МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПРИКАЗ

г. Челябинск

от «23» 07 2018 г. № 1467

Об утверждении Положения о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Министерстве здравоохранения Челябинской области

В соответствии со Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положение о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Министерстве здравоохранения Челябинской области.

2. Начальнику управления организационного и документационного обеспечения Министерства здравоохранения Челябинской области Устюжаниной Н.В. ознакомить сотрудников Министерства здравоохранения Челябинской области под подпись с настоящим приказом.

3. Директору Государственного бюджетного учреждения здравоохранения «Челябинский областной медицинский информационно-аналитический центр» Пластовцу А.И. разместить настоящий приказ на официальном сайте Министерства здравоохранения Челябинской области в сети Интернет.

4. Контроль исполнения настоящего приказа оставляю за собой.

Министр С.И. Приколотин

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «ЧЕЛЯБИНСКИЙ ОБЛАСТНОЙ МЕДИЦИНСКИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР» (ГБУЗ «ЧОМИАЦ», ИНН 7453141034, ОГРН 1057424502673)
Вх. № 1473 от 19.11.2018 г.

УТВЕРЖДЕНО
приказом
Министерства здравоохранения
Челябинской области
от «23» 07 2018 г. № 1467

Положение
о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Министерстве здравоохранения Челябинской области

I. Общие положения

1. Настоящее Положение о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Министерстве здравоохранения Челябинской области (далее именуется - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 г. № 282, и другими нормативными методическими документами по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

2. Настоящее Положение определяет порядок организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну (далее именуется - информация ограниченного доступа), в Министерстве здравоохранения Челябинской области (далее именуется - Министерство).

3. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её собственника.

4. При определении конфиденциальности документов, в том числе в электронной форме, необходимо руководствоваться Перечнем сведений конфиденциального характера (далее именуется - Перечень), утверждённым приказом Министерства здравоохранения Челябинской области.

5. Государственные гражданские служащие и работники Министерства, которые в силу служебной необходимости должны иметь доступ к информации конфиденциального характера, обязаны ознакомиться с настоящим Положением и Перечнем под роспись.

6. Ознакомление государственных гражданских служащих и работников Министерства с Положением и Перечнем, а также их инструктаж по работе с информацией конфиденциального характера осуществляется их непосредственными руководителями.

Обязательство о неразглашении информации конфиденциального характера государственным гражданским служащим или работником Министерства прописано в его должностных обязанностях (регламенте).

7. Порядок обращения со служебной информацией ограниченного доступа должен осуществляться в соответствии с требованиями Положения о порядке обращения со служебной информацией ограниченного распространения в Аппарате Губернатора и Правительства Челябинской области и органах исполнительной власти Челябинской области, утвержденного распоряжением Губернатора Челябинской области от 08.04.2015 г. № 330-р «О Положении о порядке обращения со служебной информацией ограниченного распространения в Аппарате Губернатора и Правительства Челябинской области и органах исполнительной власти челябинской области»

II. Информация, подлежащая защите, и потенциальные угрозы информационной безопасности объектов защиты

8. Защите подлежит информация ограниченного доступа (речевая информация и информация, обрабатываемая техническими средствами, а также представленная в виде носителей на бумажной, магнитной, магнито-оптической и иной основе).

Объектами защиты при этом являются:

автоматизированные системы (далее именуются - АС);

средства изготовления и размножения документов (далее именуются - СИРД).

9. В качестве угроз информационной безопасности объектов защиты необходимо рассматривать:

использование разведками иностранных государств технических средств для получения информации ограниченного доступа, перехват информации, обсуждаемой в защищаемых помещениях и циркулирующей в основных технических средствах и системах, а также воздействие на информационные ресурсы автоматизированных систем с целью разрушения, искажения и блокирования информации;

использование криминальными структурами технических средств для получения информации, представляющей ценность в интересах планирования криминальных акций;

преднамеренные действия нарушителей и злоумышленников, незаконным путем проникших на объекты посредством контактного несанкционированного доступа к элементам автоматизированных систем, к носителям информации, к вводимой и выводимой информации, к программному обеспечению, а также подключения к линиям связи;

непреднамеренные действия персонала, приводящие к утечке, искажению, разрушению информации, подлежащей защите, в том числе ошибки эксплуатации технических и программных средств автоматизированных систем.

