Авторы:

Танаев Иван Владимирович

студент

Швейкин Владислав Витальевич

студент

Завгородний Станислав Дмитриевич

студент

Дмитриев Егор Андреевич

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

ФУНКЦИИ ПОДСИСТЕМЫ ЗАЩИТЫ ОС

Аннотация: *в данной статье авторами рассматриваются основные методы защиты операционной системы и механизмы обеспечения информационной безопасности.*

Ключевые слова: *операционная система, информационная безопасность, идентификация, аутентификация, аудит, политика безопасности.*

Введение

В современном мире вопросу обеспечения информационной безопасности уделяют всё больше внимания. Это обусловлено тем, что информационная среда последовательно поглощает различные сферы жизни общества. Уязвимости или недостаточная защищенность данных, собственниками которых могут являться частные, юридические лица или даже целые государства – это следствие плохо организованной политики безопасности, а также утратившие актуальность аппаратные или программные средства защиты. В настоящей статье рассматриваются механизмы и функции подсистемы защиты операционных систем – одного из важнейших этапов организации защиты информации с помощью программных средств обеспечения безопасности.

Функции подсистемы защиты информации

Подсистема защиты далеко не всегда представляет собой единый программный модуль. Зачастую она может состоять из нескольких модулей, а некоторые её функции встраиваются непосредственно в ядро операционной системы. Организация подсистемы защиты в различных операционных системах осуществляется по-разному, однако каждая из этих систем обязана удовлетворять потребности собственника данных в защите его информационных ресурсов, а значит она должна выполнять следующие функции: разграничение доступа, идентификация и аутентификация пользователей, аудит, управление политикой безопасности, криптографические функции, сетевые функции.

Механизмы разграничения доступа

Существует два системообразующих подхода к управлению доступом – дискреционный и мандатный.

Суть дискреционного разграничения доступа характеризуется связью субъекта (который способен выполнять какие-либо операции над объектами) и объекта (любого элемента операционной системы, доступ к которому для ряда субъектов потенциально может быть ограничен). Отметим, что взаимодействие субъекта и объекта осуществляется посредством метода доступа – некоторой операции, которая определена для объекта. К каждому объекту системы привязан владелец, способный устанавливать права доступа к объекту. Система также имеет суперпользователя, который выставляет права владения для всех остальных субъектов.

Мандатный подход заключается в присвоении субъекту или объекту классификационного ярлыка, с помощью которого можно определить иерархический уровень субъекта, категорию защищенности объекта и т. д. Поэтому пользователь может производить какие-либо действия (чтение, изменение и др.) с субъектом только в том случае, если его иерархический статус соответствует классификации субъекта или превосходит её. На рисунке 1 представлена иерархическая классификация объектов и субъектов.

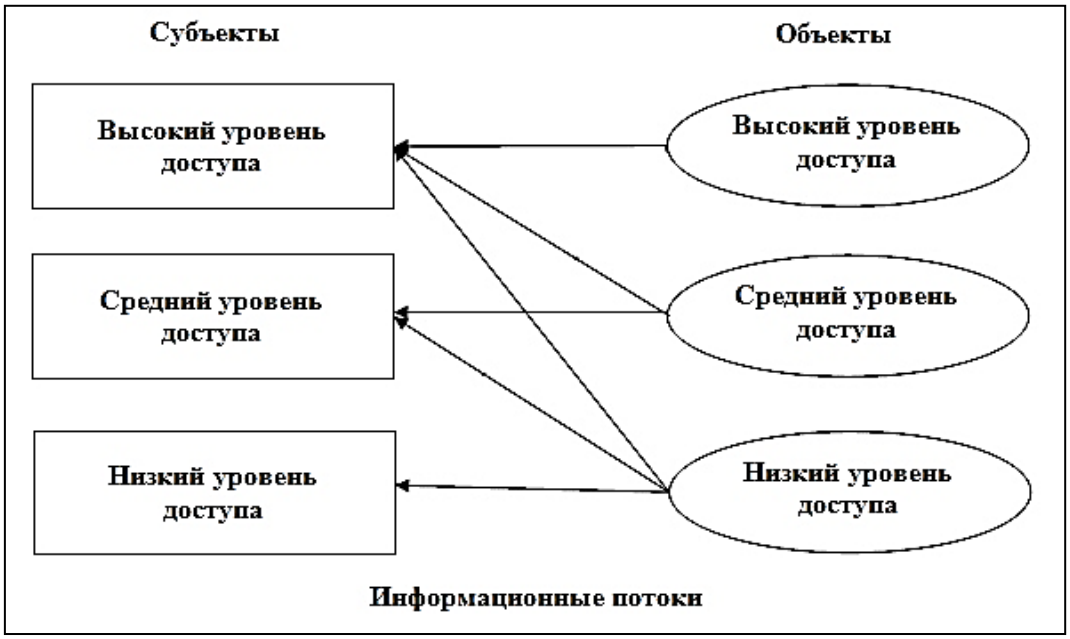

Рис. 1. Разграничение доступа

Идентификация, аутентификация и авторизация

Процедуры идентификации и аутентификации являются не менее важными аспектами в организации качественной защиты информации.

