Приложение № 9
к приказу «Об обеспечении безопасности персональных данных в информационных системах персональных данных ФГБУЗ ММЦ им. Н.И. Пирогова ФМБА России»
№ 01-147 от 12.07.2022

Инструкция администратора информационной безопасности Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства» (далее - Учреждение) по обеспечению безопасности информационных систем персональных данных (далее - ИСПДн) в Учреждении.

1.2. Администратор информационной безопасности руководствуется в своей практической деятельности положениями федеральных законов, нормативных актов Российской Федерации, документами ФСБ России, ФСТЭК России, ФАПСИ и Госстандарта России, организационно-распорядительными документами Учреждения в области обработки и защиты персональных данных (далее – ПДн).

1.3. Обучение и повышение квалификации администраторов информационной безопасности осуществляется организациями, имеющими соответствующую лицензию согласно Перечню организаций, осуществляющих образовательную деятельность, имеющих дополнительные профессиональные программы в области информационной безопасности, согласованные с ФСТЭК(https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obuchenie-spetsialistov/12-perechen-obrazovatelnykh-uchrezhdenij).

2. Обязанности администратора информационной безопасности

2.1. Администратор информационной безопасности обязан:

1) не разглашать и не передавать третьим лицам без согласия обладателя информации персональные данные и сведения конфиденциального характера, которые ему будут доверены или станут известны в процессе работы;

2) ставить в известность о предпринятых попытках третьих лиц получить сведения о защищаемой конфиденциальной информации или об имевших место попытках несанкционированного доступа к информации и техническим средствам персональных электронных вычислительных машин директора (заместителя директора) Учреждения;

3) не использовать знания о защищаемой конфиденциальной информации, средствах криптографической защиты информации (далее - СКЗИ), криптоключах к ним для занятий любым видом деятельности, которая может нанести ущерб обладателю конфиденциальной информации;

4) в случае увольнения или отстранения от исполнения возложенных обязанностей, передать своему непосредственному начальнику ключевые документы и все носители конфиденциальной информации, которые находились в его распоряжении в связи с выполнением служебных обязанностей по обеспечению безопасности информации;

5) немедленно докладывать директору (заместителю директора) об утрате или недостаче СКЗИ, ключевых документов к ним, об инцидентах и о других фактах, которые могут привести к разглашению защищаемых персональных данных и сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

6) осуществлять оперативный контроль за работой пользователей рабочих станций ИСПДн, анализировать содержимое системных журналов всех систем учета доступа к защищаемой информации и адекватно реагировать на возникающие нештатные ситуации;

7) осуществлять управление режимами работы и административную поддержку функционирования СКЗИ, применяемых на рабочих станциях ИСПДн, и специальных технических средств защиты от несанкционированного доступа (далее - НСД);

8) присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных рабочих станций и серверов, устанавливать и осуществлять настройку средств защиты, соблюдать порядок проверки работоспособности системы защиты после установки (обновления) программных средств;

9) периодически проверять состояние используемых средств защиты информации от несанкционированного доступа (далее - СЗИ от НСД), осуществлять проверку правильности их настройки (выборочное тестирование);

10) периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищаемых рабочих станций;

11) проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам ПЭВМ системы;

12) проводить занятия с сотрудниками Учреждения по правилам работы на ПЭВМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения персональных данных и безопасности информации;

13) участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД к ИСПДн;

14) устанавливать разграничение полномочий пользователей и порядок доступа к информационным ресурсам, порядок использования основных и вспомогательных технических средств и систем.

3. Права администратора информационной безопасности

3.1. Администратор информационной безопасности имеет право требовать от сотрудников Учреждения выполнения инструкций по обеспечению безопасности и защите информации персональных данных.

3.2. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.3. Непосредственно обращаться к руководителям структурных подразделений Учреждения с требованием о прекращении работы с вычислительной техникой при несоблюдении сотрудниками данных подразделений установленной технологии обработки информации и невыполнении требований по обеспечению безопасности ИСПДн.

3.4. Немедленно блокировать попытки изменения применения пользователями сети программ, с помощью которых возможны факты несанкционированного доступа к персональным данным или вычислительной сети Учреждения.

3.5. Вносить свои предложения по совершенствованию мер защиты информации в конкретной ИСПДн.

4. Ответственность администратора информационной безопасности

4.1. На администратора информационной безопасности возлагается персональная ответственность за бесперебойную работу программно-технических средств защиты ИСПДн, закрепленных за ним, и за качество проводимых им работ по обеспечению защиты информации.

4.2. За разглашение конфиденциальной информации, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации, может быть привлечен к установленной законом ответственности.

_____