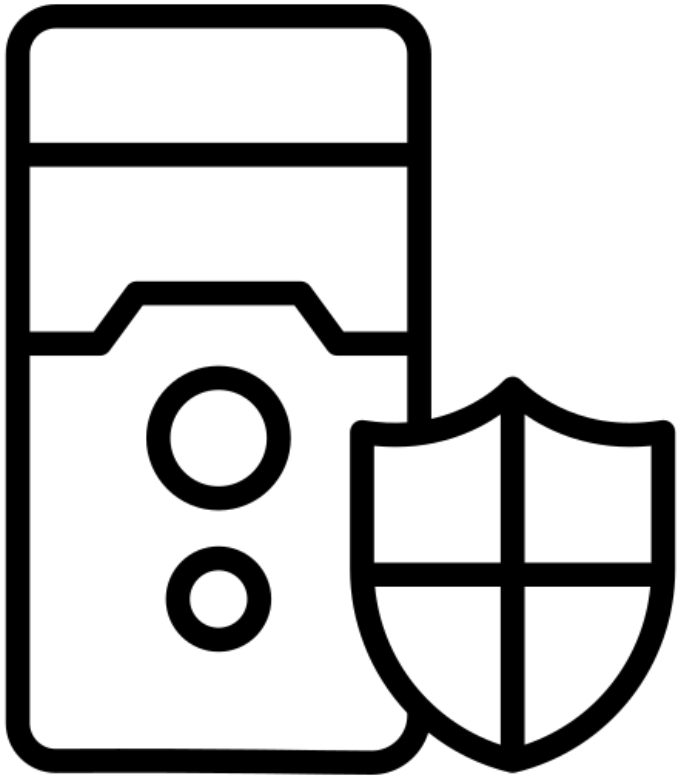
Белорусско-Российский университет
Кафедра «Программное обеспечение информационных технологий»

