МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ КАЛУЖСКОЙ ОБЛАСТИ

ГБУЗ КО «СТАНЦИЯ СКОРОЙ МЕДИЦИНСКОЙ ПОМОЩИ »

23.05.2013г. ПРИКАЗ г. Калуга

№ 66

Об утверждении правил обработки защищаемой информации

В целях обеспечения безопасности информации при её обработке на объекте автоматизации ГБУЗ КО «ССМП»

ПРИКАЗЫВАЮ:

Утвердить Правила обработки защищаемой информации в ГБУЗ КО «ССМП»

Главный врач Т.М. Гусенкова

Приложение № 1
к приказу об утверждении
правил обработки защищаемой
информации
от 23.05.2013г. № 66

ПРАВИЛА
обработки защищаемой информации

ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящий документ определяет порядок обработки защищаемой информации, регламентирует порядок работы с документами и электронными и магнитными носителями, содержащими защищаемую информацию ГБУЗ КО «ССМП».

ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2. В целях обеспечения сохранности документов, содержащих защищаемую информацию, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками ГБУЗ КО «ССМП», осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

3. Документы содержащие защищаемую информацию обрабатываются в соответствии с утвержденной инструкцией по ведению делопроизводства в ГБУЗ КО «ССМП».

4. Защищаемая информация при её обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации её на отдельных материальных носителях (далее - материальные носители), в специальных разделах или на специальных полях форм (бланков).

5. Лица, осуществляющие обработку защищаемой информации без использования средств автоматизации, должны быть проинформированы о факте обработки ими защищаемой информации, а также об особенностях и правилах осуществления такой обработки, установленных нормативными актами организации.

6. Уничтожение защищаемой информации, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этой информации с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7. Не допускается без согласования с руководителем организации формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих защищаемую информацию.

ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ И ХРАНЕНИИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

8. Безопасность информации достигается путем исключения несанкционированного, в том числе случайного, доступа к защищаемой

информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий.

9. Безопасность информации при её обработке на объекте информатизации обеспечивается с помощью системы защиты информации, включающей организационные меры и средства защиты информации, а также используемые на объекте информатизации информационные технологии.

10. Организация режима обеспечения безопасности помещений, в которых ведется работа с защищаемой информацией, должна обеспечивать сохранность носителей защищаемой информации, средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

11. При обработке защищаемой информации на объекте информатизации должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к защищаемой информации и (или) передачи её лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к защищаемой информации;

в) недопущение воздействия на технические средства автоматизированной обработки защищаемой информации, в результате которого может быть нарушено их функционирование;

г) постоянный контроль за обеспечением уровня защищенности информации.

12. Мероприятия по обеспечению безопасности защищаемой информации при её обработке на объекте автоматизации включают в себя:

а) определение угроз безопасности информации;

б) разработку системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз;

в) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

г) обучение лиц, использующих средства защиты информации правилам работы с ними;

д) учет лиц, допущенных к работе с защищаемой информацией;

е) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

ё) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей защищаемой информации, использования средств защиты информации, которые могут привести к нарушению конфиденциальности защищаемой информации или другим нарушениям, приводящим к снижению уровня защищенности информации, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

13. Лица, доступ которых к защищаемой информации, обрабатываемой в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующей информации на основании списка, утвержденного руководителем организации.

14. При осуществлении обработки защищаемой информации с использованием средств автоматизации должен быть назначен администратор системы безопасности. Техническое обслуживание оборудования должно осуществляться соответствующим обслуживающим персоналом, состав которого утверждается приказом главного врача ГБУЗ КО «ССМП».

15. Работа со съемными носителями информации проводится в соответствии с инструкцией по работе и учету электронных, магнитных и оптических носителей информации, на которых обрабатываются защищаемая информация.

16. В целях обеспечения антивирусной защиты работа с защищаемой информацией проводится в соответствии с инструкцией «По организации антивирусной защиты».

17. Уничтожение защищаемой информации производится в соответствии с Порядком уничтожения защищаемой информации.

Ответственный
за организацию обработки
защищаемой информации
начальник АСУ
А.Г. Макаров