Основные понятия безопасности ОС

Основные определения

Безопасность отдельных компьютеров – защита данных, хранящихся и обрабатывающихся компьютером, рассматриваемым как автономная система.

Сетевая безопасность – защита данных при передаче по линиям связи и защита от несанкционированного доступа в сеть.

Конфиденциальность – гарантия того, что информация будет доступна только авторизованным пользователям (легальным).

Целостность – гарантия сохранности данными правильных значений.

Основные определения

Доступность – постоянная готовность системы к обслуживанию авторизованных пользователей.

Аутентичность – способность системы проверять идентичность пользователя.

Угроза – любое действие, направленное на нарушение конфиденциальности, целостности и/или доступности информации, а также нелегальное использование ресурсов информационной системы.

Атака – реализованная угроза.

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

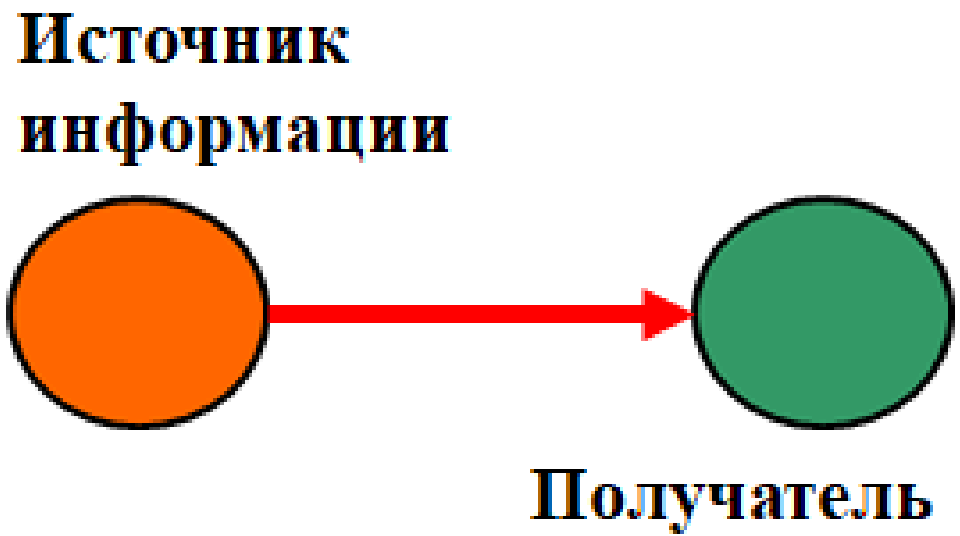
Основные определения

Типы умышленных угроз:

- незаконное проникновение в один из компьютеров сети под видом легального пользователя;
- разрушение системы с помощью программ-вирусов;
- нелегальные действия легального пользователя;
- подслушивание внутрисетевого трафика.

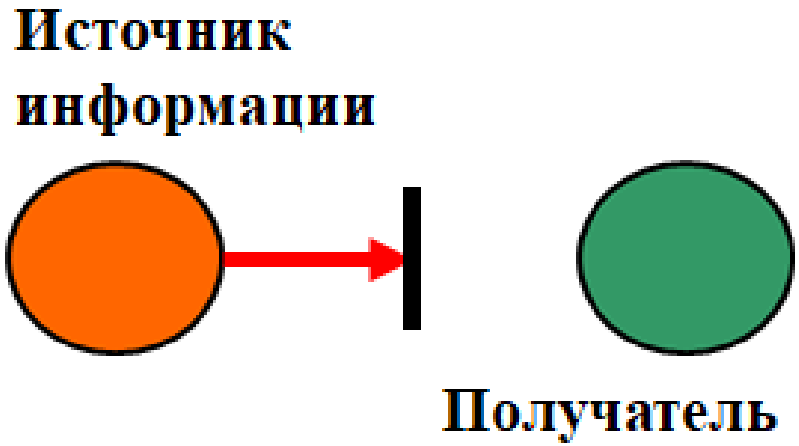
Нормальная передача

Информации от источника информации к получателю.



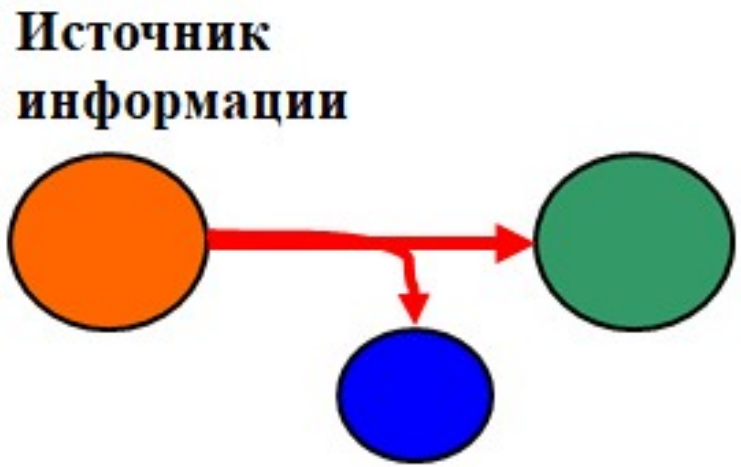
Прерывание

Компоненты системы выходят из строя, становятся недоступными или непригодными. Это атака, целью которой является нарушение доступности.



