Информационная безопасность

Лекция 3

Административный уровень

Административный уровень защиты информации

- Под **административным уровнем** информационной безопасности относятся действия общего характера, предпринимаемые руководством организации к обеспечению защиты информации.
- Главная цель – формирование политики безопасности, отражающей подход организации к защите данных.
- Политика безопасности административного уровня – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.
- Выработку политики безопасности и ее содержание рассматривают на трех горизонтальных уровнях детализации:
  - Верхний уровень – вопросы, относящийся к организации в целом;
  - Средний уровень – вопросы, касающиеся отдельных аспектов ИБ;
  - Нижний уровень – вопросы относящиеся к конкретным сервисам;

Политика безопасности верхнего уровня

- Политика безопасности верхнего уровня, затрагивающая все организацию в целом, включает в себя:
  - решение сформировать или изменить комплексную программу обеспечения информационной безопасности;
  - формулирование целей организации в области информационной безопасности, определение общих направлений в достижении данных целей;
  - обеспечение нормативной базы для соблюдения законов и правил;
  - формулирование административных решений по вопросам, затрагивающих организацию в целом.

Политика безопасности верхнего уровня

- На данном уровне выносится:
  - управление ресурсами защиты и координация использования данных ресурсов;
  - выделение персонала для защиты критически важных систем;
  - определение взаимодействия с внешними организациями, обеспечивающими или контролирующими режим безопасности;
  - определение правил соблюдения законодательных и нормативных правил, контроля за действия сотрудников, выработка системы поощрений и наказаний.

Рекомендации к политике безопасности верхнего уровня

- Британский стандарт BS 7799:1995 рекомендует следующие разделы в документ, характеризующий политику безопасности:
  - вводный, подтверждающий озабоченность руководства проблемами ИБ;
  - организационный, содержащий описание подразделений, ответственных за ИБ;
  - классификационный, описывающий имеющиеся ресурсы и уровень требуемый уровень защиты;
  - штатный, характеризующий меры безопасности применительно к персоналу;
  - раздел, относящийся к вопросам физической защиты;
  - раздел, относящийся к управлению компьютерами и сетями;
  - раздел, описывающий правила разграничения доступа к служебной информации;
  - раздел, характеризующий порядок разработки и сопровождения ИС;
  - раздел, описывающий меры, направленные на обеспечение непрерывности в работе;
  - юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

Политика безопасности среднего уровня

- К среднему уровню относят вопросы, относящиеся к отдельным аспектам информационной безопасности. Например, организация доступа сотрудников в сеть Интернет или установка и использование ПО.
- Политика среднего уровня для каждого аспекта должна освещать:
  - описание аспекта;
  - область применения;
  - позиция организации по данному вопросу;
  - роли и обязанности;
  - законопослушность;
  - точки контакта.

Политика безопасности нижнего уровня

- Политика безопасности нижнего уровня относится к работе конкретных информационных сервисов.
- Такая политика включает в себя два аспекта:
  - цели;
  - правила достижения заданных целей.
- Политика безопасности данного уровня быть выражена полно, четко и конкретно. Например, определять сотрудников, имеющих право на работу с конкретной информационной системой и данными.
- Из целей выводятся правила безопасности, описывающие кто, что и при каких условиях может выполнять те или иные процедуры с информационными сервисами.

Административный уровень защиты информации

- После формулирования политики безопасности, составляется **программа обеспечения информационной безопасности**.
- Программа безопасности также структурируется по уровням. В простом случае достаточно двух уровней:
  - верхнего (центрального) – охватывающего всю организацию;
  - нижнего (служебного) – относящегося к отдельным услугам или группам однородных сервисов.

Программа верхнего уровня

- Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. Цели такой программы:
  - Управление рисками (оценка рисков, выбор эффективных решений);
  - Координация деятельности в области информационной безопасности
  - Стратегическое планирование
  - Контроль деятельности в области информационной безопасности.
- Контроль деятельности в области ИБ должен гарантировать, во-первых, что действия организации не противоречат законам, во-вторых, что состояние безопасности в организации соответствует требованиям и реагировать на случаи нарушений.

Программы служебного уровня

- Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов.
- На нижнем уровне осуществляется выбор механизмов защиты, технических и программных средств.
- Ответственность за реализацию программ нижнего уровня обычно несут администраторы соответствующих сервисов.

Синхронизация программы безопасности с жизненным циклом системы

- В жизненном цикле информационного сервиса можно выделить следующие этапы:
  - **инициация**, определяются потребности в новом сервисе, документируется его назначение;
  - **приобретение** (разработка), составляется спецификация, варианты приобретения или разработки, собственно приобретение;
  - **установка** (внедрение), сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию;
  - **эксплуатация**, работа в штатном и регламентном режиме;
  - **утилизация** (выведение из эксплуатации).

Оценка критичности информационного сервиса

- Для обеспечения безопасной работы сервиса в рамках информационной системы на всех этапах жизненного цикла должны быть рассмотрены вопросы:
  - Какая информация предназначена для обслуживания?
  - Какие возможные последствия от реализации угроз ИБ а данном сервисе?
  - Каковы особенности данного сервиса?
  - Каковы характеристики персонала, имеющие отношения к информационной безопасности?
  - Каковы угрозы, по отношению к которым сервисы и информация наиболее уязвимы?
  - Каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?
- Результаты оценки критичности – отправная точка для составления спецификации.