Защита информации

Защита информации в операционных системах

КУТУЗОВ Виктор Владимирович

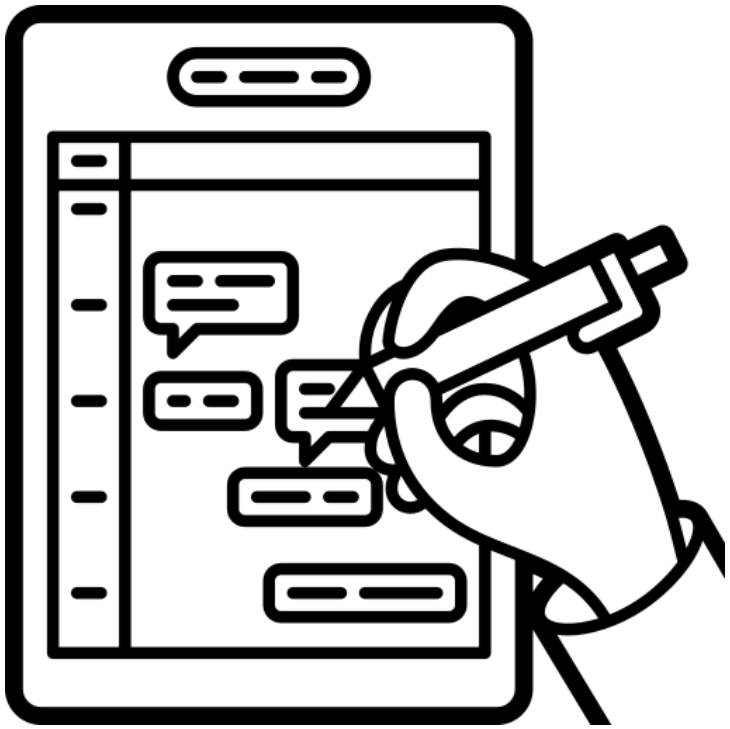
Республика Беларусь, Могилев, 2024



1. Проблемы обеспечения безопасности операционных систем

Проблемы обеспечения безопасности ОС

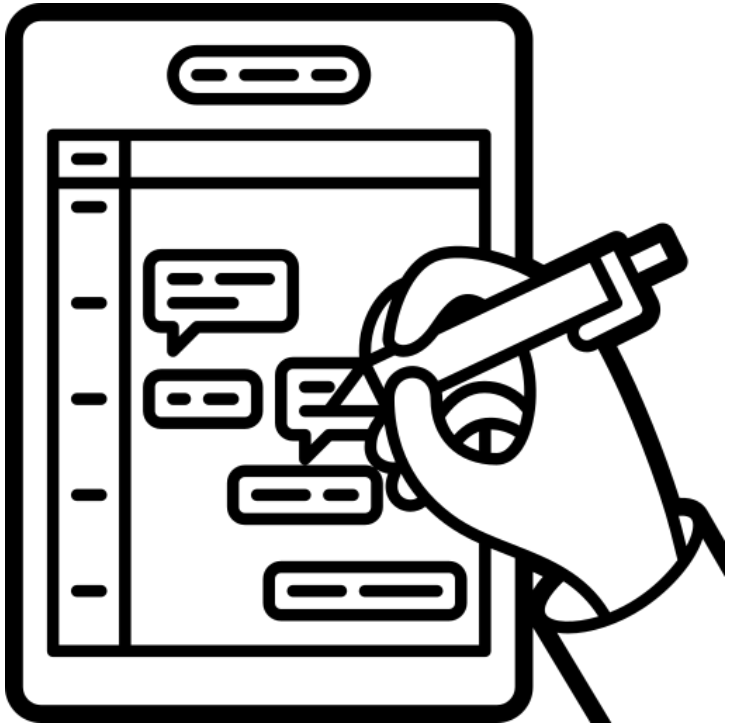
- Большинство программных средств защиты информации являются прикладными программами. Для их выполнения требуется поддержка операционной системы (ОС). Окружение, в котором функционирует ОС, называется доверенной вычислительной базой (ДВБ).
- ДВБ включает в себя полный набор элементов, обеспечивающих информационную безопасность: операционную систему, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры. Краеугольным камнем этой пирамиды является защищенная операционная система. Без нее доверенная вычислительная база оказывается построенной на песке.



1.1 Угрозы безопасности операционной системы

Угрозы безопасности ОС

- Организация эффективной и надежной 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. Например, если операционная система используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же операционная система используется как платформа провайдера интернет-услуг, очень опасны атаки на сетевое программное обеспечение операционной системы.



1.2 Классификация угроз на ОС

Классификация угроз на ОС

- Угрозы безопасности операционной системы можно классифицировать по различным аспектам их реализации.

- **Классификация угроз**
  - по цели атаки
  - по принципу воздействия на операционную систему
  - по типу используемой злоумышленником уязвимости защиты
  - по характеру воздействия на ОС

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 ОС

- 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 запрещен;
- 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 ОС

- активное воздействие – несанкционированные действия злоумышленника в системе;
- пассивное воздействие – несанкционированное наблюдение злоумышленника за процессами, происходящими в системе.

Классификация угроз на ОС

- Угрозы безопасности ОС можно также классифицировать по таким признакам, как способ действий злоумышленника, используемые средства атаки, объект атаки, способ воздействия на объект атаки, состояние атакуемого объекта ОС на момент атаки.

Типичные атаки на ОС

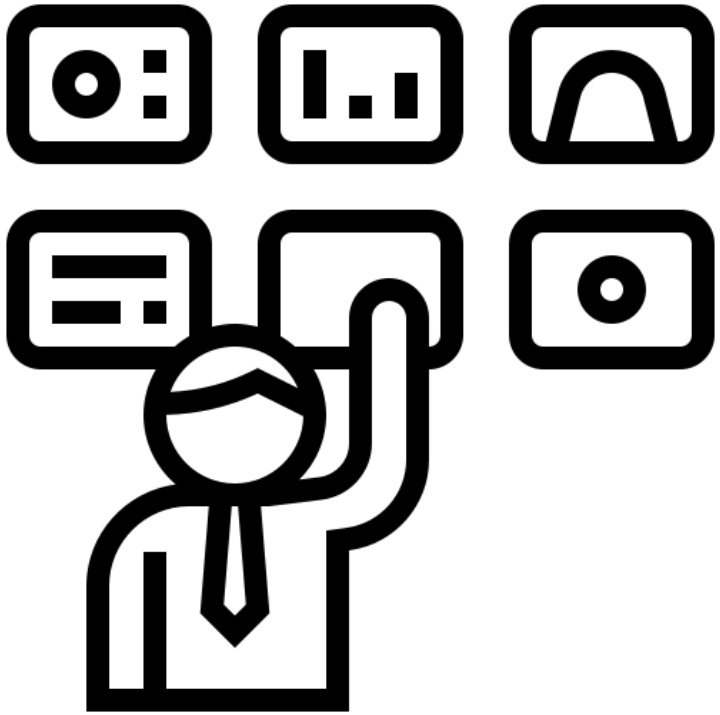
- **Сканирование файловой системы**. Злоумышленник просматривает файловую систему компьютера и пытается прочесть (или скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, который должен быть ему запрещен;
- **Подбор пароля**. Существует несколько методов подбора паролей пользователей:
  - тотальный перебор;
  - тотальный перебор, оптимизированный по статистике встречаемости символов или с помощью словарей;
  - подбор пароля с использованием знаний о пользователе (его имени, фамилии, даты рождения, номера телефона и т. д.);

Типичные атаки на ОС

- **Кража ключевой информации**. Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией (смарткарта, Touch Memory и т. д.) может быть просто украден;
- **Сборка мусора**. Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Злоумышленник восстанавливает эту информацию, просматривает ее и копирует интересующие его фрагменты;
- **Превышение полномочий**. Злоумышленник, 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;

Типичные атаки на ОС

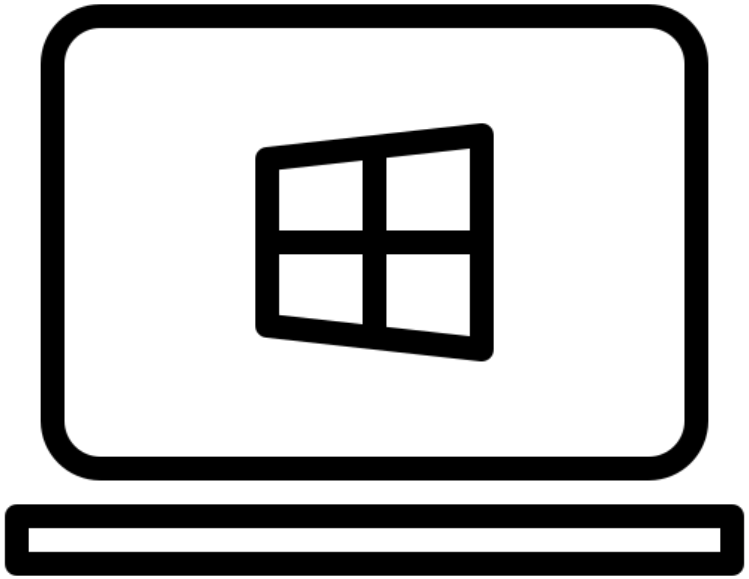
- **Программные закладки**. Программные закладки, внедряемые в операционные системы, не имеют существенных отличий от других классов программных закладок;
- **Жадные программы** – это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху операционной системы.
- **Вирусы.** Заражение ОС вирусами или шифровальщиками.



2. Архитектура подсистемы защиты операционной системы

Архитектура подсистемы защиты операционной системы

- Элементами архитектуры подсистемы защиты операционной системы являются:
  - Основные функции подсистемы защиты операционной системы
  - Идентификация, аутентификация и авторизация субъектов доступа
  - Разграничение доступа к объектам операционной системы
  - Аудит



2.1. Основные функции подсистемы защиты операционной системы

Подсистема защиты ОС

- Подсистема защиты ОС выполняет следующие основные функции:
  - Идентификация и аутентификация
  - Разграничение доступа
  - Аудит
  - Управление политикой безопасности
  - Криптографические функции
  - Сетевые функции

Подсистема защиты ОС

- **Идентификация и аутентификация**. Ни один пользователь не может начать работу с операционной системой, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.
- **Разграничение доступа**. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.
- **Аудит**. Операционная система регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

Подсистема защиты ОС

- **Управление политикой безопасности**. Политика безопасности должна постоянно 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.
- **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.
- **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 защиты ОС

- Подсистема защиты обычно не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Между различными модулями подсистемы защиты существует четко определенный интерфейс, используемый при взаимодействии модулей для решения общих задач.

2.2. Идентификация, аутентификация и авторизация субъектов доступа.

Идентификация, аутентификация и авторизация

- В защищенной ОС любой пользователь (субъект доступа), перед тем как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию.

Идентификация

- **Идентификация** *субъекта доступа* заключается в том, что пользователь (субъект) сообщает операционной системе идентифицирующую информацию о себе (имя, учетный номер) и таким образом идентифицирует себя.

Аутентификация

- Для того чтобы установить, что пользователь именно тот, за кого себя выдает, в информационных системах предусмотрена процедура **аутентификации**, задача которой – предотвращение доступа к системе нежелательных лиц.

- **Аутентификация** субъекта доступа заключается в том, что субъект предоставляет операционной системе, помимо идентифицирующей информации, еще и аутентифицирующую информацию, подтверждающую, что он действительно является тем субъектом доступа, к которому относится идентифицирующая информация.

Авторизация

- **Авторизация** субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия, необходимые для того, чтобы субъект мог начать работу в системе.

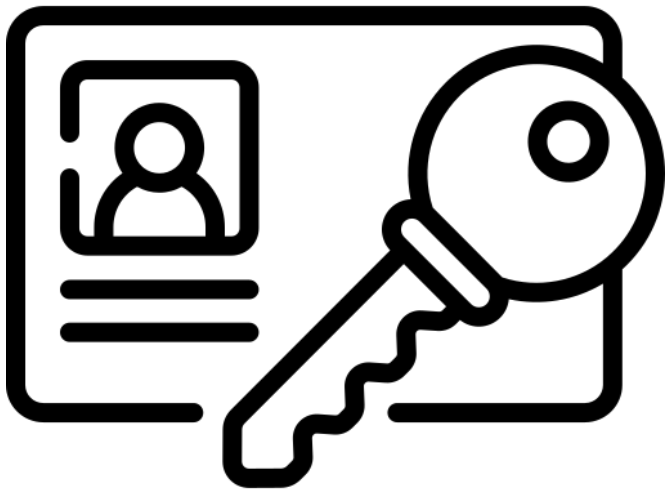
- **Авторизация** субъекта не относится напрямую к подсистеме защиты операционной системы. В процессе авторизации решаются технические задачи, связанные с организацией начала работы в системе уже идентифицированного и аутентифицированного субъекта доступа.

Идентификация и аутентификация

- С точки зрения обеспечения безопасности ОС, процедуры идентификации и аутентификации являются весьма ответственными.
- Действительно, если злоумышленник сумел войти в систему от имени другого пользователя, он легко получает доступ ко всем объектам ОС, к которым имеет доступ этот пользователь. Если при этом подсистема аудита генерирует сообщения о событиях, потенциально опасных для безопасности ОС, то в журнал аудита записывается не имя злоумышленника, а имя пользователя, от имени которого злоумышленник работает в системе.

Методы идентификации и аутентификации

- Наиболее распространенными методами идентификации и аутентификации являются следующие:
  - идентификация и аутентификация с помощью имени и пароля;
  - идентификация и аутентификация с помощью внешних носителей ключевой информации;
  - идентификация и аутентификация с помощью биометрических характеристик пользователей.



2.3. Разграничение доступа к объектам операционной системы.

Разграничение доступа к объектам ОС

- Основными понятиями процесса разграничения доступа к объектам операционной системы являются объект доступа, метод доступа к объекту и субъект доступа.

- **Объектом доступа** (или просто объектом) называют любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Возможность доступа к объектам ОС определяется не только архитектурой операционной системы, но и текущей политикой безопасности. Под объектами доступа понимают, как ресурсы оборудования, так и программные ресурсы. В качестве примера ресурсов оборудования можно привести процессор, принтер, жесткие диски и ленты. Каждый объект имеет уникальное имя, отличающее его от других объектов в системе, и может быть доступен через хорошо определенные и значимые операции.

Разграничение доступа к объектам ОС

- **Методом доступа** к объекту называется операция, определенная для объекта. Тип операции зависит от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а для файлов могут быть определены методы доступа «чтение», «запись » и «добавление» (дописывание информации в конец файла).

- **Субъектом доступа** называют любую сущность, способную инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа). Обычно полагают, что множество субъектов доступа и множество объектов доступа не пересекаются.