III. Цели и задачи технической защиты информации ограниченного доступа

10. Целями технической защиты информации ограниченного доступа являются:

исключение утечки информации ограниченного доступа с помощью технических средств разведки;

предотвращение несанкционированного доступа (далее именуется - НСД) к информации ограниченного доступа, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования в системах и средствах информатизации;

обеспечение условий быстрого, полного и всестороннего расследования случаев утечки информации;

устранение негативных последствий и условий в случае несанкционированной утечки или утраты информации.

11. Задачами технической защиты информации ограниченного доступа являются:

проведение в Министерстве государственной политики по технической защите информации;

подготовка предложений по совершенствованию правового, нормативного, методического и организационного обеспечения технической защиты информации в Министерстве;

анализ состояния и прогнозирование источников угроз безопасности информации;

разработка целевых программ по технической защите информации в Министерстве;

учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения информации, подлежащих технической защите;

контроль и анализ состояния технической защиты информации в Министерстве;

развитие и совершенствование системы подготовки кадров в области технической защиты информации в Министерстве.

IV. Порядок аттестации, ввода в эксплуатацию объектов информатизации и взаимодействия Министерства, специализированных сторонних организаций при эксплуатации объектов информатизации и системы защиты информации

12. В Министерстве документально оформляется перечень объектов информатизации (АС, СИРД), а также лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации.

13. Все объекты информатизации (далее именуются - ОИ), предназначенные для обработки (хранения, циркуляции) информации ограниченного доступа, должны быть аттестованы на соответствие установленным нормам и требованиям по защите информации.

Аттестация предусматривает комплексную проверку (аттестационные

испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

14. Аттестационные испытания проводятся аттестационной комиссией предприятий (организаций), имеющих лицензию Федеральной службы по техническому и экспортному контролю (далее именуется – ФСТЭК России) на деятельность по технической защите конфиденциальной информации (организации-лицензиаты ФСТЭК России).

Для проведения испытаний аттестационной комиссии подготавливаются и представляются:

технический паспорт на объект информатизации;

акт классификации объекта информатизации по требованиям защиты информации;

состав технических и программных средств, входящих в автоматизированную систему (или технических средств, расположенных в защищаемом помещении);

план контролируемой зоны;

перечень защищаемых в АС ресурсов (или конфиденциальность обсуждаемых в защищаемых помещении вопросов);

организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС (обсуждаемым вопросам);

инструкции пользователям и администратору безопасности информации;

инструкции по эксплуатации средств защиты информации;

сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации.

В результате аттестационных испытаний оформляется «Аттестат соответствия», которым подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативных документов по защите конфиденциальной информации, утвержденных ФСТЭК России и другими органами государственного управления в пределах их компетенции.

На основании выданного специализированной организацией аттестата соответствия издается приказ Министерства о разрешении обработки информации ограниченного доступа на объекте информатизации и назначении лиц, ответственных за обеспечение защиты информации при его эксплуатации.

Привлечение для организации работ по созданию системы защиты информации (далее именуется - СЗИ) или ее отдельных компонентов сторонних специализированных организаций осуществляется в соответствии с порядком, устанавливаемым нормативными и организационно-распорядительными документами ФСТЭК России.

В случае привлечения для обеспечения безопасности информации сторонних специализированных организаций в соответствии с требованиями Федерального закона от 05.04.2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» рекомендуется выполнение следующих условий:

наличие у организации лицензии на право проведения работ по технической защите конфиденциальной информации;

проведение инструктажа исполнителей работ по вопросам информационной безопасности;

другие условия, устанавливаемые соответствующими нормативными и организационно-распорядительными документами.

Структурная схема взаимодействия Министерства и специализированных сторонних организаций при аттестации, вводе в эксплуатацию и эксплуатации ОИ и системы защиты информации приведена на рис. 1.

