**Лабораторная работа № 10**

**Тема:** Работы по сопровождению: «проактивный» и «реактивный» подход

**Цель:** научиться осуществлять проактивный и реактивный подход в сопровождении.

**Задание 1.**

|  |  |
| --- | --- |
| **Подход к сопровождению** | **Виды работ по сопровождению** |
| Проактивный подход | - Мониторинг и анализ производительности компьютеров и программного обеспечения, чтобы предотвращать возможные сбои и проблемы.  - Проведение регулярных проверок на вирусы и другие угрозы безопасности информации.  - Оптимизация работы компьютеров и программ для повышения производительности и эффективности.  - Планирование и проведение обновлений программного обеспечения и операционных систем для обеспечения их актуальности и безопасности.  - Анализ потребностей автосалона и предложение новых технологических решений для улучшения бизнес-процессов.  - Поддержка внедрения новых программ и систем, включая обучение сотрудников и помощь в переходе на новые технологии.  - Разработка и поддержка политики безопасности информации для защиты данных автосалона от утечек и несанкционированного доступа. |

Задание 2.

|  |  |
| --- | --- |
| **Подход к сопровождению** | **Виды работ по сопровождению** |
| Активный (реактивный) подход | - Решение проблем с компьютерами и программным обеспечением, возникающих у сотрудников автосалона.  - Устранение вирусов и других угроз безопасности, которые могут возникнуть на компьютерах автосалона.  - Помощь сотрудникам в работе с программами и системами, если возникают проблемы или вопросы.  - Быстрое реагирование на сбои в работе компьютеров или программ, чтобы минимизировать простой и ущерб для бизнеса.  - Восстановление данных в случае их потери или повреждения.  - Предоставление экстренной поддержки в случае критических проблем с технологическим оборудованием или программным обеспечением. |

**Контрольные вопросы:**

**1)** 1.Разработка и внедрение проактивных мер безопасности для предотвращения угроз.

2. Проведение регулярного обновления и обслуживания компьютеров и программного обеспечения.

3. Обучение сотрудников основам безопасности информации и правильному использованию технологических ресурсов.

4. Мониторинг и анализ работы систем для выявления потенциальных проблем и улучшения производительности.

5. Разработка и внедрение планов резервного копирования данных для предотвращения потери информации.

**2)** Проактивный подход в обеспечении безопасности информации заключается в предпринятии мер, направленных на предотвращение угроз, до их возникновения. Это включает в себя разработку и внедрение мер безопасности, обучение сотрудников, мониторинг и анализ систем, а также разработку планов резервного копирования данных. Такой подход позволяет минимизировать риски и обеспечить более надежную защиту информации.

**3)** Предпроактивный подход.

Наиболее оптимальный подход с точки зрения прогнозирования потребностей пользователей на недалекую перспективу и затрат рабочих ресурсов на этот процесс.

Пользователь должен сам созреть и осознать необходимость изменения. Навязывать ему что-то, пусть даже объективно более совершенное глупо и не дальновидно.

**4)** 1. Бизнес и управление: разработка и внедрение стратегий безопасности, обучение сотрудников по правилам безопасности, анализ бизнес-процессов на предмет уязвимостей.

2. Здравоохранение: обеспечение безопасности медицинских данных пациентов, защита информации о здоровье и личных данных.

3. Финансы: защита финансовых данных клиентов, предотвращение мошенничества и кражи личной информации.

4. Государственные учреждения: защита государственных секретов, обеспечение безопасности информации о гражданах и деятельности государства.

5. Образование: защита личных данных студентов и преподавателей, обеспечение безопасности образовательных ресурсов и информации.

**5)** Активный подход (реактивный) - более высокая и оперативная степень реагирования на возникающие задачи и проблемы. Тут нет качественного перехода между подходами, нет перехода на другой уровень осознанности и зрелости организации работы, а наблюдается только количественные изменения и преобразования.

**6)** Пассивный подход — это **действие или процесс, который не требует активного вмешательства пользователя или внешнего управления для своего выполнения**. В отличие от активных действий, где пользователь явно указывает, что нужно сделать, пассивные действия происходят автоматически или в фоновом режиме.

**7)** **Пассивный подход:**

Преимущества:

- Позволяет избежать конфликтов и сохранить мирные отношения.

- Может быть полезен в ситуациях, когда нет возможности или необходимости принимать активные меры.

Недостатки:

- Может привести к упущению возможностей и проблемам, которые могли бы быть предотвращены.

- Неэффективен в решении проблем, требующих быстрого реагирования.

**Активный подход:**

Преимущества:

- Позволяет быстро и эффективно реагировать на проблемы и угрозы.

- Может помочь в решении сложных ситуаций, требующих активного вмешательства.

Недостатки:

- Может привести к конфликтам и усилению проблем, если не использовать с умом.

- Требует больших затрат на ресурсы и усилия.

**Предпроактивный подход:**

Преимущества:

- Позволяет предотвращать проблемы до их возникновения.

- Может помочь в создании стабильной и безопасной среды.

Недостатки:

- Может потребовать больших усилий и ресурсов на начальном этапе.

- Не всегда эффективен в ситуациях, требующих быстрого реагирования.

**Проактивный подход:**

Преимущества:

- Позволяет действовать впереди возможных проблем и угроз.

- Может помочь создать благоприятные условия для развития и достижения целей.

Недостатки:

- Требует постоянного мониторинга и анализа ситуации.

- Может быть сложно реализовать в некоторых ситуациях из-за неопределенности и непредсказуемости.