенный пароль не удовлетворяет требования системы, то запрос на ввод пароля может быть повторен. Если предложенный пароль удовлетворителен, ОС просит ввести его снова, чтобы убедиться в корректности ввода пароля.

Пользователи, которым разрешен вход в систему, перечислены в учетном файле пользователей /etc/passwd. Этот текстовый файл содержит следующие данные: имя пользователя, зашифрованный пароль, идентификатор пользователя, идентификатор группы, начальный текущий каталог и имя исполняемого файла, используемого в качестве интерпретатора команд. Пароль шифруется, как правило, с использованием DES-алгоритма.

Управление доступом к данным. Операционная система Unix поддерживает для любого файла комплекс характеристик, определяющих санкционированность доступа, тип файла, его размер и точное местоположение на диске. При каждом обращении к файлу система проверяет право пользоваться им. Операционная система Unix допускает выполнение трех типов операций над файлами: чтение, запись и выполнение. Чтение файла означает, что доступно его содержимое, а запись – что возможны изменения содержимого файла. Выполнение приводит либо к загрузке файла в ОП, либо к выполнению содержащихся в файле команд системного монитора Shell. Разрешение на выполнение каталога означает, что в нем допустим поиск с целью формирования полного имени на пути к файлу. Любой из файлов в ОС Unix имеет определенного владельца и привязан к некоторой группе. Файл наследует их от процесса, создавшего файл. Пользователь и группа, идентификаторы которых связаны с файлом, считаются его владельцами.

Идентификаторы пользователя и группы, связанные с процессом, определяют его права при доступе к файлам. По отношению к конкретному файлу все процессы делятся на три категории:

1. владелец файла (процессы, имевшие идентификатор пользователя, совпадающий с идентификатором владельца файла);
2. члены группы владельца файла (процессы, имеющие идентификатор группы, совпадающий с идентификатором группы, которой принадлежит файл);

3. прочие (процессы, не попавшие в первые две категории).

Владелец файла обладает одними привилегиями на доступ к нему, члены группы, в которую входит файл – другими, все остальные пользователи – третьими. Каждый файл содержит код защиты, который присваивается файлу при его создании. Код защиты располагается в индексном дескрипторе файла и содержит десять символов, причем первый символ определяет тип файла, а последующие девять – право на доступ к нему. Три вида операций (чтение, запись и выполнение) и три категории (уровни привилегий на доступ: владельцев, групп и прочих пользователей) дают в совокупности девять возможных вариантов разрешений или запретов на доступ к файлу. Первые три символа определяют возможности чтения (r), записи (w) и выполнения (e) на уровне владельца, следующие три – на уровне группы, в которую входит владелец, и последние три – на уровне остальных пользователей. Наличие символов r, w и e указывает на соответствующее разрешение.

Если процесс требует доступа к файлу, то сначала определяется категория, в которую по отношению к этому файлу он попадает. Затем из кода защиты выбираются те три символа, которые соответствуют данной категории, и выполняется проверка: разрешен ли процессу требуемый доступ. Если доступ не разрешен, системный вызов, посредством которого процесс сделал запрос на доступ, отвергается ядром ОС.

По соглашению, принятому в ОС Unix, привилегированный пользователь имеет идентификатор, равный нулю. Процесс, с которым связан нулевой идентификатор пользователя, считается привилегированным. Независимо от кода защиты файла привилегированный процесс имеет право доступа к файлу для чтения и записи. Если в коде защиты хотя бы одной категории пользователей (процессов) есть разрешение на выполнение файла, привилегированный процесс тоже имеет право выполнять этот файл.

С помощью специальных команд владелец файла (привилегированный пользователь) может изменять распределение привилегий. Команда Change mode позволяет изменить код защиты, команда Change owner меняет право на владение фай-лом, а команда Change group – принадлежность к той или иной группе. Пользователь может изменять режимы доступа только для файлов, которыми он владеет.

Защита хранимых данных. Для защиты хранимых данных в составе ОС Unix имеется утилита crypt, которая читает данные со стандартного ввода, шифрует их и направляет на стандартный вывод. Шифрование применяется при необходимости предоставления абсолютного права владения файлом.

Восстановление файловой системы. Операционная система Unix поддерживает три основных набора утилит копирования: программы volcopy/labelit, dump/restor и cpio. Программа volcopy целиком переписывает файловую систему, проверяя с помощью программы labelit соответствие меток требуемых томов. Программа dump обеспечивает копирование лишь тех файлов, которые были записаны позднее определенной даты (защита накоплением). Программа restor может анализировать данные, созданные программой dump, и восстанавливать отдельные файлы или всю файловую систему полностью. Программа cpio предназначена для создания одного большого файла, содержащего образ всей файловой системы или какой-либо ее части.

Для восстановления поврежденной, например, в результате сбоев в работе аппаратуры файловой системы используются программы fsck и fsdb.

За сохранность файловой системы, адаптацию программного обеспечения к конкретным условиям эксплуатации, периодическое копирование пользовательских файлов, восстановление потерянных данных и другие операции ответственность возложена на администратора системы.

Усложненное управление доступом. В составе утилит ОС Unix находится утилита cron, которая предоставляет возможность запускать пользовательские программы в определенные моменты (промежутки) времени и, соответственно, ввести временные параметры для ограничения доступа пользователей. Для управления доступом в ОС Unix также применяется разрешение установки идентификатора владельца. Такое раз-решение дает возможность получить привилегии владельца файла на время выполнения соответствующей программы. Владелец файлов может установить режим, в котором другие пользователи имеют возможность назначать собственные идентификаторы режима.

Доступ, основанный на полномочиях, использует соответствие меток. Для этого вводятся метки объектов (файлов) и субъектов (процессов), а также понятия доминанты и равенства меток (для выражения отношения между метками). Создаваемый файл наследует метку от создавшего его процесса. Вводятся соотношения, определяющие права процессов по отношению к файлам. Интерфейс

дискретного доступа существенно детализирует имеющиеся механизмы защиты ОС Unix. Вводимые средства можно разделить на следующие группы:

1. работа со списками доступа при дискретной защите;
2. проверка права доступа;
3. управление доступом на основе полномочий;
4. работа привилегированных пользователей.

В рамках проекта Posix создан интерфейс системного администратора. Указанный интерфейс определяет объекты и множества действий, которые можно выполнить над объектами. В качестве классов субъектов и объектов предложены пользователь, группа пользователей, устройство, файловая система, процесс, очередь, вход в очередь, машина, система, администратор, программное обеспечение и др. Определены атрибуты таких классов, операции над классами и события, которые могут с ними происходить.

Заключение

Стремительное развитие информационных технологий привело к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Однако с развитием информационных технологий возникают и стремительно растут риски, связанные с их использованием, появляются совершенно новые угрозы, с последствиями, от реали-зации которых человечество раньше не сталкивалось.

Одним из главных инструментов для реализации конкретных информационных технологий являются информационные системы, задача обеспечения безопасности которых является приоритетной, так как от сохранения конфиденциальности, целостности и доступности информационных ресурсов зависит результат деятельности информационных систем.

Операционная система является важнейшим программным компонентом любой вычислительной машины, поэтому от уровня реализации политики безопасности в каждой конкретной операционной системе во многом зависит и общая безопасность информационной системы.

В связи с этим знания в области современных методов и средств обеспечения безопасности операционных систем являются необходимым условием для формирования специалиста по информационной безопасности.