Рис 1. Структурная схема взаимодействия Министерства и специализированных сторонних организаций при аттестации, вводе в эксплуатацию и эксплуатации ОИ и системы защиты информации

V. Контроль состояния защиты информации в Министерстве

15. Контроль состояния защиты информации в Министерстве осуществляется в целях:

предупреждения и пересечения возможности получения техническими средствами разведки охраняемых сведений об объектах информатизации органа;

выявления и предотвращения утечки информации по техническим каналам;

исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации;

предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

16. Основными задачами контроля являются:

проверка организации выполнения мероприятий по защите информации в подразделениях Министерства, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

проверка выполнения установленных норм и требований по защите информации;

оценка достаточности и эффективности мероприятий по защите

информации;

проверка выполнения требований по защите автоматизированных систем от несанкционированного доступа;

проверка выполнения требований по антивирусной защите автоматизированных рабочих мест;

проверка знаний должностных лиц по вопросам защиты информации и их соответствия необходимому уровню подготовки для конкретного рабочего места;

оперативное принятие мер по пресечению нарушений требований (норм) защиты информации на объектах информатизации Министерства.

17. Повседневный контроль за выполнением мероприятий по защите информации осуществляет специалист, ответственный за эксплуатацию ОИ.

18. Периодический контроль за выполнением мероприятий по защите информации проводится руководителями структурных подразделений, где эксплуатируется объект информатизации, совместно с администратором АС и специалистом, ответственным за эксплуатацию объекта информатизации не реже одного раза в полгода.

В ходе контроля проверяется:

соблюдение организационно-режимных требований;

выполнение требований по защите автоматизированных систем от несанкционированного доступа;

выполнение требований по антивирусной защите автоматизированных систем.

19. Контроль эффективности принятых мер защиты информации на объектах информатизации Министерства с использованием технических средств осуществляется не реже одного раза в год организациями-лицензиатами ФСТЭК России с оформлением протокола ежегодной проверки на соответствие требованиям по защите информации и заключения по результатам ежегодной проверки на соответствие требованиям по защите информации объекта информатизации.

Результаты контроля отражаются в техническом паспорте объекта информатизации.

VI. Ответственность должностных лиц

20. Ответственность за организацию работ по защите информации в Министерстве возлагается на должностное лицо, назначенное ответственным за непосредственное руководство работами по защите информации.

21. Ответственность за планирование работ по защите информации, организацию контроля за эффективностью их выполнения, организацию разработки нормативно-методических документов по технической защите информации, разработку (совместно со структурными подразделениями, эксплуатирующими ОИ) распорядительных документов по вопросам организации технической защиты информации, аттестацию объектов информатизации возлагается на ответственного за обеспечение безопасности информации в Министерстве.

22. Ответственность за выполнение установленных мероприятий по технической защите информации на введенных в эксплуатацию объектах информатизации, возлагается на руководителя структурного подразделения, эксплуатирующего объект информатизации и ответственного за эксплуатацию объекта информатизации.

23. Ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и обновление баз данных вирусных описаний на АС возлагается на администратора безопасности.

24. Ответственность за своевременное ознакомление государственных гражданских служащих и работников Министерства с руководящими документами по организации защиты информации и порядку работы с информацией ограниченного доступа несут их непосредственные руководители.

25. Должностные лица, допустившие разглашение информации ограниченного доступа, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Министерство здравоохранения Челябинской области

Служебная записка

Кому: руководителям структурных подразделений Министерства здравоохранения Челябинской области

От: начальника управления организационного и документационного обеспечения Министерства здравоохранения Челябинской области Устюжаниной Н.В.

Дата: 01.11.2018 г.

Номер: № 104

Уважаемые коллеги!

Прошу ознакомиться и ознакомить под подпись сотрудников курируемых Вами структурных подразделений с приказом Министерства здравоохранения Челябинской области № 1467 от 23.07.2018 г. «Об утверждении Положения о порядке организации и проведения работ по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в Министерстве здравоохранения Челябинской области».

Листы ознакомления прошу вернуть в отдел организационной и контрольной работы управления организационного и документационного обеспечения (каб. 403) в срок **до 02.11.2018 г.**

Приложение: на 8 л. в 1 экз.

Начальник управления
организационного и
документационного обеспечения Н.В. Устюжанина

Кучина Людмила Валерьевна
240-22-22 (доб. 140)