

**Приказ Федеральной службы по техническому и
экспортному контролю, Федеральной службы
безопасности Российской Федерации, Министерства
информационных технологий и связи
Российской Федерации
от 13.02.2008 № 55/86/20
«Об утверждении Порядка проведения классификации
информационных систем персональных данных»**

В соответствии с пунктом 6 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2007, № 48, часть II, ст.6001),

приказываем:

Утвердить прилагаемый Порядок проведения классификации информационных систем персональных данных.

Директор Федеральной службы
по техническому и экспортному контролю

С.Григоров

Директор Федеральной службы
безопасности Российской Федерации

Н.Патрушев

Министр информационных технологий
и связи Российской Федерации

Л.Рейман

Зарегистрировано в Министерстве юстиции
Российской Федерации 3 апреля 2008 года,
регистрационный № 11462

УТВЕРЖДЕН
приказом ФСТЭК России,
ФСБ России,
Мининформсвязи России
от 13.02.2008 № 55/86/20

Порядок проведения классификации информационных систем персональных данных

1. Настоящий Порядок определяет проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее — информационные системы).

2. Классификация информационных систем проводится государственными органами, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее — оператор).

3. Классификация информационных систем проводится на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

4. Проведение классификации информационных систем включает в себя следующие этапы:

— сбор и анализ исходных данных по информационной системе;

— присвоение информационной системе соответствующего класса и его документальное оформление.

5. При проведении классификации информационной системы учитываются следующие исходные данные:

— категория обрабатываемых в информационной системе персональных данных — $X_{пд}$;

— объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе) — $X_{нпд}$;

- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

6. Определяются следующие категории обрабатываемых в информационной системе персональных данных ($X_{пд}$):

- 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.

7. $X_{нпд}$ может принимать следующие значения:

- 1 — в информационной системе одновременно обрабатываются персональные данные более чем 100000 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 100000 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.

8. По заданным оператором характеристикам безопасности персональных данных, обрабатываемых в информационной системе, 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.

9. 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).

10. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений.

11. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на однопользовательские и многопользовательские.

12. По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

13. Информационные системы в зависимости от местонахождения их технических средств подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

14. 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.

15. Класс типовой информационной системы определяется в соответствии с таблицей.

$X_{пд} \setminus X_{нпд}$	3	2	1
категория 4	K4	K4	K4
категория 3	K3	K3	K2
категория 2	K3	K2	K1
категория 1	K1	K1	K1

16. 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 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

17. 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.

18. Результаты классификации информационных систем оформляются соответствующим актом оператора.

19. 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.