В процессе идентификации субъект сообщает системе данные о себе (имя, логин, учетный номер). Но, для того, чтобы установить что пользователь, прошедший идентификацию, является именно тем, за кого себя выдает, ему следует пройти процедуру аутентификации, которая заключается в сообщении системе уникальной информации, например, пароля. После успешного осуществления вышеперечисленных действий начинается авторизация – предоставление субъекту доступа возможности начать работу в системе.

Аудит

Вследствие того, что операционная система не может отличить случайные ошибки пользователей от действий злоумышленников, способных нанести исключительный вред системе, существует необходимость в регистрации подозрительной активности (событий, угрожающих безопасности данных). Данная информация записывается в журнал безопасности. Пользователи, которые наделены привилегией читать журнал аудита называются аудиторами или, другими

словами, администраторами. Для них крайне важно проводить мониторинг и выявлять потенциальные угрозы. В случае проведения успешной атаки на систему, используя журнал безопасности, аудиторы выясняют параметры, характеризующие данную атаку – время и способ её проведения. Совокупность правил, определяющих, какие события должны регистрироваться в журнале аудита называется политикой аудита. В журнале безопасности обязательно должны быть зарегистрированы попытки входа или выхода пользователей в систему (из системы), попытки изменения списка пользователей, попытки изменения политики аудита и, как следствие, политики безопасности.

Политика безопасности

Данное словосочетание используется для описания пошагового подхода к обеспечению информационной безопасности системы, организации или государства. Это достаточно обширное понятие, которое включает в себя правила, директивы и практические навыки, определяющие то, каким образом информационные ценности обрабатываются и защищаются. В нашем случае политика безопасности должна реагировать на изменения внутри операционных систем. При этом необходимо оценивать потенциальные угрозы безопасности и дополнять программные средства защиты информации административными, т.е. при помощи администратора. В его задачи входит осведомление абонентов операционных систем о правилах безопасности при работе с ОС, контроль за изменениями в параметрах системы (в том числе с помощью аудита). Оптимальная и адекватная политика безопасности препятствует реализации несанкционированных действий злоумышленниками.

Криптографические функции подсистемы защиты ОС

Криптографические средства защиты фигурируют повсеместно в вопросе обеспечения безопасности информационных систем. Например, в операционных системах шифрование задействовано при хранении и передаче по каналам связи данных о пользователях и некоторых других информационных ресурсов, особо важных в контексте безопасности системы. Для шифрования паролей в системах семейства Unix используется известный алгоритм DES, а, например, в Windows

NT помимо DES задействован также MD4. Отметим, что безопаснее хранить только закодированные пароли, а чтобы осуществлять передачу пароля необходимо использовать специальные криптографические протоколы.

Сетевые функции подсистемы защиты ОС

Как правило, многие операционные системы работают не изолированно, а в составе локальных и глобальных компьютерных сетей. Таким образом отдельные ОС в составе единой сети взаимодействуют между собой для решения комплекса поставленных задач, которые также включают в себя защиту информации.

Заключение

В заключение следует отметить, что невозможно выстроить лишенную недостатков систему обеспечения информационной безопасности. Какими бы совершенными ни были аппаратные, программные средства защиты или технические решения, всегда остаются уязвимости, которыми может воспользоваться потенциальный злоумышленник. Однако, чтобы уменьшить вероятность компрометации личных данных, собственник информационных ресурсов обязан планомерно создавать систему безопасности, используя как можно больше известных на сегодняшний день надежных механизмов защиты. Одним из главных помощников в этом является подсистема защиты операционных систем.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных [Текст]: Учебное пособие для вузов / С.Н. Смирнов – М.: Гелиос АРВ, 2007. – 352 с.

2. Сайт Your Private Network Архитектура подсистемы защиты ОС [Электронный ресурс]. – Режим доступа: http://ypn.ru/309/os-security-subsystem-architecture/