КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Методология определения класса ИСПДн

ЭТАПЫ ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ

СБОР И АНАЛИЗ ИСХОДНЫХ ДАННЫХ ПО ИНФОРМАЦИОННОЙ СИСТЕМЕ;

ПРИСВОЕНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЕ СООТВЕТСТВУЮЩЕГО КЛАССА И ДОКУМЕНТАЛЬНОЕ ЕГО ОФОРМЛЕНИЕ.

ИСХОДНЫЕ ДАННЫЕ

- КАТЕГОРИЯ ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ДАННЫХ - $X_{ПД}$;
- ОБЪЁМ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ (КОЛИЧЕСТВО СУБЪЕКТОВ $ПД_н$, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ – $X_{НПД}$;
- ЗАДАНИЕ ОПЕРАТОРОМ ХАРАКТЕРИСТИКИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ;
- СТРУКТУРА ИНФОРМАЦИОННОЙ СИСТЕМЫ;
- НАЛИЧИЕ ПОДКЛЮЧЕНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ К СЕТЯМ ОБЩЕГО ПОЛЬЗОВАНИЯ И (ИЛИ) СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА;
- РЕЖИМ ОБРАБОТКИ $ПД_н$;
- РЕЖИМ РАЗГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ;
- МЕСТОНАХОЖДЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ $ИСПД_н$.

КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

КАТЕГОРИЯ 1 - ПЕРСОНАЛЬНЫЕ ДАННЫЕ, КАСАЮЩИЕСЯ РАСОВОЙ, НАЦИОНАЛЬНОЙ ПРИНАДЛЕЖНОСТИ, ПОЛИТИЧЕСКИХ ВЗГЛЯДОВ, РЕЛИГИОЗНЫХ И ФИЛОСОФСКИХ УБЕЖДЕНИЙ, СОСТОЯНИЯ ЗДОРОВЬЯ, ИНТИМНОЙ ЖИЗНИ.

КАТЕГОРИЯ 2 - ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОЗВОЛЯЮЩИЕ ИДЕНТИФИЦИРОВАТЬ СУБЪЕКТА ПДн И ПОЛУЧИТЬ О НЁМ ДОПОЛНИТЕЛЬНУЮ ИНФОРМАЦИЮ, ЗА ИСКЛЮЧЕНИЕМ ПДн, ОТНОСЯЩИХСЯ К КАТЕГОРИИ 1.

КАТЕГОРИЯ 3 - ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОЗВОЛЯЮЩИЕ ИДЕНТИФИЦИРОВАТЬ СУБЪЕКТА ПДн.

КАТЕГОРИЯ 4 – ОБЕЗЛИЧЕННЫЕ И (ИЛИ) ОБЩЕДОСТУПНЫЕ ПДн.

КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Законодательство определяет различные категории персональных данных: общедоступные, специальные категории ПДн, категории ПДн, обрабатываемые в информационных системах ПДн, биометрические ПДн и другие.

ОБЩЕДОСТУПНЫЕ ПДн

Данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или которые в соответствии федеральными законами не распространяются требования соблюдения конфиденциальности (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются справочники, адресные книги и т.п.). Такие сведения могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

К специальным категориям относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

- **субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;**
- **персональные данные являются общедоступными;**
- **персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;**
- **обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПДн;**
- **обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.**

КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Биометрические персональные данные

(аутентификация, опирающаяся на уникальные биологические показатели человека. К основным биометрическим идентификаторам относятся отпечатки пальцев, рукописные подписи, образцы голоса, результаты сканирования сетчатки и радужной оболочки глаза, формы ладони или черт лица)

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн.Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Исходя из определения биометрических ПДн, к ним относятся фотографии и видеоизображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения – в системах видеонаблюдения и т.п.

ОБЪЁМ ПДн (значение Хнпд)

1 - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

ТИПЫ ИНФОРМАЦИОННЫХ СИСТЕМ

информационные системы подразделяются на типовые и специальные информационные системы

Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.

Специальные информационные системы - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:

информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

СТРУКТУРА ИНФОРМАЦИОННЫХ СИСТЕМ

По структуре информационные системы подразделяются

на автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки персональных данных (автоматизированные рабочие места);

на комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

на комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

ДРУГИЕ ИСХОДНЫЕ ДАННЫЕ

ПО НАЛИЧИЮ ПОДКЛЮЧЕНИЯ ПОДРАЗДЕЛЯЮТСЯ НА:

- **ИМЕЮЩИЕ ПОДКЛЮЧЕНИЯ**
- **НЕ ИМЕЮЩИЕ ПОДКЛЮЧЕНИЯ**

ПО РЕЖИМУ ОБРАБОТКИ ПОДРАЗДЕЛЯЮТСЯ НА:

- **ОДНОПОЛЬЗОВАТЕЛЬСКИЕ**
- **МНОГОПОЛЬЗОВАТЕЛЬСКИЕ**

ПО РАЗГРАНИЧЕНИЮ ПРАВ ДОСТУПА ПОДРАЗДЕЛЯЮТСЯ НА:

БЕЗ РАГРАНИЧЕНИЯ ПРАВ ДОСТУПА
С РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА

В ЗАВИСИМОСТИ ОТ МЕСТОНАХОЖДЕНИЯ ПОДРАЗДЕЛЯЮТСЯ НА:

все технические средства которых находятся в пределах Российской Федерации

системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

КЛАССЫ ИНФОРМАЦИОННЫХ СИСТЕМ

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

ТАБЛИЦА ДЛЯ ОПРЕДЕЛЕНИЯ КЛАССА

Х пд\Хнпд	3	2	1
Категория 4	к4	к4	к4
Категория 3	к3	к3	к2
Категория 2	к3	к2	к1
Категория 1	к1	к1	к1

ТАБЛИЦА-ПОДСКАЗКА

	менее 1000 чел.	от 1000 до 100000	более 100000
Обезличенные ПДн	к4	к4	к4
ФИО, адрес, дата рождения	к3	к3	к2
Образование, финансы	к3	к2	к1
Здоровье, любовь, вероисповедание	к1	к1	к1

ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП РАБОТЫ

По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

Результаты классификации информационных систем оформляются соответствующим актом оператора.

Класс информационной системы может быть пересмотрен:

- **по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;**
- **по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.**