**Бабаев Антон,Юрчик Максим группа 215**

**Тема 17. Сетевая безопасность**  
**Ответы на вопросы:**  
  
1. Что относится к безопасности компьютера?  
К безопасности компьютера относят все проблемы защиты данных, хранящихся и обрабатывающихся компьютером, который рассматривается как автономная система. Эти проблемы решаются средствами операционных систем и приложений, таких как базы данных, а также встроенными аппаратными средствами компьютера.  
  
2. Что понимается под сетевой безопасностью?  
Под сетевой безопасностью понимают все вопросы, связанные с взаимодействием устройств в сети, это прежде всего защита данных в момент их передачи по линиям связи защита от несанкционированного удаленного доступа в сеть.  
  
3. Дайте определение безопасной информационной системе. Какими свойствами она обладает?  
Безопасная информационная система — это система, которая, во-первых, защищает данные от несанкционированного доступа, во-вторых, всегда готова предоставить их своим пользователям, а в-третьих, надежно хранит информацию и гарантирует неизменность данных. Таким образом, безопасная система по определению обладает свойствами конфиденциальности, доступности и целостности.  
  
4.Что называется угрозой?  
Любое действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети, называется угрозой  
  
5. Что называется атакой?  
Реализованная угроза называется атакой.  
  
6.Что такое «риск»?  
Риск — это вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки.  
  
7.Охарактеризуйте умышленную угрозу, неумышленную.  
Неумышленные угрозы вызываются ошибочными действиями лояльных сотрудников, становятся следствием их низкой квалификации или безответственности.  
  
Умышленные угрозы могут ограничиваться либо пассивным чтением данных или мониторингом системы, либо включать в себя активные действия, например нарушение целостности и доступности информации, приведение в нерабочее состояние приложений устройств.  
  
8.Перечислите 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 графика.  
9.Перечислите средства защиты сетевой безопасности.  
- морально-этические средства защиты;  
- законодательные средства защиты;  
- административные меры;  
- психологические меры;  
- физические средства защиты.  
  
10. На какие вопросы подразумевает ответы политика информационной безопасности?  
- Какую информацию защищать?  
- Какой ущерб понесет предприятие при потере или при раскрытии тех или иных данных?  
- Кто или что является возможным источником угрозы, какого рода атаки на безопасность системы могут быть предприняты?  
- Какие средства использовать для защиты каждого вида информации?  
  
11. Какие принципы нужно учитывать при формировании политики информационной безопасности?  
- минимальный уровень привилегий;  
- комплексный подход;  
- баланс надежности защиты всех уровней;  
- максимальная защита;  
- принцип единого контрольно-пропускного пункта;  
- принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение.  
  
12. Какие пункты включает в себя политика доступа к сетевым службам Интернета?  
- Определение списка служб Интернета, к которым пользователи внутренней сети должны иметь ограниченный доступ;  
- Определение ограничений на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и РРР (Point-to-Point Protocol).  
- Принятие решения о том, разрешен ли доступ внешних пользователей из Интернета во внутреннюю сеть. Если да, то кому.   
  
  
  
**Отметка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** **Подпись преподавателя \_\_\_\_\_\_\_\_\_\_\_ / А.И. Недера**