«Антивирусный центр»

Информационная Безопасность Офиса

Создание Систем Защиты Персональных Данных

Сергей Золотухин
Антивирусный центр
www.AntiVirusPro.com
project@antiviruspro.com

Часть 1

Для операторов персональных данных

Всего 4 шага…

- **Уведомить** уполномоченный орган о намерении осуществлять обработку персональных данных
- **Разработать** комплект документов, регламентирующих обработку персональных данных в организации
- **Создать** систему защиты персональных данных
- **Аттестовать** или декларировать соответствие требованиям безопасности

Мероприятия по техническому обеспечению безопасности ПДн

- Мероприятия реализуются в рамках подсистем:
  - **управления доступом**
  - **межсетевого экранирования**
  - **регистрации и учета**
  - **обеспечения целостности**
  - **криптографической защиты**
  - **антивирусной защиты**
  - **обнаружения вторжений**
- Должна проводиться сертификация ПО на отсутствие НДВ, а так же периодический анализ защищенности системного и прикладного ПО
- Для систем 1 и 2 классов должны быть реализованы мероприятия по защите от утечки за счет ПЭМИН
- При наличии голосового ввода ПДн должны быть реализованы мероприятия по защите акустической информации
- Для исключения утечки видовой информации – оборудование помещений шторами (жалюзи).

Основные принципы обеспечения безопасности ПДн

- Обеспечение безопасности достигается реализацией совокупности **организационных и технических мер**
- В обязательном порядке подлежат защите **технические и программные средства**, используемые при обработке, и **носители информации**
- Целесообразно максимально использовать **традиционные подходы** к технической защите информации

Последовательность действий

- Организационные мероприятия
- Инвентаризация
- Концепция ИБ
- Модель угроз и модель нарушителя
- Акт классификации
- Проект (описание) системы защиты
- Установка средств защиты согласно проекта
- Инструкции (правовое, организационное, техническое обеспечение)
- Аттестация (проверка защищенности)
- Эксплуатация системы

Организационные мероприятия

- Приказы
- Распоряжения
- Назначение ответственных
- Создание комиссии

Инвентаризация

- Активы
- Перечни данных
- Технологии обработки
- Средства защиты

Модель угроз

К1-К4 для типовых систем

Модель для специальных систем

Проектирование

- Общее описание системы защиты
- Структурная схема
- Технические средства
- Программные средства
- Политики использования
- Настройки

Приведение в соответствие

Закупка аппаратного обеспечение

Закупка программного обеспечения

Модернизация существующих систем

Внедрение новых систем

Заключение договоров на сопровождение

Регламентирующие документы

- Перечни
  - сведений ограниченного доступа
  - лиц допущенных…
  - помещений…
- Регламенты
- Инструкции
- Положения
- Договора с сотрудниками и контрагентами

Оценка соответствия

Обязательная аттестация

Декларирование соответствия

Аттестат
не ОБЕСПЕЧИВАЕТ
а ПОДТВЕРЖДАЕТ
соответствие

Эксплуатация

Соблюдение регламентов

Мониторинг ситуации

Выявление недостатков

Внесение изменений

Повышение защищенности

Часть 2

Оптимизация

Оптимизация стоимости решения

- Объем данных
- Модель угроз
- Схема защиты
- Стоимость средств защиты
- Эксплуатация
- Сопровождение

Критерии оптимизации

Малые Риски ⇒ **Большие Затраты**

Малые Затраты ⇒ **Большие Риски**

Риски ⇔ Затраты ⇔ Сроки

Проектный подход

1. Цели и задачи
2. Пути реализации
3. Результаты
4. Сроки
5. Бюджеты

Деление на этапы:

Этап 0: Анкета

Этап 1: Подготовительный

Этап 2: Создание системы

Этап 3: Оценка соответствия

Этап 1. Подготовительный

Цели:

- Предварительная модель угроз, класс
- Выбор оптимального варианта
- Понимание «цены вопроса»

Результаты:

- Концепция системы защиты
- Определение бюджета

Документы:

- Техническое задание
- Договор на создание системы

Этап 2. Создание системы

Цели:

Зависят от предыдущего этапа

Результаты:

В зависимости от задач

Документы:

В зависимости от результатов

Выбор оптимального варианта

- Защищаем «как есть»
- Перестраиваем
- Модернизируем
- Принимаем оргмеры
- Ничего не делаем

Риски ⇔ Затраты ⇔ Сроки

Оптимальное проектирование

- Традиционные подходы
- Баланс организационных и технических мер
- Баланс аппаратных и программных средств
- Типовые решения

Проектная команда

- Единое понимание целей и задач
- Совместная работа (Единая команда)
- Ориентация на конкретный результат
- Управление проектом
- Поддержка на всех стадиях проекта

Оптимальное внедрение

- Закупка программного обеспечения
- Закупка аппаратного обеспечение
- Модернизация существующих систем
- Внедрение новых систем

Часть 3

Для операторов персональных данных
и операторов НЕ персональных данных

Защита НЕ персональных данных

Общая концепция защиты
Защита от внешних угроз
Защита от внутренних угроз
Compliance (соответствие требованиям)
Disaster Recovery

Информационная система должна работать на вас!

IT-Решения vs Защита ПДн

- Антивирусная защита
- Антиспам
- URL-фильтрация
- IDS/IPS
- Firewall
- Разграничение доступа
- NAC
- Утечки информации
- Резервное копирование
- Лицензионное ПО
- Управление рисками
- Техническая поддержка и сопровождение
- SOC
- Виртуализация

- Антивирусная защита
- Обнаружение вторжений
- Межсетевое экранирование
- Управление доступом
- Регистрация и учет
- Обеспечение целостности
- Криптографическая защита
- Периодический анализ защищенности системного и прикладного ПО
- сертификация ПО на отсутствие НДВ
- мероприятия по защите от утечки за счет ПЭМИН
- защита акустической информации
- защита видовой информации

А много ли различий?

Два проекта по цене одного ☺

Выводы

Планируйте действия

Обрабатывайте риски

Оптимизируйте процессы

Готовьте бюджеты

Обращайтесь!

На следующий день…

1. Постараться вспомнить ВСЁ
2. Связаться с организатором
3. Заявить готовность работать
4. Заполнить анкету
5. Узнать результаты
6. Согласовать Цели, Сроки, Бюджеты:
7. Заключить договор
8. Стать оператором соответствующим 152-ФЗ

Спасибо за внимание!

Опыт построения системы защиты информации

Александр Витальевич
Отделение ПФР по РК

IT-Решения vs Защита ПДн

- Антивирусная защита
- Антиспам
- URL-фильтрация
- IDS/IPS
- Firewall
- Разграничение доступа
- NAC
- Утечки информации
- Резервное копирование
- Лицензионное ПО
- Управление рисками
- Техническая поддержка и сопровождение
- SOC
- Виртуализация

- Антивирусная защита
- Обнаружение вторжений
- Межсетевое экранирование
- Управление доступом
- Регистрация и учет
- Обеспечение целостности
- Криптографическая защита
- Периодический анализ защищенности системного и прикладного ПО
- сертификация ПО на отсутствие НДВ
- мероприятия по защите от утечки за счет ПЭМИН
- защита акустической информации
- защита видовой информации

А много ли различий?

Вопросы?