# Приложение 2

К приказу от \_\_\_\_\_\_\_№

«Об утверждении концепции информационной безопасности и назначении

ответственных за ее исполнение»

# УТВЕРЖДАЮ

Директор МБУ ДО «Центр ДО детей и эвенкийских народных ремёсел»

\_\_\_\_\_\_\_\_\_\_\_ О.Н. Цыбикова

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_ г.

# ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

Администратора информационной безопасности МБУ ДО «Центра ДО детей и эвенкийских народных ремёсел»

**1. Общие положения**

* 1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности МБУ ДО «Центра ДО детей и эвенкийских народных ремёсел»(далее - организация)
	2. Администратор информационной безопасности назначается приказом руководителя организации.
	3. Администратор информационной безопасности осуществляет свою деятельность в интересах организации 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.
	4. Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности организации. Защита информации представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний в отношении технических и программных средств организации и информации, циркулирующей в них.
	5. Администратор информационной безопасности несет ответственность за реализацию принятой в организации политики безопасности, закрепленной в Концепции информационной безопасности организации.
	6. Инструкция регулирует отношения между администратором информационной безопасности, 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, хранения, поиска, распространения и предоставления пользователю документированной информации;

- при создании, внедрении и эксплуатации новых информационных технологий.

* 1. Администратор информационной безопасности обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.
	2. Требования администратора информационной безопасности, связанные с выполнением ими своих функций, обязательны для исполнения всеми пользователями АИС.
1. **Обязанности администратора информационной безопасности**

Администратор информационной безопасности обязан:

* 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. Организовывать доступ пользователей и посторонних лиц в помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации.
	3. Организовывать, в установленном порядке, передачу информации, составляющей коммерческую тайну организации на сменных магнитных носителях и иными способами.
	4. Организовывать сопровождение работ по категорированию объектов средств вычислительной техники организации
	5. Знать перечень установленных в подразделениях организации серверов, рабочих станций, средств копировально-множительной техники, устройств и топологию локально-вычислительной сети.
	6. Иметь перечень информационных ресурсов организации.
	7. Обеспечить доступ к защищаемой информации пользователям АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения;
	8. Осуществлять учет и периодический контроль за составом и полномочиями пользователей:

- локальной сети организации;

- в корпоративном чате;

- в корпоративной электронной почте.

2.9. Осуществлять оперативный контроль за работой пользователей защищаемых рабочих станций, анализировать содержимое системных журналов всех РС и реагировать на возникающие нештатные ситуации.

* 1. Запрещать и немедленно блокировать приме
	2. нение пользователям сети программ, с помощью которых возможны факты несанкционированного доступа к ресурсам АИС.
	3. Не допускать установку, использование, хранение и размножение в АИС программных средств, не связанных с выполнением функциональных задач.
	4. Не допускать к работе на рабочих станциях и серверах ЛВС посторонних лиц.
	5. 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.
	6. Контролировать физическую сохранность средств и оборудования АИС.
	7. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных рабочих станций и серверов.
	8. Участвовать в приемке новых программных и аппаратных средств;
	9. Периодически проверять состояние используемых СЗИ НСД, осуществлять проверку правильности их настройки.

2.18. 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 организации.
	4. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.
	5. Периодически представлять руководству отчет о состоянии защиты и о нештатных ситуациях на объектах АИС и допущенных пользователями нарушениях установленных требований по защите информации.
	6. 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 администратора информационной безопасности**

Администратор информационной безопасности имеет право:

3.1. Проводить мероприятия по защите конфиденциальной информации от несанкционированного доступа.

3.2. Требовать от сотрудников организации 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 руководителям подразделений с требованием прекращения работы в АИС при несоблюдении установленной технологии обработки информации и невыполнении требований по защите информации пользователями подразделения.

3.5. Отключать от сети пользователей, осуществивших НСД к защищаемым ресурсам ЛВС и БД или нарушивших другие требования по безопасности информации.

3.6. Запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение.

**4. Ответственность администратора информационной безопасности**

4.1. Администратор информационной безопасности 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 организации.

4.2. На администратора информационной безопасности 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.