Конференция "152 ФЗ – основные ловушки и способы разминирования".

Обобщенный опыт для тех у кого «конь не валялся» и нет лишних миллионов на консультантов…

Татьяна Плотникова. Член совета клуба 4CIO

Каковы требования регуляторов?

- Учредительные документы
- Организационно - распорядительные документы
- Специальные документы в соответствии с требованиями закона и регуляторов

С чего начать ?

- Инициировать назначение **ответственного лица и/или ответственного подразделения** !
- Создать и утвердить приказом рабочую группу, в которую необходимо включить представителей всех подразделений, участвующих в обработке персональных данных, а также юристов и специалистов по безопасности.

…

- Поинтересоваться тем, что уже сделано в этой области коллегами до вас.

Создание карты персональных данных

Задача данного этапа – **получить полное понимание того, Где? Как? и Какие? персональные данные обрабатываются, Откуда оператор получает персональные данные? и Куда передает?**

Описывайте в карте обработку максимально подробно. На основе полученных данных вы будете проводить все последующие работы и, естественно, параллельно вносить изменения в карту.
Карта персональных данных – это ваш внутренний пакет документов и в первую очередь **он должен быть понятным**, поэтому подобную карту можно составлять в виде перечней, таблиц, а для наглядности можно использовать схемы, графики и т.д.

Сокращение перечня сведений составляющих персональные данные

Прежде чем защищать какие-то сведения, составляющие персональные данные, нужно выяснить, а нужно ли их вообще обрабатывать?

Объем обрабатываемых сведений должен соответствовать целям обработки!

Проверить (через юристов) правовые основания на обработку некоторых сведений

Уменьшить количество обрабатываемых сведений, а, следовательно, и требования по защите ОЧЕНЬ реально.

Необходимо помнить : чем меньше сведений оператор обрабатывает, тем ниже класс системы и соответственно ниже требования по защите.

Обезличивание персональных данных

Федеральный закон о персональных данных дал определение обезличиванию (как процессу):

обезличивание персональных данных *– действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных*

1) Право на обезличивание персональных данных у оператора есть по федеральному закону.

2) Требований к «правильному» обезличиванию не существует.

3) Способы и алгоритмы обезличивания персональных данных ***оператор****, осуществляющий обработку персональных данных,* ***определяет самостоятельно***

Написание основных документов

1. Модели угроз безопасности персональных данных для каждой ИСПДн;
2. Акты классификации ИСПДн;
3. Положение о защите персональных данных;
4. Положение о назначении подразделения по защите персональных данных;
5. Должностные регламенты лиц, ответственных за защиту персональных данных;
6. Схема организации ИСПДн;
7. Копия договора об оказании услуг (если есть);
8. Копия трудового договора с сотрудниками;
9. Письменное согласие субъектов персональных данных;
10. Приказ с перечнем лиц, допущенных к обработке персональных данных;
11. Документы учета обращений граждан (субъектов персональных данных) о выполнении их законных прав;
12. Приказ о назначении лиц, ответственных за ведение и периодическую проверку содержания журнала обращений;
13. Приказ о ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска на территорию;
14. Копия уведомления об обработке персональных данных (если уведомление до проверки не будет подано, то это 100%-е нарушение статьи 19.7 КоАП РФ Непредставление сведений…).

Начнем с модели угроз…

- Модель угроз - это документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности ПДн и уязвимостей при их обработке в ИС ПДн, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ПДн.
  Цель разработки модели угроз – определение актуальных для конкретной ИС ПДн угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться для классификации ИС ПДн, а также в качестве исходных данных для построения (проектирования) обоснованной и эффективной системы защиты персональных данных.

Откуда ждать помощи ???

НТЦ «Сфера» http://www.ntc-sfera.ru/products/

А чем именно??

Программный комплекс WingDoc ПД

. Программа имеет модульную архитектуру. В состав программы входят следующие модули:

Модуль «Модель угроз ИСПДн»

Модуль «Модель угроз ИСПДн-К»

программа выдает документ «Модель угроз», в который попадают введенные, обработанные данные, списки угроз.

Модуль «Документы»

Подводные камни автоматизированной системы…

Внимание! Заполнение сведений для модели угроз задача не тривиальная. Перед тем как приступить убедитесь в наличии исходной информации и проведите инвентаризацию ресурсов.

Модель угроз сформированная системой может быть избыточной (оптимальности никто не обещал!), а поэтому убедитесь в применимости лично для вашей организации сделанных системой выводов и при необходимости скорректируйте документ.

Заключение

Удачи Вам в нелегком труде и плодотворной работы на сегодняшней конференции!

Помните жизненный принцип воинов-самураев, «Делай, что должен - и будь, что будет».

Спасибо за внимание!

Выражаю благодарность виртуальным коллегам Алексею Лукацкому и Евгению Цареву , чьи посты были использованы мной частично, за проделанный труд.

Рекомендуемые ресурсы…

Портал персональных данных http://pd.rsoc.ru/
Компания Элвис- плюс http://www.elvis.ru/anticry_ext.shtml
Ответы на вопросы по ПДн http://www.elvis.ru/anticry_FAQ.shtml
Всё об информационных системах персональных данных http://ispdn.ru/

Блоги:

Алексей Лукацкий: Бизнес без опасности http://lukatsky.blogspot.com/
Царев Евгений: Персональные данные по русски http://pers-data.livejournal.com/
http://www.tsarev.biz/
Хайров Игорь: Безопасность, как бизнес http://hayrov.blogspot.com/
http://toparenko.livejournal.com/