Разграничение доступа к объектам ОС

- Иногда к субъектам доступа относят процессы, выполняющиеся в системе. Однако логичнее считать субъектом доступа именно пользователя, от имени которого выполняется процесс. Естественно, под субъектом доступа подразумевают не физического пользователя, работающего с компьютером, а «логического», от имени которого выполняются процессы операционной системы.

- Таким образом, **объект доступа** – **это то, к чему осуществляется доступ**, **субъект доступа – это тот, кто осуществляет доступ**, и **метод доступа – это то, как осуществляется доступ.**

- Для объекта доступа может быть определен **владелец – субъект**, которому принадлежит данный объект и который несет ответственность за конфиденциальность содержащейся в объекте информации, а также за целостность и доступность объекта.

Разграничение доступа к объектам ОС

- Обычно владельцем объекта автоматически назначается субъект, создавший данный объект; в дальнейшем владелец объекта может быть изменен с использованием соответствующего метода доступа к объекту. На владельца, как правило, возлагается ответственность за корректное ограничение прав доступа к данному объекту других субъектов.
- **Правом доступа к объекту** называют право на получение доступа к объекту по некоторому методу или группе методов. Например, если пользователь имеет возможность читать файл, говорят, что он имеет право на чтение этого файла. Говорят, что субъект имеет некоторую привилегию, если он имеет право на доступ по некоторому методу или группе методов ко всем объектам ОС, поддерживающим данный метод доступа.
- **Разграничением доступа субъектов к объектам** является совокупность правил, определяющая для каждой тройки субъект–объект–метод, разрешен ли доступ данного субъекта к данному объекту по данному методу. При избирательном разграничении доступа возможность доступа определена однозначно для каждой тройки субъект–объект–метод, при полномочном разграничении доступа ситуация несколько сложнее.
- Субъекта доступа называют суперпользователем, если он имеет возможность игнорировать правила разграничения доступа к объектам.

Правила разграничения доступа

- Правила разграничения доступа, действующие в операционной системе, устанавливаются администраторами системы при определении текущей политики безопасности. За соблюдением этих правил субъектами доступа следит монитор ссылок – часть подсистемы защиты операционной системы.

- **Правила разграничения доступа должны удовлетворять следующим требованиям:**

1. Правила разграничения доступа, принятые в операционной системе, должны соответствовать аналогичным правилам, принятым в организации, в которой установлена эта ОС.

Иными словами, если согласно правилам организации, доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен.

Правила разграничения доступа

2. Правила разграничения доступа не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ОС.
3. Любой объект доступа должен иметь владельца. Недопустимо присутствие ничейных объектов – объектов, не имеющих владельца.
4. Недопустимо присутствие недоступных объектов – объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа.
5. Недопустима утечка конфиденциальной информации.

Основные модели разграничения доступа

- **Существуют две основные модели разграничения доступа:**
  - **избирательное (дискреционное) разграничение доступа;**
  - **полномочное (мандатное) разграничение доступа.**

- **При избирательном разграничении доступа (Discretionary Access Control)** определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов.
- Большинство операционных систем реализуют именно избирательное разграничение доступа.
- **Полномочное разграничение доступа** заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов.

Избирательное разграничение доступа

- Система правил избирательного разграничения доступа формулируется следующим образом.

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой тройки субъект–объект–метод возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа.

Избирательное разграничение доступа

- Избирательное разграничение доступа является наиболее распространенным способом разграничения доступа. Это обусловлено его сравнительной простотой реализации и необременительностью правил такого разграничения доступа для пользователей. Главное достоинство избирательного разграничения доступа – гибкость; основные недостатки – рассредоточенность управления и сложность централизованного контроля.

- Вместе с тем защищенность операционной системы, подсистема защиты которой реализует только избирательное разграничение доступа, в некоторых случаях может оказаться недостаточной.

Изолированная (или замкнутая) программная среда

- Расширением модели избирательного разграничения доступа является **изолированная (или замкнутая) программная среда**.
- При использовании изолированной программной среды права субъекта на доступ к объекту определяются не только правами и привилегиями субъекта, но и процессом, с помощью которого субъект обращается к объекту.
- Можно, например, разрешить обращаться к файлам с расширением .doc только программам Word, Word Viewer и WPview.

