Практическое занятие 1. Настройка политики безопасности.

Контрольные вопросы

1. Какие события безопасности должны фиксироваться в журнале аудита?

В журнал аудита следует записывать события, важные для контроля безопасности системы, такие как попытки входа в систему (успешные и неудачные), изменение прав доступа, создание новых учетных записей, удаление файлов и прочие операции, способные повлиять на безопасность.

2. Какие параметры определяют политику аудита?

Политику аудита формируют три основных параметра:

-Уровень подробностей фиксации событий (детализация);

-Объем хранимых журналов (ограниченный срок хранения или неограниченное хранение);

-Возможность мониторинга действий определенных групп пользователей (например, сотрудников с повышенными привилегиями).

3. Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?

Нет, такое объединение нежелательно. Разделение обязанностей повышает прозрачность процессов управления системой и снижает вероятность злоупотребления полномочиями.

4. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

Анонимный доступ потенциально опасен, так как затрудняет отслеживание действий пользователей и увеличивает риск несанкционированного вмешательства. Рекомендуется ограничить анонимный доступ, вводя идентификацию и авторизацию.

5. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя аутентифицирующая информация)?

Пароль пользователя должен передаваться зашифрованным способом и храниться в хешированном виде, обеспечивая невозможность перехвата пароля злоумышленниками.

6. Нужно ли ограничивать права пользователей прикладных программ и почему?

Да, ограничение прав минимизирует риски воздействия вредоносных программ и уменьшает возможные последствия взлома аккаунта пользователя. Пользователи должны получать минимальные полномочия, достаточные для выполнения рабочих задач.

7. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?

Эффективным считается правило "белого списка" приложений, разрешающее запуск только проверенных и утвержденных программ. Это существенно сокращает угрозу запуска вредоносного ПО.

8. Из каких этапов состоит построение политики безопасности для компьютерной системы?

-Определение ключевых угроз и уязвимостей;

-Формулирование целей политики безопасности;

-Назначение ответственных лиц;

-Создание документа, регламентирующего меры безопасности;

-Реализацию механизмов контроля исполнения политики;

-Периодический мониторинг и обновление политики.

9. К чему может привести ошибочное определение безопасности (приведите примеры)?

-Недостаточный уровень защиты, способствующий утечке конфиденциальных данных;

-Чрезмерные ограничения, снижающие продуктивность сотрудников;

-Потеря доверия клиентов вследствие нарушений конфиденциальности или атак хакеров.

10. Почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

Часто причины пренебрежения связаны с недостатком осведомленности о важности мер безопасности, отсутствием необходимого опыта настройки или ограниченными ресурсами для реализации комплексной политики безопасности. Однако недооценка последствий нарушения безопасности ведет к серьезным рискам и убыткам для организаций