Тема 2.1 Защита информации в компьютерных сетях

Сегодня защита информации становится обязанностью каждого пользователя системы, что требует не только навыков обращения с системой безопасности, но и знаний о способах неправомерного доступа для предотвращения такового.

Надежный контроль над информацией обеспечивает безопасность бизнеса, а так же позволяет качественно и своевременно устранять ошибки, возникающие в течение производственных процессов, облегчая работу персонала.

Можно выделить три основных уровня защиты информации:

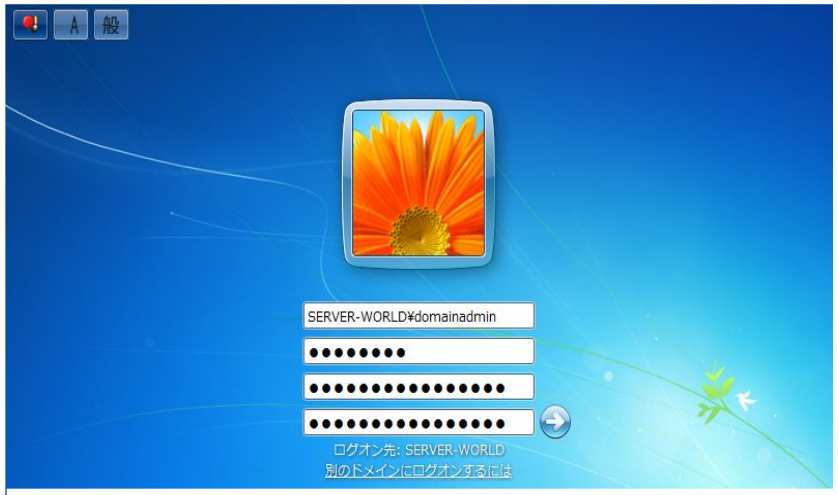
1. *защита информации на уровне рабочего места пользователя;*
2. *защита информации на уровне подразделения предприятия;*
3. *защита информации на уровне предприятия.*

Основными методами совершения преступления являются:

1. Надувательство с данными является самым распространенным методом при совершении компьютерных преступлений, так как он не требует технических знаний и относительно безопасен. Информация меняется в процессе ее ввода в компьютер или вовремя вывода. Например, при вводе документы могут быть заменены фальшивыми, вместо рабочих дискет подсунуты чужие, и данные могут быть сфальсифицированы.

2. Сканирование является распространенным методом получения информации, который может привести к преступлению. Служащие, читающие файлы других, могут обнаружить там персональную информацию о своих коллегах. Информация, позволяющая получить доступ к компьютерным файлам или изменить их, может быть найдена после просмотра мусорных корзин. Дискеты, оставленные на столе, могут быть прочитаны, скопированы и украдены. Существуют сканирующие программы, которые могут, просматривая лишь остаточную информацию, оставшуюся на компьютере или на носителе информации после выполнения сотрудником задания и удаления своих файлов, получать эту информацию в более полном виде.

3. Метод «троянский конь» предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам).



Меры защиты информации

1. Контроль доступа к информации в компьютере и к прикладным программам. Вы должны иметь гарантии того, что только авторизованные пользователи имеют доступ к информации и приложениям.

Требуйте, чтобы пользователи выполняли процедуры входа в компьютер, и используйте это как средство для идентификации в начале работы.

2. Другие меры защиты. Пароли - только один из типов идентификации - что-то, что знает только пользователь. Двумя другими типами идентификации, которые тоже эффективны, является что-то, чем владеет пользователь (например, магнитная карта), или уникальные характеристики пользователя (его голос).

Если в компьютере имеется встроенный стандартный пароль (пароль, который встроен в программы и позволяет обойти меры по управлению доступом), обязательно измените его. Сделайте так, чтобы программы в компьютере после входа пользователя в систему сообщали ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит своевременно получать информацию о попытках проникновения в защищаемую систему.

3. Защита файлов. Помимо идентификации пользователей и процедур авторизации разработайте процедуры по ограничению доступа к файлам с данными.

Межсетевой экран, сетевой экран, файервол, брандмауэр (Firewall) — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Контрольные вопросы:

1. Перечислите рекомендации по созданию сложного *пароля (5-6 рекомендаций).*
2. *Что такое авторизация?*
3. *Что такое аутентификация?*
4. *Что такое электронная цифровая подпись?*
5. *Что такое шифрование?*
6. *Что такое криптографическая стойкость?*