Изолированная (или замкнутая) программная среда

- Система правил разграничения доступа для модели изолированной программной среды формулируется следующим образом:

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой четверки субъект–объект–метод–процесс возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу.
5. Для каждого субъекта определен список программ, которые этот субъект может запускать.

Изолированная (или замкнутая) программная среда

- Изолированная программная среда существенно повышает защищенность операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы. Кроме того, при использовании данной модели повышается защищенность целостности данных, хранящихся в системе. В то же время изолированная программная среда создает определенные сложности в администрировании операционной системы. Например, при установке нового программного продукта администратор должен изменить списки разрешенных программ для пользователей, которые должны иметь возможность работать с этим программным продуктом.
- Изолированная программная среда не защищает от утечки конфиденциальной информации.

Полномочное разграничение доступа с контролем информационных потоков

- Полномочное, или мандатное, разграничение доступа (Mandatory Access Control) обычно применяется в совокупности с избирательным разграничением доступа. Рассмотрим именно такой случай.

Правила разграничения доступа в данной модели формулируются следующим образом:

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.

Полномочное разграничение доступа с контролем информационных потоков

3. Для каждой четверки субъект–объект–метод–процесс возможность доступа определена однозначно в каждый момент времени. При изменении состояния процесса со временем возможность предоставления доступа также может измениться. Вместе с тем в каждый момент времени возможность доступа определена однозначно. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.

Полномочное разграничение доступа с контролем информационных потоков

5. В множестве объектов выделяется множество объектов полномочного разграничения доступа. Каждый объект полномочного разграничения доступа имеет гриф секретности. Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен. Если объект не является объектом полномочного разграничения доступа или несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа.
6. Каждый субъект доступа имеет уровень допуска. Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект. Нулевое значение уровня допуска означает, что субъект не имеет допуска. Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.

Полномочное разграничение доступа с контролем информационных потоков

7. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:

   – объект является объектом полномочного разграничения доступа;

   – гриф секретности объекта строго выше уровня допуска субъекта, обращающегося к нему;

   – субъект открывает объект в режиме, допускающем чтение информации.

   Это правило называют правилом NRU (Not Read Up – не читать выше).

8. Каждый процесс операционной системы имеет уровень конфиденциальности, равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования. Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.

Полномочное разграничение доступа с контролем информационных потоков

9. Доступ субъекта к объекту должен быть запрещен независимо от состояния матрицы доступа, если:
   – объект является объектом полномочного разграничения доступа;
   – гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему;
   – субъект собирается записывать в объект информацию.
   Это правило разграничения доступа предотвращает утечку секретной информации. Это так называемое правило NWD (Not Write Down – не записывать ниже).

10. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:
   – имеет доступ к объекту согласно правилу 7;
   – обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

Полномочное разграничение доступа с контролем информационных потоков

- При использовании данной модели разграничения доступа существенно страдает производительность операционной системы, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтения/записи.

- Кроме того, данная модель разграничения доступа создает пользователям определенные неудобства, связанные с тем, что если уровень конфиденциальности процесса строго выше нуля, то вся информация в памяти процесса фактически является секретной и не может быть записана в несекретный объект.

Сравнительный анализ моделей разграничения доступа

Свойства модели	Избирательное разграничение доступа	Изолированная программная среда	Полномочное разграничение доступа с контролем потоков
Защита от утечки информации	Отсутствует	Отсутствует	Имеется
Защищенность от разрушающих воздействий	Низкая	Высокая	Низкая
Сложность реализации	Низкая	Средняя	Высокая
Сложность администрирования	Низкая	Средняя	Высокая
Затраты ресурсов компьютера	Низкие	Низкие	Высокие
Использование ПО, разработанного для других систем	Возможно	Возможно	Проблематично

2.4. Аудит

Аудит

- Процедура аудита применительно к ОС заключается в регистрации в специальном журнале, называемом журналом аудита, или журналом безопасности, событий, которые могут представлять опасность для операционной системы. Пользователи системы, обладающие правом чтения журнала аудита, называются аудиторами.

Аудит

- Необходимость включения в защищенную операционную систему функций аудита обусловлена следующими обстоятельствами:
  - обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;
  - подсистема защиты ОС может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал аудита, сможет установить, что произошло при вводе пользователем неправильного пароля – ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20–30 раз – это явная попытка подбора пароля;
  - администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом. Такую возможность обеспечивает журнал аудита;
  - если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась. Журнал аудита может содержать всю необходимую информацию.

