

УТВЕРЖДЕНА
приказом ГБУ АО «Центр
мониторинга в образовании»
от 12.01.2018 № 029

**Политика информационной безопасности
Государственного бюджетного учреждения Астраханской области
«Центр мониторинга в образовании»**

1. Настоящая политика определяет цели и принципы обеспечения информационной безопасности Государственного бюджетного учреждения Астраханской области «Центр мониторинга в образовании» (далее – Центр).
 2. Политика обязательна для исполнения всеми сотрудниками Центра, а также лицами, работающими с информацией, получаемой у Центра, 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 Центра от реализации угроз информационной безопасности.
 5. В Центре обрабатываются следующие категории информации ограниченного доступа (конфиденциальная информация):
 - персональные данные работников;
 - персональные данные, содержащиеся в материалах, необходимых для обеспечения процесса проведения государственной итоговой аттестации;
 - персональные данные, содержащиеся в материалах, необходимых для обеспечения процесса проведения аттестации педагогических работников;
 - служебная информация Центра, 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 Центре производится с соблюдением следующих принципов:
 - соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами, а также целостности и доступности информации;
 - дифференцированный подход к обеспечению безопасности информации на основе ее классификации по степени ущерба от нарушений свойств безопасности;
 - ответственности и отчетности Центра перед гражданином (в том числе перед сотрудником Центра) за обработку сведений, содержащих его персональные данные;
 - учет и контроль всех этапов автоматизированной и неавтоматизированной обработки конфиденциальной информации;
 - осведомленность сотрудников Центра, осуществляющих обработку конфиденциальной информации, в вопросах информационной безопасности;
 - персональная ответственность сотрудников Центра за выполнение норм информационной безопасности;

- использование принципа минимальных привилегий: 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 директора Центра.
7. Организация, предоставляющая Центру базы данных с персонифицированной информацией (реестры, перечни и т.п.), несет ответственность перед субъектом персональных данных за действия Центра согласно п.5. Ст.6 152-ФЗ «О персональных данных». Центр, в свою очередь, несет ответственность перед Организацией.
 8. Меры защиты информации, выбираемые Центром, внедряются по результатам проведения оценки рисков информационной безопасности. Оценка рисков информационной безопасности проводится систематически, а также в случае значительных изменений в структуре Центра, и ее производственных процессах. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.