**Лекция 6: Классификация ИСПД**

**Цель лекции**: рассмотреть критерии, на основании которых производится классификация ИСПД и цели классификации.

На начальном этапе построения СЗПД определяется *класс* для каждой ИСПД в конкретной организации. От класса ИСПД зависит, какие требования *по* обеспечению безопасности должны выполняться для заданной ИСПД, следовательно, выбор мер, способов защиты и их *стоимость*. Классификация ИСПД проводится в соответствии с Приказом.

Классификация ИСПД проводится на этапе ее создания или в ходе эксплуатации, но обязательно до построения СЗПД. В общем случае все *информационные системы*, обрабатывающие *персональные данные*, подразделяются на 2 *класса в зависимости* от характеристик безопасности обрабатываемых данных:

**Типовые информационные системы** – системы, где требуется обеспечить только *конфиденциальность* обрабатываемых персональных данных.

**Специальные информационные системы** – системы, где требуется обеспечить хотя бы одну из характеристик безопасности, отличную от конфиденциальности (например, *целостность* или доступность). К специальным информационным системам должны быть отнесены:

1. ИСПД, связанные с обработкой ПД о состоянии здоровья субъектов ПД;
2. ИСПД, принимающие решения на основании исключительно автоматизированной обработки ПД. При этом принятые решения могут повлечь за собой юридические последствия для субъекта ПД или иным способом затронуть его законные права и интересы.

Согласно предлагаемой в Приказе методике ИСПД классифицируется в зависимости от количества субъектов, чьи данные обрабатываются, и типа обрабатываемых персональных данных.

В зависимости от объема обрабатываемых в ИСПД данных XНПД выделяют следующие категории ИСПД:

**1 категория** – в информационной системе одновременно обрабатываются *персональные данные* **более чем 100 000** субъектов ПД или *персональные данные* субъектов ПД в пределах субъекта Республики Казахстан;

**2 категория** – в информационной системе одновременно обрабатываются *персональные данные* **от 1000 до 100 000**субъектов ПД или *персональные данные* субъектов ПД, работающих в отрасли экономики Республики Казахстан, в органе государственной власти, проживающих в пределах муниципального образования;

**3 категория** – в информационной системе одновременно обрабатываются *персональные данные* **менее чем 1000** субъектов ПД или *персональные данные* субъектов ПД в пределах конкретной организации.

Таким образом, данная категория ИСПД определяется на основании количества субъектов ПД, чьи данные обрабатываются в системе.

Определяются следующие категории обрабатываемых в информационной системе персональных данных (ХПД):

**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 персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

**категория 3** – *персональные данные*, позволяющие идентифицировать субъекта персональных данных;

**категория 4** – обезличенные и (или) общедоступные *персональные данные*.

*По* результатам анализа вышеперечисленных данных определяется *класс* ИСПД в соответствии с [таблицей 6.1](https://www.intuit.ru/studies/courses/697/553/lecture/12450?page=1" \l "table.6.1).

|  |  |  |  |
| --- | --- | --- | --- |
| Таблица 6.1. Определение класса информационной системы | | | |
| **ХНПД** | **Категория 3** | **Категория 2** | **Категория 1** |
| **ХПД** |  | | |
| категория 4 | К4 | К4 | К4 |
| категория 3 | К3 | К3 | К2 |
| категория 2 | К3 | К2 | К1 |
| категория 1 | К1 | К1 | К1 |

Рассмотрим, что значит каждый *класс* ИСПД в отдельности:

* **класс 1 (К1)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПД;
* **класс 2 (К2)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;
* **класс 3 (К3)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПД;
* **класс 4 (К4)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.

Наивысшим считается *класс* 1. Если в составе ИСПД выделяют несколько подсистем, то *класс* ИСПД в целом будет соответствовать наиболее высокому классу входящих компонентов.

