



ПРАВИТЕЛЬСТВО АРХАНГЕЛЬСКОЙ ОБЛАСТИ

**МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
И СОЦИАЛЬНОГО РАЗВИТИЯ
АРХАНГЕЛЬСКОЙ ОБЛАСТИ**

РАСПОРЯЖЕНИЕ

06.09.2010

№ 715-рд

г. Архангельск

О мониторинге реализации
положений Федерального закона
от 27 июля 2006 года №152-ФЗ
«О защите персональных данных»

В целях организации работ по реализации положений Федерального закона от 27 июля 2006 года №152-ФЗ «О защите персональных данных»:

1. Утвердить прилагаемую форму мониторинга «Обеспечение защиты персональных данных в учреждении».
2. Руководителям учреждений системы здравоохранения и социальной защиты населения Архангельской области назначить лиц ответственных за обеспечение информационной безопасности из числа сотрудников учреждения.
3. Руководителям **учреждений системы здравоохранения** Архангельской области обеспечить представление данных мониторинга в соответствии с утвержденной формой в отдел сетевых технологий и защиты информации государственного учреждения здравоохранения «Медицинский информационно-аналитический центр» **не позднее 1 и 15 числа каждого месяца по электронной почте на адрес ozl@msa.ru**.
4. Руководителям **учреждений системы социальной защиты населения** Архангельской области обеспечить представление данных мониторинга в соответствии с утвержденной формой в отдел организационной и информационной работы управления организационной, правовой и кадровой работы министерства здравоохранения и социального развития Архангельской области **не позднее 1 и 15 числа каждого месяца по электронной почте на адрес sergey@uszn.atknet.ru**.
5. Директору государственного учреждения здравоохранения «Медицинский информационно-аналитический центр» Клещинову Н.М.:
 - 5.1. обеспечить сбор представленных учреждениями системы здравоохранения Архангельской области мониторингов;
 - 5.2. проводить анализ ситуации в области защиты персональных данных в учреждениях системы здравоохранения Архангельской области;

5.3. обеспечить проведение разъяснительной работы с руководителями учреждений системы здравоохранения Архангельской области по вопросам организации работ по реализации положений Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

6. Ведущему консультанту отдела организационной и информационной работы управления организационной, правовой и кадровой работы министерства здравоохранения и социального развития Архангельской области Жаринову С.В.:

6.1. обеспечить сбор представленных учреждениями системы социальной защиты населения Архангельской области мониторингов;

6.2. проводить анализ ситуации в области защиты персональных данных в учреждениях системы социальной защиты населения Архангельской области;

6.3. обеспечить проведение разъяснительной работы с руководителями учреждений системы социальной защиты населения Архангельской области по вопросам организации работ по реализации положений Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

7. Контроль за исполнением настоящего распоряжения оставляю за собой.

Министр

Н.А. Макарова

Утверждена
распоряжением министерства здравоохранения
и социального развития Архангельской области
от 06.09.2010 №715-рд

Форма мониторинга «Обеспечение защиты персональных данных в учреждении»

наименование учреждения _____

дата заполнения « _____ » _____ 201__ год

1. Наличие в учреждении перечня конфиденциальной, служебной коммерческой и другой критичной информации, подлежащей защите (Да – 1, Нет – 0)	
2. Наличие в учреждении организационно-распорядительной документации, регламентирующей проведение мероприятий по защите информации:	
2.1. Приказ «Об утверждении перечня ПДн» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.2. Уведомление об обработке (о намерении осуществлять обработку) ПДн (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.3. План мероприятий по обеспечению защиты ПДн учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.4. Приказ «О назначении ответственного за обеспечение информационной безопасности» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.5. Инструкция ответственного за обеспечение безопасности информации (администратора информационной безопасности) (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.6. Приказ «Об утверждении Положения о защите персональных данных» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.7. Приказ «Об утверждении Положения об особенностях обработки персональных данных осуществляемой без использования средств автоматизации» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.8. Приказ «О проведении обследования организации обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.9. Положение об обработке в информационных системах персональных данных (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.10. Образец письменного согласия на обработку ПДн и обязательства о неразглашении информации ограниченного распространения, утвержденного руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.11. Приказ «Об утверждении Порядка проведения классификации информационных систем персональных данных» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.12. Частная модель угроз безопасности информационной системы персональных данных, утвержденная руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.13. Акт классификации информационной системы ПДн (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.14. Какой класс присвоен ИСПДн	
2.15. Приказ «Об информационной безопасности при работе со сведениями конфиденциального характера» (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.16. Перечень лиц, обслуживающих информационную систему, утвержденный руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.17. Проведена ли аттестация по требованиям безопасности информации (для ИСПДн 1 и 2 класса) (если проведена – указывать номер документа и дату принятия, если нет – «не проведена»)	

2.18. Инструкция по обеспечению защиты конфиденциальной информации, обрабатываемой в информационной системе (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.19. Состав программного обеспечения информационной системы, утвержденный руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.20. Перечень лиц, допущенных работать с информационной системой, утвержденный руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.21. Перечень защищаемых ресурсов информационной системы и уровень их конфиденциальности, утвержденный руководителем учреждений (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.22. Матрица доступа субъектов информационной системы, утвержденная руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.23. Акт установки системы технической защиты информации в информационной системе (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.24. Описание настроек системы разграничения доступа системы защиты информации от несанкционированного доступа информационной системы (утвержденного руководителем учреждения) (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.25. Описание технологического процесса обработки информации в информационной системе, утвержденного руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.26. Положение об учете, порядке работы, хранения, уничтожения документов и машиночитаемых носителей, содержащих персональные данные и иную конфиденциальную информацию (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
2.27. Организация охраны и физическая защита ресурсов ИСПДн, утвержденная руководителем учреждения (если есть – указывать номер документа и дату принятия, если нет – «отсутствует»)	
3.Наличие в учреждении политики применения криптографических средств защиты (Да – 1, Нет – 0)	
4.Наличие в учреждении документов, регламентирующих информационный обмен с другими юридическими или физическими лицами (Да – 1, Нет – 0)	
5.Наличие в учреждении защищенных помещений (Да – 1, Нет – 0)	
6.Наличие в учреждении выделенного, недоступного для посторонних, серверного помещения (Да – 1, Нет – 0)	
7.Проведение обучения или повышение их квалификации лиц, ответственных за обеспечение информационной безопасности (Да – 1, Нет – 0)	
8.Подключение ИСПДн к системам общего пользования (интранет, интернет) (Да – 1, Нет – 0)	
9.Использование межсетевых экранов для отделения ИСПДн от остальных сетей (Да – 1, Нет – 0)	
10.Какие средства криптографической защиты используются	
11.Какие средства антивирусной защиты используются	

Ф.И.О. ответственного за заполнение формы _____ тел. _____