ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГБУЗ «ВОЛГОГРАДСКОЕ ОБЛАСТНОЕ БЮРО СУДЕБНО-МЕДИЦИНСКОЙ ЭКСПЕРТИЗЫ»

1. Настоящая политика определяет цели и принципы обеспечения информационной безопасности ГБУЗ «Волгоградское областное бюро судебно-медицинской экспертизы» (далее – Учреждение).

2. Политика обязательна для исполнения всеми сотрудниками, а также лицами, работающими с информацией, принадлежащей Учреждению, в рамках заключенных договоров.

3. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

4. Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности и улучшение деловой репутации Учреждения.

5. В Учреждении обрабатываются следующие категории информации ограниченного доступа (конфиденциальная информация):

- Персональные данные работников Учреждения.
- Персональные данные граждан (в бумажном и электронном виде), к которым Учреждение получает доступ в рамках своей основной деятельности.
- Служебная информация, не содержащая персональных данных.

Порядок обработки и защиты каждой категории сведений, закрепление ответственности за лицами, имеющими к ним доступ, в том числе санкции за невыполнение норм безопасности, регулирующих обработку и защиту конфиденциальной информации, закрепляются соответствующими локальными нормативными актами.

6. Обработка информации в Учреждении производится с соблюдением следующих принципов:

- соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами;
- соблюдение конфиденциальности в отношении сведений, составляющих врачебную тайну;
- дифференцированный подход к обеспечению безопасности информации на основе ее классификации по степени ущерба от нарушений свойств безопасности;
- ответственности и отчетности Учреждения перед гражданином за обработку сведений, содержащих его персональные данные;

7. Доступ к конфиденциальной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме. При этом разовый, либо постоянный допуски к конфиденциальной информации оформляются приказом начальника Учреждения.

8. Порядок обработки и защиты конфиденциальной информации, закрепление ответственности за лицами, имеющими к ней доступ, в том числе санкции за невыполнение требований норм, регулирующих обработку и защиту конфиденциальной информации, закрепляются соответствующими локальными нормативными актами.

9. Организация, предоставляющая Учреждению базы данных с персонифицированной информацией (реестры, перечни и т.п.), несет ответственность перед субъектом персональных данных за действия Учреждения согласно п.5. Ст. 6 152-ФЗ «О персональных данных». Учреждение, в свою очередь, несет ответственность перед Организацией.

10. Меры защиты информации, выбираемые Учреждением, внедряются по результатам проведения оценки рисков информационной безопасности. Оценка рисков информационной безопасности проводится систематически, а также в случае значительных изменений в структуре Учреждения, и ее производственных процессах. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.