**Дата: 09.12.2020**

**Группа: 19ИСиП 1д**

**Наименование дисциплины: Операционные системы и среды.**

**Тема: Управление безопасностью.**

*Безопасность* – одна из наиболее актуальных проблем в области ИТ в настоящее время, ввиду сильной зависимости повседневной деятельности и бизнеса от компьютерных технологий и ввиду резко возрастающего числа *сетевых атак* (*киберпреступности*). Особенно важна *безопасность* для операционных систем и сетей как основных объектов атак.

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями может быть успешно решена только на основе комплексной защиты корпоративных информационных систем. Защищенные операционные системы относятся к базовым средствам многоуровневой комплексной защиты КИС.
Проблемы обеспечения безопасности ОС
Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка операционной системы (ОС). Окружение, и котором функционирует ОС, называется доверенной вычислительной базой (ДВБ). ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: операционную систему, программы, сетевое оборудование, сродства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная операционная система. Без нее доверенная вычислительная база оказывается построенной на песке.
Угрозы безопасности операционной системы
Организация эффективной и падежной защиты операционной системы невозможна без предварительного анализа возможных угроз ее безопасности. Угрозы безопасности операционной системы существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т. д. Например, если операционная система используется для организации электронного документооборота, наиболее опасны угрозы, снизанные с несанкционированным доступом (НСД) к файлам. Если же операционная система используется как платформа провайдера интернет-услуг, очень опасны атаки на сетевое программное обеспечение.
Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации.
**Классификация угроз по цели атаки:**•    несанкционированное чтение информации;
•    несанкционированное изменение информации;
•    несанкционированное уничтожение информации;
•    полное или частичное разрушение операционной системы.
**Классификация угроз по принципу воздействия на операционную систему:**•    использование известных (легальных) каналов получения информации, например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запретен;
•    использование скрытых каналов получения информации, например угроза использования злоумышленником недокументированных возможностей операционной системы;
•    создание новых каналов получения информации с помощью программных закладок.
**Классификация угроз по типу используемой злоумышленником уязвимости защиты:**•    неадекватная политика безопасности, в том числе и ошибки администратора системы;
•    ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе и так называемые люки - случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
•    ранее внедренная программная закладка
**Классификация угроз по характеру воздействия на операционную систему:**•    активное воздействие - несанкционированные действия злоумышленника в системе;
•    пассивное воздействие - несанкционированное наблюдение злоумыш-ленника за процессами, происходящими в системе.
 Понятие защищенной операционной системы
Операционную систему называют защищенной, если она предусматривает средства защиты от основных классов угроз. Защищенная операционная система обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с операционной системой. Кроме того, защищенная операционная система должна содержать средства противодействия случайному или преднамеренному выводу операционной системы из строя.
Если операционная система предусматривает .защиту не от всех основных классов угроз, а только от некоторых, такую ОС называют частично защищенной.
Подходы к построению защищенных операционных систем
Существует дна основных подхода к созданию защищенных операционных систем - фрагментарный и комплексный.
При фрагментарном подходе вначале организуется защита от одной угрозы, затем от другой п т. д. Примером фрагментарного подхода может служить ситуация, когда за основу берется незащищенная операционная система (например, Windows 98), на нее устанавливают антивирусный пакет, систему шифрования, систему регистрации действий пользователей п т. д.
При комплексном подходе защитные функции вносятся в операционную систему на этапе проектирования архитектуры операционной системы и являются ес неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при реше-нии различных задач, связанных с организацией защиты информации, поэтому конфликты между ее отдельными компонентами практически невозможны. Подсистема защиты, созданная на основе комплексного подхода, может быть устроена так, что при фатальных сбоях в функционировании ее ключевых элементов она вызывает крах операционной системы, что не позволяет злоумышленнику отключать защитные функции системы. При фрагментарном подходе такая организация подсистемы защиты невозможна.
Как правило, подсистему защиты операционной системы, созданную на основе комплексного подхода, проектируют так, чтобы отдельные ее элементы были заменяемы. Соответствующие программные модули могут быть заменены другими модулями.

**Архитектура подсистемы защиты операционной системы**Основные функции подсистемы защиты операционной системы
**Подсистема защиты ОС выполняет следующие основные функции**:
1.    Идентификация и аутентификация. Ни один пользователь не может на-чать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.
2.    Разграничение доступа. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.
3.    Аудит. Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.
4.    Управление политикой безопасности. Политика безопасности должна по-стоянно поддерживаться в адекватном состоянии, то есть должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в операционную систему.
5.    Криптографические функции. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по  каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.
6.    Сетевые функции. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе имеющих прямое отношение к защите информации.
Подсистема танины обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функции подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями подсистемы защиты должен существовать четко определенный интерфейс, используе-мый при взаимодействии модулей для решения общих задач.
В таких операционных системах, как Windows ХР, подсистема защиты четко выделяется в общей архитектуре ОС; в других, например UNIX, защитные функции распределены практически по всем элементам операционной системы. Однако любая ОС. удовлетворяющая стандарту защищенности, должна содержать подсистему защиты, выполняющую все вышеперечисленные функции. Обычно подсистема защиты ОС допускает расширение дополнительными программными модулями.

