|  |
| --- |
| **C:\Users\user\Desktop\Контент-фильтрация\ДИ1.jpeg** |

* 1. Организовывать, в установленном порядке, передачу информации, составляющей коммерческую тайну Учреждения на сменных магнитных носителях и иными способами.
  2. Организовывать сопровождение работ по категорированию объектов средств

вычислительной техники Учреждения.

* 1. Знать перечень установленных в подразделениях Учреждения серверов, рабочих станций, средств копировально-множительной техники, устройств и топологию локально вычислительной сети.
  2. Иметь перечень информационных ресурсов Учреждения.
  3. Обеспечить доступ к защищаемой информации пользователям АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения;
  4. Осуществлять оперативный контроль за работой пользователей защищаемых рабочих станций, анализировать содержимое системных журналов всех PC и реагировать на возникающие нештатные ситуации.
  5. Запрещать и немедленно блокировать применение пользователям сети программ, с помощью которых возможны факты несанкционированного доступа к ресурсам АИС.
  6. Не допускать установку, использование, хранение и размножение в АИС программных средств, не связанных с выполнением функциональных задач.
  7. Не допускать к работе на рабочих станциях и серверах ЛВС посторонних лиц.
  8. 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.
  9. Контролировать физическую сохранность средств и оборудования АИС.
  10. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно- программных средств защищенных рабочих станций и серверов.
  11. Участвовать в приемке новых программных и аппаратных средств;
  12. Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки.
  13. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах

защищенных рабочих станций

* 1. Вести контроль за процессом резервирования и дублирования важных ресурсов АИС.
  2. Вести наблюдение за состоянием антивирусного контроля в организации.
  3. Контролировать информацию, передаваемую по электронной почте, с целью исключения утечки конфиденциальной информации по открытым каналам связи в Учреждении.
  4. Участвовать в расследовании причин совершения нарушений и возникновения

серьезных кризисных ситуаций в результате НСД.

* 1. Периодически представлять руководству отчет о состоянии защиты и о нештатных ситуациях на объектах АИС и допущенных пользователями нарушениях установленных требований по защите информации.
  2. 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.

1. **Права ответственного за информационную безопасность**

**Ответственный за информационную безопасность имеет право:**

* 1. Проводить мероприятия по защите конфиденциальной информации от

несанкционированного доступа.

* 1. Требовать от сотрудников Учреждения соблюдения установленных технологий обработки информации и выполнения инструкций по защите информации.

Проводить служебные расследования по фактам нарушения установленных

требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АИС.

Обращаться к руководителю Учреждения с требованием прекращения работы в

АИС при несоблюдении установленной технологии обработки информации и невыполнении требований по защите информации пользователями.

Отключать от сети пользователей, осуществивших НСД к защищаемым ресурсам

ЛВС и БД или нарушивших другие требования по безопасности информации.

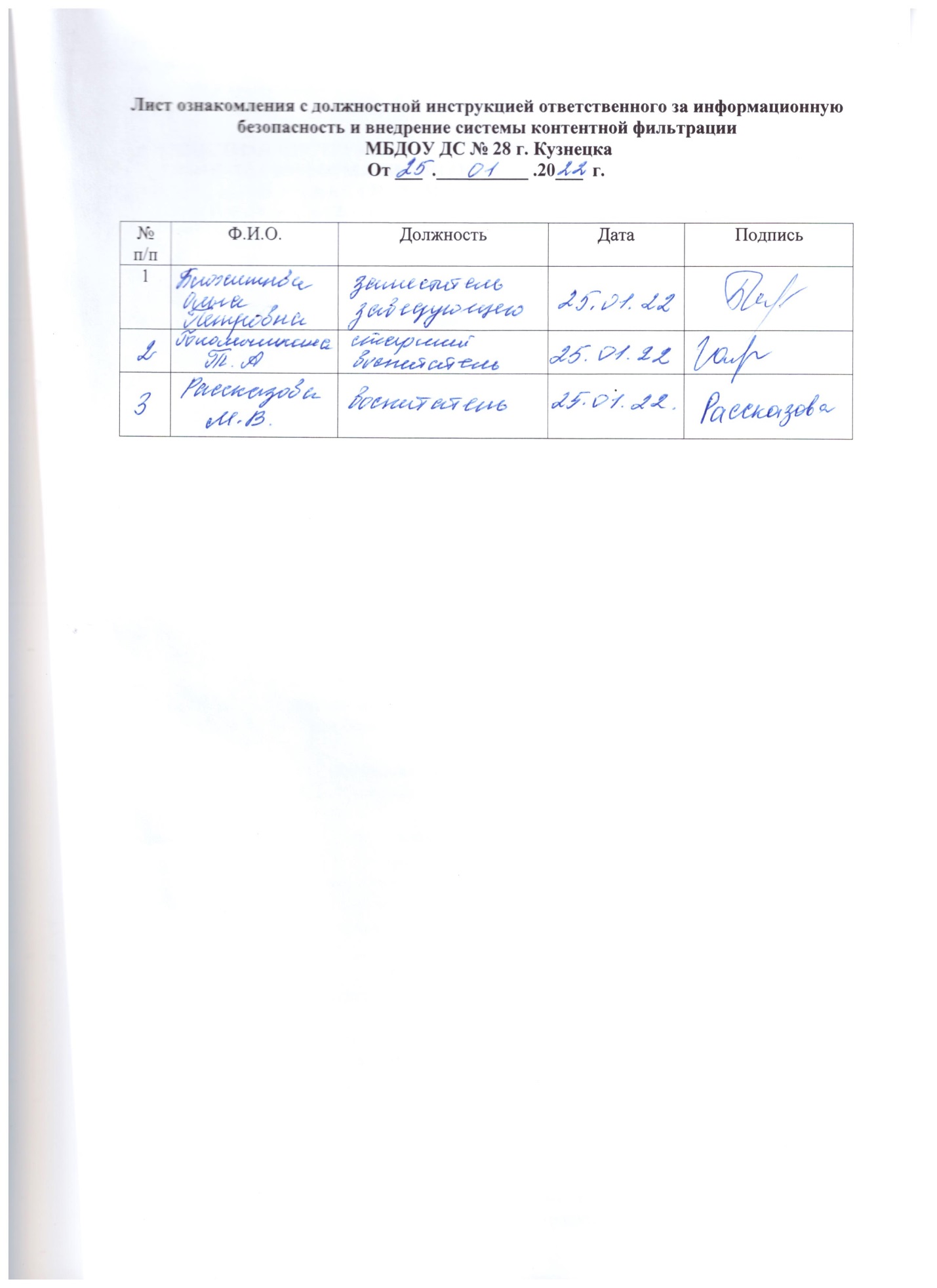
Запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение. Ответственность лица, ответственного за информационную безопасность

Ответственный за информационную безопасность несет ответственность за

качественное и своевременное выполнение задач, возложенных на него и изложенных в настоящей инструкции, а также определенных в текущих приказах и распоряжениях руководителя Детского сада

На ответственного за информационную безопасность возлагается персональная

ответственность за программно-технические и криптографические средства защиты информации, и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

****

