**КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Согласно Письму Федерального агентства по образованию от 28.04.2008 г. № ФАО-6748/52/17-02-09/72 «Об обеспечении безопасности персональных данных» руководители образовательных учреждений должны провести классификацию  информационных систем, обрабатывающих персональные данные на бумажном и электронном носителях согласно «Порядку проведения классификации информационных систем персональных данных» (совместный Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности РФ (ФСБ России), Министерства информационных технологий и связи РФ (Мининформсвязи России) от 13.02. 2008 г. № 55/86/20).

Согласно этому порядку все ***информационные системы подразделяются на 4 класса***в зависимости от объема и категории обрабатываемых персональных данных:

|  |  |  |  |
| --- | --- | --- | --- |
| **Х нпд (объем****данных)****Х пд****(категория****данных)** | **3**(данные до 1000 субъектов или субъектов одной организации) | **2**(данные от 1000 до 1000000 субъектов или субъектов отрасли в пределах муниципального района) | **1**(данные более 100000 субъектов или субъектов региона) |
| **Категория 4**(обезличенные и (или) общедоступные персональные данные) | **Класс 4 (К4)**(нарушение, заданной характеристики  безопасности персональных данных не приводит к негативным последствиям для субъектов персональных данных) | **Класс 4 (К4)**(нарушение, заданной характеристики  безопасности персональных данных не приводит к негативным последствиям для субъектов персональных данных) | **Класс 4 (К4)**(нарушение, заданной характеристики  безопасности персональных данных не приводит к негативным последствиям для субъектов персональных данных) |
| **Категория 3**(персональные данные позволяющие идентифицировать субъекта данных) | **Класс 3 (К3)**(нарушение, заданной характеристики  безопасности персональных данных может привести к незначительным негативным последствиям для субъектов персональных данных) | **Класс 3 (К3)**(нарушение, заданной характеристики  безопасности персональных данных может привести к незначительным негативным последствиям для субъектов персональных данных) | **Класс 2 (К2)**(нарушение, заданной характеристики  безопасности персональных данных может привести к негативным последствиям для субъектов ) персональных данных |
| **Категория 2**(персональные данные позволяющие идентифицировать субъекта данных и получить о нем дополнительную информацию, за исключением данных **категории 1**) | **Класс 3 (К3)**(нарушение, заданной характеристики  безопасности персональных данных может привести к незначительным негативным последствиям для субъектов персональных данных ) | **Класс 2 (К2)**(нарушение, заданной характеристики  безопасности персональных данных может привести к негативным последствиям для субъектов персональных данных) | **Класс 1 (К1)**(нарушение, заданной характеристики  безопасности персональных данных может привести к значительным негативным последствиям для субъектов ) персональных данных |
| **Категория 1**(персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни) | **Класс 1 (К1)**(нарушение, заданной характеристики  безопасности персональных данных может привести к значительным негативным последствиям для субъектов персональных данных) | **Класс 1 (К1)**(нарушение, заданной характеристики  безопасности персональных данных может привести к значительным негативным последствиям для субъектов персональных данных ) | **Класс 1 (К1)**(нарушение, заданной характеристики  безопасности персональных данных может привести к значительным негативным последствиям для субъектов персональных данных) |

Исходя из приведенных критериев, информационные системы персональных данных, используемые в образовательных учреждениях, лишь в редких случаях могут быть отнесены к **Классу 3** (**К3**) (в случае, если общее количество субъектов персональных данных (учащихся, их законных представителей и работников образовательного учреждения) не превышает 1000 и персональные данные не содержат информацию о состоянии здоровья, национальной принадлежности и иной информации **Категории 1.**

В большинстве же случаев информационные системы персональных данных, используемые в образовательных учреждениях, должны быть отнесены к **Классу 2** (**К2**), так как общее количество субъектов персональных данных превышает 1000, или даже **Классу 1** (**К1**), так как персональные данные содержат как минимум информацию о состоянии здоровья или иную информацию, отнесенную к **Категории 1**.

***Примечания:***

После проведения классификации информационных систем необходимо заполнить типовую форму перечня информационных систем и направить ее по адресу: ispd@ministry.ru(Приложение 2 к Письму Федерального агентства по образованию от 28.04.2008 г. № ФАО-6748/52/17-02-09/72 «Об обеспечении безопасности персональных данных»).

После этого «нормативно-методические документы ФСТЭК России для уточнения классификации и проведения предусмотренных мероприятий по обеспечению информационной безопасности ***будут дополнительно переданы представителям образовательных учреждений, сообщивших о наличии указанных систем»*** (Письмо Федерального агентства по образованию от 28.04.2008 г. № ФАО-6748/52/17-02-09/72 «Об обеспечении безопасности персональных данных»).

Здесь не лишне будет напомнить, что:

* нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) – влечет предупреждение или наложение административного штрафа на должностных лиц в размере от пятисот до одной тысячи рублей (ст. 13.11. Кодекса РФ об административных правонарушениях);
* использование несертифицированных информационных систем и средств защиты информации, если они подлежат обязательной сертификации – влечет наложение на должностных лиц административного штрафа в размере от одной до двух тысяч рублей (ст. 13.12. Кодекса РФ об административных правонарушениях);
* неправомерный доступ к охраняемой законом компьютерной информации, повлекший уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети наказывается (ст. 272, ч. 2 Уголовного кодекса РФ):

- штрафом в размере от ста до трехсот тысяч рублей или в размере заработной платы или иного дохода за период от одного года до двух лет,

- исправительными работами на срок от одного года до двух лет,

- арестом на срок от трех до шести месяцев,

- лишением свободы на срок до пяти лет.