Способы идентификации пользователя

Прежде чем получить доступ к ВС, пользователь должен идентифицировать себя, а механизмы защиты сети затем подтверждают подлинность пользователя, т. е. проверяют, является ли пользователь действительно тем, за кого он себя выдает. В соответствии с логической моделью механизма защиты ВС размещены на рабочей ЭВМ, к которой подключен пользователь через свой терминал или каким-либо иным способом. Поэтому процедуры идентификации, подтверждения подлинности и наделения полномочиями выполняются в начале сеанса на местной рабочей ЭВМ.

В дальнейшем, когда устанавливаются различные сетевые протоколы и до получения доступа к сетевым ресурсам, процедуры идентификации, подтверждения подлинности и наделения полномочиями могут быть активизированы вновь на некоторых удаленных рабочих ЭВМ с целью размещения требуемых ресурсов или сетевых услуг.

Когда пользователь начинает работу в вычислительной системе, используя терминал, система запрашивает его имя и идентификационный номер. В соответствии с ответами пользователя вычислительная система производит его идентификацию. В сети более естественно для объектов, устанавливающих взаимную связь, идентифицировать друг друга.

Пароли - это лишь один из способов подтверждения подлинности. Существуют другие способы:

1. Предопределенная информация, находящаяся в распоряжении пользователя: пароль, личный идентификационный номер, соглашение об использовании специальных закодированных фраз.

2. Элементы аппаратного обеспечения, находящиеся в распоряжении пользователя: ключи, магнитные карточки, микросхемы и т.п..

3. Характерные личные особенности пользователя: отпечатки пальцев, рисунок сетчатки глаза, размеры фигуры, тембр голоса и другие более сложные медицинские и биохимические свойства.

4. Характерные приемы и черты поведения пользователя в режиме реального времени: особенности динамики, стиль работы на клавиатуре, скорость чтения, умение использовать манипуляторы и т.д.

5. Привычки: использование специфических компьютерных заготовок.

6. Навыки и знания пользователя, обусловленные образованием, культурой, обучением, предысторией, воспитанием, привычками и т.п.

Если кто-то желает войти в вычислительную систему через терминал или выполнить пакетное задание, вычислительная система должна установить подлинность пользователя. Сам пользователь, как правило, не проверяет подлинность вычислительной системы. Если процедура установления подлинности является односторонней, такую процедуру называют процедурой одностороннего подтверждения подлинности объекта

**Специализированные программные средства защиты информации**

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых следует отметить следующие две системы, позволяющие ограничить информационные потоки.

Firewalls - брандмауэры (дословно firewall -- огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

Proxy-servers (proxy - доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью -- попросту отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе. Очевидно также, что этот метод не дает достаточной защиты против атак на более высоких уровнях - например, на уровне приложения (вирусы, код Java и JavaScript).

Рассмотрим подробнее работу брандмауэра. Это метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами. Брандмауэр является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра). Брандмауэр конфигурируется в соответствии с принятой в организации политикой контроля доступа к внутренней сети. Все входящие и исходящие пакеты должны проходить через брандмауэр, который пропускает только авторизованные пакеты.

Брандмауэр с фильрацией пакетов [packet-filtering firewall] - является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отбраковывать определенные виды входящих и исходящих пакетов. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP- заголовках пакетов (адреса отправителя и получателя, их номера портов и др.).

Брандмауэр экспертного уровня [stateful inspecthion firewall] - проверяет содержимое принимаемых пакетов на трех уровнях модели OSI - сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Создание брандмауера относится к решению задачи экранирования. Формальная постановка задачи экранирования состоит в следующем. Пусть имеется два множества информационных систем. Экран - это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рис. 6). Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рис. 7).

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (МЭ) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet.

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Экранирование может быть частичным, защищающим определенные информационные сервисы (например, экранирование электронной почты).

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Контрольные вопросы:

1. Почему в настоящее время безопасность актуальная проблема в области ИТ.
2. Каким образом можно решить проблему защиты от несанкционированного доступа.
3. Перечислите мне классификации угроз по цели атаки
4. Перечислите мне классификацию угроз по характеру воздействия на операционную систему
5. Какие функции выполняет подсистема защиты ОС

 Преподаватель\_\_\_\_\_\_\_\_\_А.К.Хунарикова