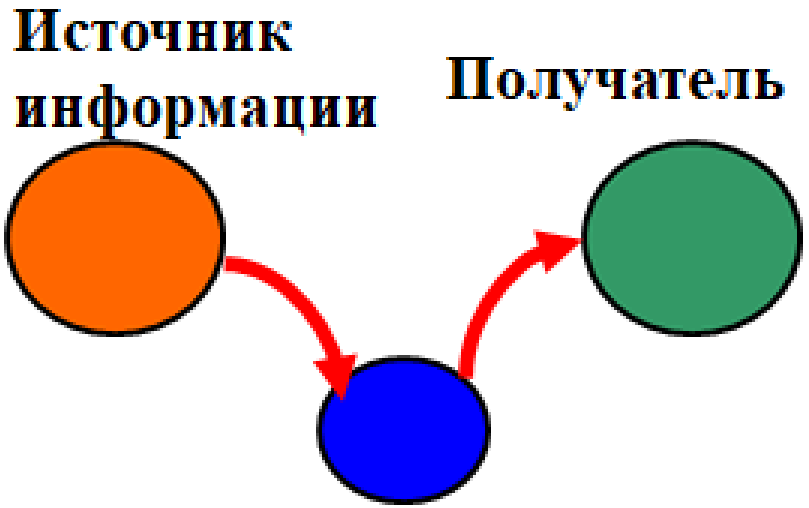
Перехват

Это атака, целью которой является нарушение конфиденциальности, в результате чего доступ к компонентам системы получают несанкционированные стороны.



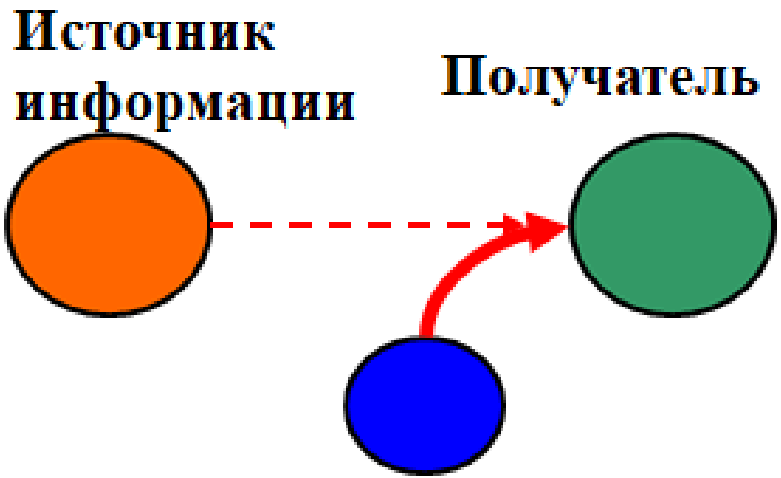
Изменение

Несанкционированная сторона не только получает доступ к системе, но и вмешивается в работу ее компонентов. Целью атаки является нарушение целостности.



Подделка

Несанкционированная сторона помещает в систему поддельные объекты. Целью этой атаки является нарушение аутентичности.



Злоумышленник

Злоумышленник – нелегальный пользователь, сумевший зарегистрироваться в системе.

Пассивный злоумышленник пытается прочитать то, что ему не положено.

Активный злоумышленник пытается незаконно изменить данные с различными целями, вплоть до разрушения системы (хакеры, кракеры).

Злоумышленник

Злоумышленник – нелегальный пользователь, сумевший зарегистрироваться в системе.

Пассивный злоумышленник пытается прочитать то, что ему не положено.

Активный злоумышленник пытается незаконно изменить данные с различными целями, вплоть до разрушения системы (хакеры, кракеры).

Категории злоумышленников

- Случайные любопытные пользователи, не применяющие специальных технических и программных средств.
- Притворщик – лицо, не обладающее полномочиями по использованию компьютера, проникающее в систему путем использования учетной записи законного пользователя.
- Правонарушитель – законный пользователь, получающий доступ к ресурсам, к которым у него нет доступа, или тот, у которого есть такой доступ, но он злоупотребляет своими привилегиями.
- Тайный пользователь – лицо, завладевшее управлением в режиме суперпользователя и использующее его, чтобы избежать аудита и преодолеть контроль доступа.
- Лица, занимающиеся коммерческим или военным шпионажем.
- Взломщики.

Защищенные системы

- Можно ли создать защищенную компьютерную систему?
- Если да, то почему она до сих пор не создана?