Безопасность персональных данных по законодательству России

Блок 6.1.

6.1.1. Обязанность обеспечить безопасность по Федеральному закону «О персональных данных»

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. К таким мерам относятся:

- Определение угроз безопасности персональных данных;
- Выполнение требований к защите персональных данных, обеспечивающих установленные Правительством Российской Федерации уровни защищенности персональных данных;
- Применение сертифицированных средств защиты информации;
- Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- Обнаружение фактов несанкционированного доступа к персональным данным;
- Установление правил доступа к персональным данным, учёт всех действий с данными;
- Контроль за мерами по обеспечению безопасности персональных данных

6.1.2. Уровни защищенности персональных данных

Правительство РФ с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Состав и содержание мер, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности устанавливаются ФСБ и ФСТЭК

Безопасность персональных данных
Тема 6

Лучшие мировые практики в сфере безопасности персональных данных

Блок 6.2.

6.2.1. Подход GDPR

- **Управление данными** - политика конфиденциальности, планы управления данными и реагирования на инциденты; авторизация доступа, контроль доступа на основе ролей сотрудников.

- **Классификация, шифрование и псевдонимизация данных** – надо знать, где хранятся конфиденциальные данные и шифровать их в базах и хранилищах, а также при передаче.

- **Непрерывный мониторинг** - способность своевременно восстанавливать доступ к данным в случае физического или технического инцидента; предотвращение потери данных; уведомления о нарушении, обнаружение необычных способов доступа.

- **Метаданные** - установка ограничения на срок хранения данных и регулярный анализ необходимости архивирования

6.2.2. Privacy by design (встроенная приватность)

1. Предотвращение вреда, а не реагирование на вред
2. Приватность как настройка «по умолчанию»
3. Приватность как часть устройства информационных систем
4. Сочетание интересов приватности с бизнес-интересами (win-win)
5. Защита информации от самого начала до самого конца её обработки
6. Открытость документации и транспарентность обработки
7. Интересы пользователя как основа архитектуры информационных систем и бизнес-процессов

6.2.3. Наиболее распространенные угрозы безопасности данных

- уязвимые и вредоносные приложения и программы;
- использование неавторизованных устройств и программного обеспечения;
- инсайдеры и плохо обученные сотрудники;
- отсутствие плана действий в случае нарушения безопасности;
- неадекватное удаление персональных данных;
- отсутствие прозрачности в политиках, условиях и условиях конфиденциальности;
- сбор ненужных данных;
- обмен данными и передача по незащищенным каналам;
- неверные или устаревшие личные данные;
- физическая кража устройств с данными (ноутбуков, телефонов)

6.2.4. Меры по обеспечению безопасности

- первоначальная и регулярная оценка рисков обработки;
- разработка политики конфиденциальности и внутренних актов, регулирующих доступ и обработку данных;
- документирование всех процессов обработки данных и применяемых мер безопасности;
- регулярное тестирования целостности и безопасности данных;
- обезличивание, шифрование и псевдонимизация данных;
- обеспечение конфиденциальности данных путем включения условий об этом в договоры, с контролем сотрудников, которые занимаются обработкой данных;
- повышение осведомленности сотрудников о защите данных и предоставление инструкций;
- назначение лиц, ответственных за обеспечение безопасности данных;
- ведение автоматического электронного журнала (лога), фиксирующего все операции и автоматической системы выявления и пресечения несанкционированного доступа, уничтожения или изменения;
- регулярный аудит информационных систем

Задания для самостоятельной работы по Теме 6

- Федеральный закон «О персональных данных» (статья 19)
- Требования к защите персональных данных при их обработке в информационных системах персональных данных
  (утв. постановлением Правительства РФ от 1 ноября 2012 г. № 1119)
- Конвенция Совета Европы (статья 10)
- GDPR (статьи 24, 25, 32)
- Принципы Privacy by Design https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf