

**ИНСТРУКЦИЯ**  
**ответственного за информационную безопасность**  
**в муниципальном бюджетном дошкольном образовательном учреждении**  
**«Детский сад № 10 комбинированного вида»**

**1. Общие положения**

- 1.1. Настоящая Инструкция определяет функции, права и обязанности ответственного за информационную безопасность в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад № 10 комбинированного вида» (далее – детский сад).
- 1.2. Ответственный за информационную безопасность назначается приказом заведующего детским садом.
- 1.3. Ответственный за информационную безопасность осуществляет свою деятельность в интересах детского сада в информационной сфере путем обеспечения защиты информации и поддержания достигнутого уровня защиты автоматизированных информационных систем (АИС) и ее ресурсов на всех этапах создания, модернизации и эксплуатации АИС.
- 1.4. Мероприятия по защите информации являются составной частью управленческой, производственной деятельности детского сада. Защита информации представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний в отношении технических и программных средств детского сада и информации, циркулирующей в них.
- 1.5. Инструкция регулирует отношения между ответственным за информационную безопасность, пользователями АИС, сторонними организациями, возникающие при:
  - эксплуатации и развитии АИС;
  - формировании и использовании данных, сообщений, баз данных, информационных ресурсов на основе создания, сбора, обработки, накопления поиска, хранения, распространения и предоставления пользователю документированной информации;
  - при создании, внедрении и эксплуатации новых информационных технологий.
- 1.6. Ответственный за информационную безопасность обладает правом доступа к любым программным и аппаратным ресурсам и любой информации на рабочих местах пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.
- 1.7. Требования ответственного за информационную безопасность, связанные с выполнением им своих функций, обязательны для исполнения всеми пользователями АИС.

**2. Обязанности ответственного за информационную безопасность**

- 2.1. Обеспечить информационную безопасность, защиту конфиденциальной информации, в том числе и на бумажных носителях, от несанкционированного доступа, искажения и уничтожения при ее передаче, обработке и хранении с использованием средств вычислительной техники.
- 2.2. Контролировать доступ в помещения, где хранятся средства информатизации, а также носители информации.
- 2.3. Обеспечивать доступ к защищаемой информации пользователям АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения.
- 2.4. Запрещать и немедленно блокировать применение пользователями сети программ, с помощью которых возможны факты несанкционированного доступа к ресурсам АИС.
- 2.5. Не допускать установку, использование, хранение, размножение в АИС программных средств, не связанных с выполнением функциональных задач.

- 2.6. Не допускать к работе на рабочих местах и серверах посторонних лиц.
- 2.7. Аппаратными и программными средствами выявлять факты несанкционированного доступа к информационным ресурсам АИС, а также другие нарушения, которые могут привести к разглашению или утрате конфиденциальной информации, и принимать меры по их пресечению.
- 2.8. Контролировать физическую сохранность средств и оборудования АИС.
- 2.9. Присутствовать при внесении изменений в конфигурацию (модификацию) аппаратно-программных средств защищенных АРМ.
- 2.10. Участвовать в приемке новых программных и аппаратных средств.
- 2.11. Периодически проверять состояние используемых систем защиты информации от несанкционированного доступа, осуществлять проверку правильности их настройки.
- 2.12. Вести контроль за процессом резервирования и дублирования важных ресурсов АИС.
- 2.13. Вести наблюдение за состоянием антивирусного контроля в организации.
- 2.14. Контролировать информацию, передаваемую по электронной почте, с целью исключения утечки конфиденциальной информации по открытым каналам связи.
- 2.15. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате несанкционированного доступа.
- 2.16. Периодически представлять руководству отчет о состоянии защиты и о нештатных ситуациях на объектах АИС и допущенных пользователями нарушениях установленных требованиями по защите информации.
- 2.17. Вносить предложения для принятия решений о привлечении виновных к ответственности за грубые нарушения требований нормативных документов по обеспечению сохранности конфиденциальной информации, а также о приостановке работ в случае обнаружения условий для утечки информации или материалов с пометкой для служебного пользования.

### **3. Права ответственного за информационную безопасность**

- 3.1. Проводить мероприятия по защите конфиденциальной информации от несанкционированного доступа.
- 3.2. Требовать от сотрудников детского сада соблюдения установленных технологий обработки информации и выполнения инструкций по защите информации.
- 3.3. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АИС.
- 3.4. Обращаться к руководителю детского сада с требованием прекращения работы в АИС при несоблюдении установленной технологии обработки информации и невыполнении требований по защите информации пользователями.
- 3.5. Отключать от сети пользователей, осуществивших несанкционированный доступ или нарушивший другие требования безопасности информации.
- 3.6. Запрещать устанавливать на АРМ нештатное программное обеспечение.

### **4. Ответственность лица, ответственного за информационную безопасность**

- 4.1. Ответственный за информационную безопасность несет ответственность за качественное и своевременное выполнение задач, возложенных на него в настоящей инструкции, а также определенных в текущих приказах руководителя детского сада.
- 4.2. На ответственного за информационную безопасность возлагается персональная ответственность за программно-технические и криптографические средства защиты информации, за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.