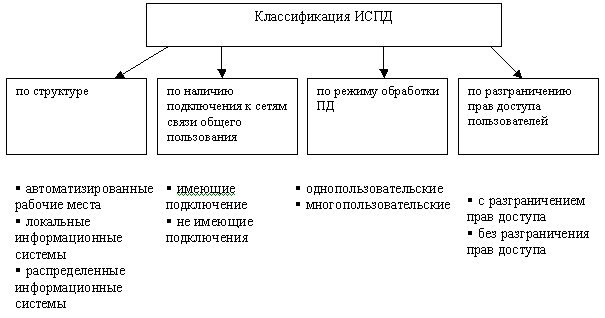
Таким образом, чем выше *класс* ИСПД, тем выше требования *по* обеспечению безопасности персональных данных.

Порядок определения класса для специальных систем несколько отличается от типовых. *Класс* специальных ИСПД определяется на основе частной модели угроз организации в соответствии с методическими документами ФСТЭК. Отнесение информационной системы к специальной позволяет существенно снизить *затраты* на построение СЗПД, так как оператор в данном случае может обоснованно выбрать минимальное количество актуальных угроз, от которых необходима защита ПД. Например, если в системе есть сведения о доходах человека (например, 1С), такая система может быть отнесена к специальной, так как затрагиваются законные интересы человека. То же самое относится к информации об инвалидности, расовой принадлежности и пр. Отнесение ИСПД к специальной на практике является достаточно спорным моментом.

*Класс* ИСПД может быть пересмотрен:

* по решению оператора после проведения анализа и оценки угроз безопасности с учетом особенностей или (и) изменений информационной системы;
* по результатам испытаний по контролю за выполнением требований по обработке ПД.

ИСПД также классифицируются *по* структуре, *по* наличию подключений к сетям общего пользования, *по* режиму обработки ПД, *по* разграничению прав доступа. Приведенные классификации отображены схематически на [рисунке 6.1](https://www.intuit.ru/studies/courses/697/553/lecture/12450?page=1" \l "image.6.1).



**Рис. 6.1.**

Классификация ИСПД - не формальная процедура, так как на основании класса системы будут определяться меры и способы *защиты персональных данных*, существенно отличающиеся друг от друга. Более того, для 1 и 2 класса систем обязательно *лицензирование* используемых технических средств защиты, а сами ИСПД должны быть аттестованы. Результат классификации оформляется соответствующим актом оператора.

При классификации информационных систем на практике выявляется множество факторов, впоследствии влияющих на построение СЗПД. Например, если в информационной системе помимо стандартных данных о сотрудниках, таких как ФИО, *адрес* и телефон, хранятся фотографии, значит, система обрабатывает биометрические ПД. А если наряду со стандартной информацией обрабатывается дата рождения, можно сказать, что ИСПД содержит дополнительную информацию о субъекте и отнести ее не к классу 3, а к классу 2.

При внимательном анализе на предпроектном этапе построения СЗПД, можно оптимизировать некоторые моменты обработки ПД. Так, например, если в системе учета кадров вместо ФИО использовать табельный номер работника, речь будет идти об обработке обезличенных персональных данных, требования к безопасности которых минимальны. *Оптимизация* представления данных в системе может повлиять на проектирование СЗПД и существенно сократить *затраты* в конечном итоге.

### Вопросы для закрепления:

1. Какова цель классификации информационных систем персональных данных (ИСПД)?
2. На каком этапе определяется класс ИСПД в организации?
3. В чем заключается основное отличие типовых и специальных информационных систем персональных данных?
4. Какие два критерия лежат в основе классификации ИСПД?
5. Какие категории выделяются по количеству субъектов персональных данных (ХНПД)?
6. Какие категории выделяются по типу обрабатываемых персональных данных (ХПД)?
7. Что означает класс ИСПД К1? Какие последствия возможны при нарушении безопасности в системах этого класса?
8. Чем отличается класс К2 от классов К1 и К3?
9. Какие данные относятся к категории 1 по ХПД?
10. В какой ситуации ИСПД может быть отнесена к специальной?
11. Как влияет определение класса ИСПД на выбор мер и средств защиты персональных данных?
12. Как определяется итоговый класс ИСПД, если система состоит из нескольких подсистем?
13. Может ли класс ИСПД быть изменен после его первоначального установления? В каких случаях?
14. Почему классификация ИСПД считается неформальной процедурой?
15. Как можно снизить затраты на построение системы защиты персональных данных за счёт классификации?