**Государственное областное автономное учреждение**

**социального обслуживания населения**

**«Ковдорский дом-интернат для престарелых и инвалидов»**

**ГОАУСОН «Ковдорский ДИПИ»**

# П Р И К А З

**30 декабря 2016 года № 146-од**

г. Ковдор

|  |
| --- |
| Об ответственном за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах ГОАУСОН «Ковдорский ДИПИ» |

В целях обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, и выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», **приказываю:**

1. Назначить ответственным за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах ГОАУСОН «Ковдорский ДИПИ» программиста Салацкого Сергея Владимировича.

2. Утвердить прилагаемую инструкцию ответственного за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах ГОАУСОН «Ковдорский ДИПИ».

3. Контроль за исполнением настоящего приказа оставляю за собой.

|  |  |
| --- | --- |
| **Директор** | **О.П. Макарова** |

Ознакомлен: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Салацкий

Утверждена

приказом ГОАУСОН «Ковдорский ДИПИ»

от 30.12.2016 № 146-од

**Инструкция ответственного за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах ГОАУСОН «Ковдорский ДИПИ»**

1. Общие положения
	1. Ответственный за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах государственного областного автономного учреждения социального обслуживания населения «Ковдорский дом-интернат для престарелых и инвалидов» (далее – Ответственный) назначается приказом государственного областного автономного учреждения социального обслуживания населения «Ковдорский дом-интернат для престарелых и инвалидов» (далее – Учреждение) и отвечает за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), в процессе ее обработки в информационных системах (далее – ИС) Учреждения.
	2. Ответственный должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации.
	3. В своей деятельности Ответственный руководствуется Политикой в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Учреждении, рекомендациями ответственного за организацию обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Учреждении (далее – Ответственный за организацию обработки защищаемой информации), настоящей Инструкцией.
	4. Методическое руководство работой Ответственного осуществляет Ответственный за организацию обработки защищаемой информации.
2. Основные функции и обязанности ответственного за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственной тайну, в информационных системах

Функции Ответственного:

* 1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по обеспечению безопасности защищаемой информации при решении следующих основных вопросов:
* проведение аналитической работы по комплексной защите и предупреждению утечки защищаемой информации;
* подготовка решений в отношении сведений о работах, выполняемых Учреждением, подлежащих защите;
* рассмотрение проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной защите информации, при научных исследованиях, при проведении других работ;
* координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;
* проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки защищаемой информации;
* подготовка предложений по совершенствованию действующей системы защиты информации с последующим предоставлением Ответственному за организацию обработки защищаемой информации Учреждения и/или руководителю Учреждения;
* учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей защищаемой информации;
* обеспечение соответствия проводимых работ в части обработки защищаемой информации технике безопасности, правилам и нормам охраны труда;
* осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

Ответственный обязан:

* 1. Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации.
	2. Знать состав, структуру, назначение и выполняемые задачи ИС, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку защищаемой информации.
	3. Осуществлять общее техническое сопровождение ИС:
* контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;
* контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;
* вести журнал учета и выдачи используемых материальных носителей информации;
* контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;
* проводить инструктаж сотрудников, осуществляющих обработку защищаемой информации и имеющих доступ к защищаемой информации, обрабатываемой в ИС Учреждения (далее – Пользователи ИС) по правилам работы в ИС.
	1. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИС:
* реализовывать полномочия доступа (чтение, запись) для каждого Пользователя ИС к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИС;
* назначать пароли Пользователей ИС;
* контролировать плановую смену паролей Пользователями ИС для доступа в ИС;
* своевременно удалять профиль Пользователя ИС при увольнении или переводе сотрудника;
* вводить в базу данных системы защиты от несанкционированного доступа (далее –НСД) описания событий, подлежащих регистрации в системном журнале;
* регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИС;
* своевременно информировать Ответственного за организацию обработки защищаемой информации о несанкционированных действиях персонала для организации расследования попыток НСД.
	1. Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИС:
* обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Министерства;
* обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;
* обеспечивать регулярное и своевременное создание резервных копий ИС Министерства;
* осуществлять настройку и сопровождение системы защиты от НСД в ИС.
	1. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИС.
	2. Требовать прекращения обработки защищаемой информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
	3. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.
	4. Участвовать при проведении внутреннего контроля соответствия обработки защищаемой информации установленным требованиям.
	5. Контролировать выполнение Пользователями ИС требований Инструкции пользователя информационных систем Учреждения, а также установленных требований по обеспечению безопасности защищаемой информации.
	6. Контролировать правильность применения Пользователями ИС средств защиты информации.
	7. В случае получения от Пользователей ИС информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности защищаемой информации в пределах своих полномочий.
	8. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИС:
* антивирусного программного обеспечения;
* средств защиты от несанкционированного доступа.
	1. В случае нарушения работоспособности технических средств и программного обеспечения ИС, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.
	2. Своевременно информировать Ответственного за организацию обработки защищаемой информации о выявленных нарушениях требований по обеспечению безопасности защищаемой информации и попытках несанкционированного доступа к ИС.
1. Права ответственного за обеспечение безопасности защищаемой информации, не составляющей государственной тайны, в информационных системах

Ответственный имеет право:

* 1. Знакомиться с нормативными актами Учреждения, регламентирующими процессы обработки защищаемой информации.
	2. Вносить предложения руководителю Учреждения по совершенствованию существующей системы защиты информации.
	3. Привлекать по согласованию Ответственным за организацию обработки защищаемой информации и руководителем Учреждения к работе по созданию и совершенствованию системы защиты информации других сотрудников Учреждения.
	4. Требовать от Пользователей ИС соблюдения требований Инструкции пользователя информационных систем Учреждения, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации.
	5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность защищаемой информации, вносить свои предложения по совершенствованию организационных и технических мер обеспечения безопасности защищаемой информации в ИС.
	6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности защищаемой информации.
	7. Требовать прекращения работы в ИС, как в целом, так и отдельных Пользователей ИС, в случае выявления нарушений требований по обеспечению безопасности защищаемой информации или в связи с нарушением функционирования ИС.
	8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности защищаемой информации к Ответственному за организацию обработки защищаемой информации.