Аудит

- К числу событий, которые могут представлять опасность для операционной системы, обычно относят следующие:
  - вход или выход из системы;
  - операции с файлами (открыть, закрыть, переименовать, удалить);
  - обращение к удаленной системе;
  - смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).
- Если фиксировать в журнале аудита все события, объем регистрационной информации будет расти слишком быстро, что затруднит ее эффективный анализ. Необходимо предусмотреть выборочное протоколирование как в отношении пользователей, так и в отношении событий.

Политика аудита

- **Политика аудита – это совокупность правил, определяющих то, какие события должны регистрироваться в журнале аудита.**
- Для обеспечения надежной защиты операционной системы **в журнале аудита должны обязательно регистрироваться следующие события:**
  - попытки входа/выхода пользователей из системы;
  - попытки изменения списка пользователей;
  - попытки изменения политики безопасности, в том числе и политики аудита.
- Окончательный выбор того, какие события должны регистрироваться в журнале аудита, а какие не должны, возлагается на аудиторов. При выборе оптимальной политики аудита следует учитывать ожидаемую скорость заполнения журнала аудита. Политика аудита должна оперативно реагировать на изменения в конфигурации операционной системы, в характере хранимой и обрабатываемой информации, а особенно на выявленные попытки атаки операционной системы.
- В некоторых ОС подсистема аудита, помимо записи информации о зарегистрированных событиях в специальный журнал, предусматривает возможность интерактивного оповещения аудиторов об этих событиях.

Шесть основных средств усиления защиты операционной системы

Усиление защиты		
Удаление ненужного ПО	Удаление ненужных служб	Замена аккаунтов по умолчанию
Принцип наименьших привилегий	Регулярные обновления	Ведение журнала и аудит

Методы и средства зашиты информации в типовых ОС

- **Операционная система (ОС)** есть специально организованная совокупность программ, которая управляет ресурсами системы (ЭВМ, вычислительной системы, других компонентов И ВС) в целях наиболее эффективного их использования и обеспечивает интерфейс пользователя с ресурсами.
- Под **механизмами защиты ОС** понимаются 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.

Методы и средства зашиты информации в типовых ОС

- **Под безопасностью ОС** понимается 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.

Методы и средства зашиты информации в типовых 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, которые обусловлены наличием следующих событий:
  - Игнорирование идентификации ресурсов
  - Использование паролей
  - Незащищенное хранение списка паролей
  - Неограниченное число попыток несанкционированного входа
  - Подразумеваемое доверие
  - Использование общей памяти
  - Разрыв связи
  - Передача параметров по ссылке
  - Большое количество элементов используемых ОС

Дефекты ОС с точки зрения обеспечения безопасности данных

- **Игнорирование идентификации ресурсов.** 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.
- **Использование паролей.** Большинство пользователей выбирают простейшие пароли, которые легко подобрать или угадать.
- **Незащищенное хранение списка паролей.** Хранение списка паролей в незашифрованном виде дает возможность его компрометации с последующим НСД к данным.

Дефекты ОС с точки зрения обеспечения безопасности данных

- **Неограниченное число попыток несанкционированного входа.** Для предотвращения попыток несанкционированного входа в систему с помощью подбора пароля необходимо ограничить число таких попыток, что в некоторых ОС не предусмотрено.
- **Подразумеваемое доверие.** Во многих случаях программы ОС считают, что другие программы работают правильно.
- **Использование общей памяти.** При использовании общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП).

Дефекты ОС с точки зрения обеспечения безопасности данных

- **Разрыв связи.** В случае разрыва связи ОС должна немедленно закончить сеанс работы с пользователем или повторно установить подлинность субъекта.
- **Передача параметров по ссылке**, а не по значению. При передаче параметров но ссылке возможно сохранение параметров в ОП после проверки их корректности, нарушитель может изменить эти данные до их использования.
- **Большое количество элементов используемых ОС**. ОС использует большое количество элементов, например, программ, имеющих различные привилегии.

Дефекты ОС с точки зрения обеспечения безопасности данных

- **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.

Защита информации

Тема: Защита информации в операционных системах

Благодарю за внимание

КУТУЗОВ Виктор Владимирович