ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

Персональные данные и защита их при обработке в информационных системах персональных данных

Лекция 3. Построение системы защиты персональных данных

ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

Построение системы защиты ПДн

Установление уровня защищенности ПДн

Выбор мер по обеспечению безопасности информации

Проектирование подсистемы защиты информации

Установка и настройка средств защиты информации

Ввод в постоянную эксплуатацию ИСПДн

ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

Структура системы защиты ИСПДн

Подсистемы защиты ИСПДн, реализующие

- Организационные меры
  - Приказы, инструкции, Политики…
  - Модель угроз, Акт, журналы …
- Технические меры
  - идентификация и аутентификация
  - управление доступом
  - ограничение программной среды
  - защита машинных носителей информации
  - регистрация событий безопасности
  - антивирусная защита
  - обнаружение (предотвращение) вторжений
  - обеспечение целостности
  - обеспечение доступности
  - обеспечение конфиденциальности
  - контроль (анализ) защищенности
  - защита среды виртуализации
  - защита технических средств
  - защита информационной системы
  - выявление инцидентов и реагирование на них
  - управление конфигурацией ИС и СЗИ ИСПДн

Организационные меры по обеспечению безопасности информации

1. ***Согласие*** на обработку Пдн (если необходимо).
2. ***Приказ о назначении ответственного*** за организацию обработки Пдн.
3. ***Инструкция ответственному за организацию*** обработки Пдн.
4. ***Политика оператора*** в отношении обработки Пдн, ***Правила обработки*** Пдн, ***Правила рассмотрения запросов*** субъектов ПДн, ***Правила осуществления внутреннего контроля*** соответствия обработки ПДн, ***Типовое обязательство служащего*** осуществляющего обработку Пдн, в случае расторжения государственного или муниципального контракта, ***Типовая форма согласия на обработку Пдн*** служащих государственного или муниципального органа.
5. ***Акт о проведении обучения сотрудников*** по работе с Пдн и (или) Акт об ознакомлении сотрудников с политикой обработки Пдн в организации (или) Журнал инструктажа сотрудников, имеющих доступ к персональным данным.
6. ***Акт установления уровня защищенности*** ПДн.
7. ***Модель угроз***.
8. ***Журнал учета машинных носителей*** Пдн.
9. ***Журнал обращений и запросов*** субъектов Пдн.
10. ***Перечень ИСПДн***.
11. ***Перечень ПДн*** обрабатываемых в государственном или муниципальном органе.
12. ***Перечень ответственных за обезличивание*** Пдн (если производится).
13. ***Перечень служащих***, замещение которых предусматривает осуществление обработки Пдн.
14. ***Порядок доступа*** служащих государственного или муниципального органа в помещение, где обрабатываются ПДн.
15. ***Технологический процесс обработки*** информации.
16. ***Приказ о назначении ответственного за защиту информации***.
17. ***Приказ об определении контролируемой зоны***.
18. ***Рекомендации по нейтрализации*** выявленных ***угроз*** безопасности информации.
19. ***Техническое задание на создание подсистемы защиты*** информации и ***Технический проект***.
20. ***Акт приемки в опытную эксплуатацию СЗИ***.
21. ***Журнал опытной эксплуатации СЗИ***.