Защита информации от утечки

Судаков Леонид
Коркин Федор

Содержание

- Несанкционированный доступ
- Средства защиты информации
- Биометрические системы защиты
- Методы защиты от вредоносных программ
- Резервное копирование и восстановление данных
- Хакерские утилиты и защита от них
- Заключение

Несанкционированный доступ

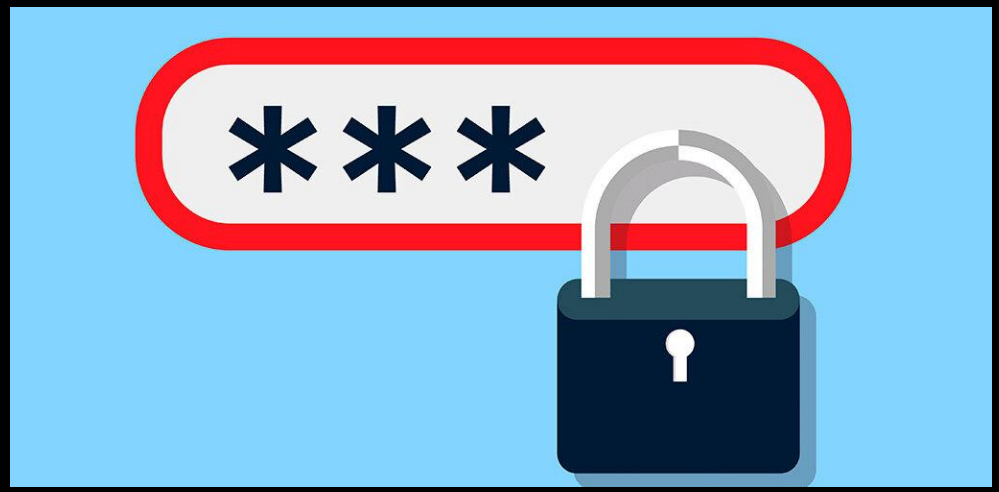
Несанкционированный доступ - действия, нарушающие установленный порядок
доступа или правила разграничения, доступ к программам и данным, который получают абоненты, которые не прошли регистрацию и не имеют права на ознакомление или работу
с этими ресурсами.
Для предотвращения несанкционированного доступа осуществляется контроль доступа

Защита с использованием паролей

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются пароли.

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам.

При этом может производиться регистрация всех попыток несанкционированного доступа.



Защита информации

Защита информации – это деятельность, направленная на предотвращение утечки информации, несанкционированных и непреднамеренных воздействий на информацию

Средства защиты информации

Средства защиты информации — это совокупность инженерно-технических, электронных, и других устройств и приспособлений, приборов используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Средства защиты информации разделяются на:

- Технические (аппаратные) средства
- Программные средства
- Организационные средства

Биометрические системы защиты

Для защиты от несанкционированного доступа к информации используются биометрические системы идентификации.

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.

Цифровая (электронная) подпись

eSign - программа для идентификации подписи, использующая специальную цифровую ручку и электронный блокнот для регистрации подписи.
В процессе регистрации eSign запоминает не только само изображение подписи, но и динамику движения пера. eSign анализирует целый ряд параметров, включающих и общие признаки почерка конкретного лица.

Хакерские утилиты и защита от них

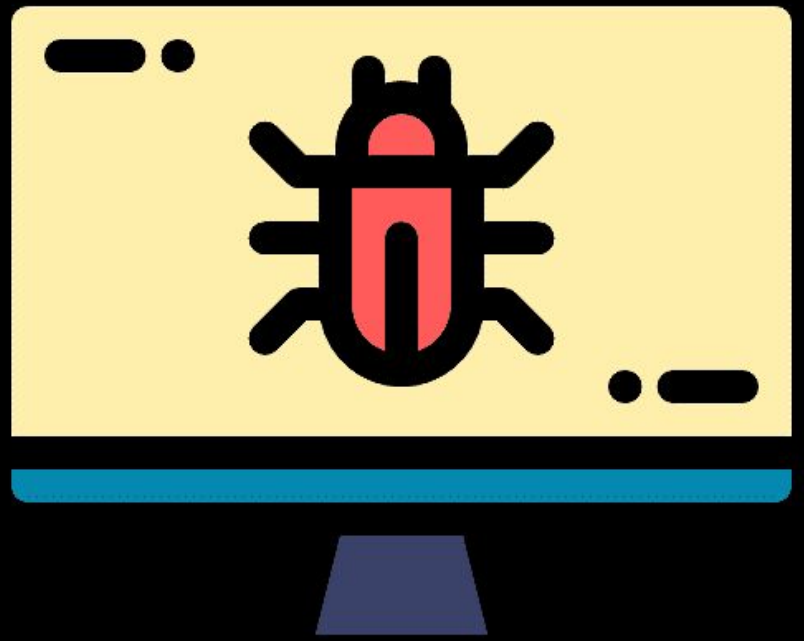
Сетевые атаки на удаленные серверы
реализуются с помощью специальных программ, которые посылают
на них многочисленные запросы. Это приводит к зависанию сервера, если ресурсы атакуемого сервера недостаточны для обработки всех поступающих запросов.

Некоторые хакерские утилиты реализуют фатальные сетевые атаки. Такие утилиты используют уязвимости в операционных системах и приложениях и отправляют специально оформленные запросы на атакуемые компьютеры в сети. В результате сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении, и система прекращает работу.

Утилиты взлома удалённых компьютеров

Утилиты взлома удаленных компьютеров предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими или для внедрения во взломанную систему других вредоносных программ.

Профилактическая защита от таких хакерских утилит состоит в своевременной загрузке из Интернета обновлений системы безопасности операционной системы и приложений.



Заключение

Информация сегодня стоит дорого и её необходимо охранять. Массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.