Основные понятия и проблемы БКС

1. Под защитой информации в системах и сетях подразумевается ограничение доступа к информации в целях сохранности и конфиденциальности данных посредством применения технических, организационных и правовых мер.
2. ИБ КИС (информационная безопасность корпоративных информационных систем) – организация хранения и способов доступа к данным опираясь на требования корпорации, при этом обеспечив сохранность и конфиденциальность данных корпорации.
3. Угроза конфиденциальности – угроза получения личных или же иных ценных данных третьими лицами.

Угроза целостности – угроза безвозвратной потери личных или же иных ценных данных.

Угроза доступности – угроза потери доступа к данным.

Все вышеперечисленные категории угроз могут быть вызваны сбоем системы, ошибкой, человеческим фактором или преднамеренной атакой.

1. Порча средств хранения или доступа к информации

Кража средств хранения или доступа к информации

Получение информации о средствах хранения, доступа к информации, программного обеспечения и средств безопасности.

Попытка получения доступа к информации при помощи найденных уязвимостей

Применение софта, способного взламывать пароли или обходить защиту

Отслеживание и дешифровка сетевого трафика

1. Информационная система – система, предназначенная для хранения и обработки информации, включающая в себя аппаратное и программное обеспечение.
2. Информационные ресурсы – ресурсы, представленные в виде баз данных, документов, библиотек, предназначенные для многократного использования.
3. Основу политики безопасности составляет совокупность требований к защищённости данных, на которую опираются люди при построении информационной системы.
4. Отсутствие подключения к глобальной сети или полный контроль над обменом данными с глобальной сетью посредством аппаратно-программного комплекса.

Использование наиболее совершенных методов шифрования для передачи данных через глобальную сеть.

Резервное копирование данных.

Ограничение доступа для пользователей.

Использование только лицензионного ПО и его постоянное обновление.

Запрет на использование макрокоманд приложениям и файлам, не имеющим доверия.

1. Объект защиты информации – информация, носитель информации или информационный процесс, которые необходимо защищать.
2. К информационным процессам относится: получение, хранение, передача, обработка и использование информации.
3. Ответ в 5-ом
4. Ответ в 6-ом
5. Если речь идёт о защите данных, то можно привести следующие примеры:

Маршрутизатор с программой, позволяющей отслеживать трафик и выводить на экран ПК. Позволят максимально обезопасить устройство, или локальную сеть от утечки данных.

Сканер отпечатка пальцев с программой, сопоставляющий сканированный отпечаток с отпечатком, привязанным к аккаунту. Позволяет не вводить пароль.

Система видео наблюдения в серверных. Позволяет отследить, кто получал доступ напрямую к серверу с данными.