Тема 6: Административный уровень обеспечения информационной безопасности

Цели, задачи и содержание административного уровня

- Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.
- Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.
- Содержанием административного уровня являются следующие мероприятия:
- Разработка политики безопасности.
- Проведение анализа угроз и расчета рисков.

Разработка политики информационной безопасности

- **Политика безопасности** – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.
- Основные направления разработки политики безопасности:
- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

- Результатом разработки политики безопасности является комплексный документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.
- Этот документ является методологической основой практических мер по обеспечению информационной безопасности и включает следующие группы сведений:
- основные положения информационной безопасности организации;
- область применения политики безопасности;
- цели и задачи обеспечения информационной безопасности организации;
- распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

- При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.
- В состав автоматизированной информационной системы входят следующие компоненты:
- **аппаратные средства** – компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – дисководы, принтеры, контроллеры), кабели, линии связи и т. д.;
- **программное обеспечение** – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т. д.;
- **данные** – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т. д.;
- **персонал** – обслуживающий персонал и пользователи.

- С точки зрения обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):
- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- менеджер отдела;
- операторы;
- аудиторы.

- **Специалист по информационной безопасности** (начальник службы безопасности, администратор по безопасности) играет основную роль в разработке и соблюдении политики безопасности предприятия. Он проводит расчет и перерасчет рисков, выявляет уязвимости системы безопасности по всем направлениям (аппаратные средства, программное обеспечение и т. д.).
- **Владелец информации** – лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случае именно владелец информации может определить ее ценность и конфиденциальность.
- **Поставщики аппаратного и программного обеспечения** обычно являются сторонними лицами, которые несут ответственность за поддержание должного уровня информационной безопасности в поставляемых им продуктах.

- **Администратор сети** – лицо, занимающееся обеспечением функционирования информационной сети организации, поддержанием сетевых сервисов, разграничением прав доступа к ресурсам сети на основании соответствующей политики безопасности.
- **Менеджер отдела** является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за их выполнением на рабочих местах. Менеджеры должны доводить до подчиненных все аспекты политики безопасности, которые непосредственно их касаются.
- **Операторы** обрабатывают информацию, поэтому должны знать класс конфиденциальности информации и какой ущерб будет нанесен организации при ее раскрытии.
- **Аудиторы** – внешние специалисты по безопасности, нанимаемые организацией для периодической проверки функционирования всей системы безопасности организации.