Приложение №2

УТВЕРЖДАЮ»
Главный врач
ГБУ РО «ДГБ №1» в г. Ростове-на-Дону

_____ Ж.Г. Мушегян

«___» _____ 2023 г.

ПОЛОЖЕНИЕ
о безопасной эксплуатации средств криптографической защиты информации в автоматизированной системе Государственного бюджетного учреждения Ростовской области «Детская городская больница №1» в г. Ростове-на-Дону

1. Источники разработки

Настоящее положение разработано в соответствии с:

- Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных».
- Федеральным законом Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Указом Президента Российской Федерации от 6 марта 1997 г. №188 «Перечень сведений конфиденциального характера».
- Указом Президента Российской Федерации от 17.03.2008 N 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (Утверждены руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432).
- Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- Приказом Федеральной службы безопасности (ФСБ России) 9.02.2005 г. №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
- Приказом ФАПСИ от 13.06.2001 г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

2. Общие положения

2.1. Настоящее Положение определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ), в целях обеспечения безопасности эксплуатации СКЗИ в автоматизированной системе (далее - АС) Государственного бюджетного учреждения Ростовской области «Детская городская больница №1» в г. Ростове-на-Дону (далее - Учреждение).

2.2. В Учреждении с учетом особенностей деятельности могут разрабатываться не противоречащие настоящему положению организационно-распорядительные и методические документы, уточняющие порядок работы с СКЗИ и криптографическими ключами.

2.3. В качестве СКЗИ в АС Учреждения используется:

- Средство криптографической защиты информации АПКШ «Континент»;
- Средство криптографической защиты информации «Крипто-Про».

2.4. Ввод СКЗИ в эксплуатацию осуществляется на основании Акта ввода СКЗИ в эксплуатацию, форма которого приведена в Приложении №2.1.

2.5. Руководство Учреждения назначает ответственного пользователя СКЗИ, который организует и обеспечивает работу по техническому обслуживанию СКЗИ при непосредственном физическом доступе обслуживающей организации.

3. Ответственный пользователь СКЗИ

3.1. Ответственный пользователь СКЗИ назначается из числа сотрудников

Учреждения и освобождается от этих обязанностей приказом руководства Учреждения.

3.2. Ответственный пользователь СКЗИ должен быть ознакомлен под роспись с нормативно-правовыми актами, определяющими правила и процедуры обеспечения безопасности информации на объекте информатизации.

3.3. Функции и обязанности ответственного пользователя СКЗИ:

- своевременно и качественно исполнять поручения руководства данные в пределах их полномочий, установленных законодательством Российской Федерации;
- оказывать консультационную помощь по вопросам соблюдения защиты информации при обращении с СКЗИ;
- постоянно повышать профессиональные навыки и умения, необходимые для надлежащего исполнения функциональных обязанностей;
- знать правила пользования СКЗИ и осуществлять контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящим положением;
- соблюдать режим конфиденциальности при обращении со сведениями, полученными при исполнении функциональных обязанностей, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;
- осуществлять поэкземплярный учет СКЗИ, ключевой информации, эксплуатационной и технической документации к ним;
- обеспечивать надежное хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.
- выявлять попытки посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним и своевременное оповещать об этом руководителя Учреждения.
- незамедлительно принимать меры по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.
- участвовать в расследованиях и составлении заключений по фактам нарушения условий использования СКЗИ и разрабатывать и внедрять меры по предотвращению возможных негативных последствий от подобных нарушений.

3.4. На ответственного пользователя СКЗИ возлагается ежедневный контроль функционирования и безопасности СКЗИ как объекта защиты. Ответственным пользователем СКЗИ должно контролироваться соблюдение следующих обязательных мер защиты:

- постоянное закрытие дверей помещений/стоек, где расположены СКЗИ, на замок и их открытия только для санкционированного прохода, а также постановку их под охрану по окончании рабочего дня;
- утверждение и поддержание в актуальном состоянии списка лиц, имеющих право доступа к помещениям/стойкам, где расположены СКЗИ и правил (целей) такого доступа;
- осуществление поэкземплярного учета СКЗИ, ключевой информации, дистрибутивов и документации, машинных носителей персональных данных, который достигается путем ведения соответствующих журналов журнала учета с использованием регистрационных (заводских) номеров;
- поддержание в актуальном состоянии документа, определяющего перечень лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей.

3.5. Права ответственного пользователя СКЗИ:

- осуществлять плановые и внеплановые проверки функционирования СКЗИ, наличия ключевых документов и технической документации с СКЗИ;

- осуществлять, в рамках своей компетенции, взаимодействие с организациями-производителями СКЗИ;

- при изменении состава СКЗИ получить профессиональную переподготовку, повышение квалификации и стажировку в порядке, установленном законодательством Российской Федерации;

- ходатайствовать о проведении служебной проверки.

3.6. В случае неисполнения или ненадлежащего выполнения требований настоящего положения ответственный пользователь СКЗИ может быть привлечен к дисциплинарной, административной или уголовной ответственности в соответствии с действующим Законодательством Российской Федерации.

4. Учет и хранение СКЗИ и документации

4.1. Поэкземплярный учет СКЗИ, ключевых документов, ключевой информации, эксплуатационной и технической документации к ним ведет ответственный пользователь СКЗИ в Журнале по форме, приведенной в Приложении №2.2. к настоящему Положению. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация с использованием их серийных номеров.

4.2. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале (Приложение №2.3.), ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

4.3. Дистрибутивы СКЗИ на магнитных носителях или оптических дисках, эксплуатационная и техническая документация к СКЗИ хранятся у ответственного пользователя СКЗИ.

4.4. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

4.5. Ответственный пользователь должен ежедневно проверять сохранность используемого оборудования и целостность печатей.

4.6. В случае обнаружения факта повреждения печати на корпусе СКЗИ, механического взлома коммутационного шкафа или серверного помещения работа должна быть прекращена. По данному факту проводится служебное расследование, и осуществляются работы по анализу и ликвидации последствий данного нарушения.

4.7. Вскрытие коммутационного шкафа или помещения, в котором установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться только в присутствии ответственного за эксплуатацию СКЗИ.

5. Организация режима в помещениях

5.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ (далее – режимные помещения), должны обеспечивать сохранность СКЗИ.

5.2. При обустройстве режимных помещений/стоек должны выполняться требования формуляров к размещению, монтажу СКЗИ, а также другого оборудования

функционирующего с СКЗИ.

5.3. Режимные помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

5.4. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, должны оборудоваться металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

5.5. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также визуальное наблюдение посторонними лицами за проведением работ в помещении.

5.6. Режимные помещения, оснащаются охранной и пожарной сигнализацией.

Приложение №2.1. к Положению о безопасной эксплуатации средств криптографической защиты информации в автоматизированной системе Государственного бюджетного учреждения Ростовской области «Детская городская больница №1» в г. Ростове-на-Дону

АКТ

установки средств криптографической защиты информации, ввода в эксплуатацию и закрепления их за ответственными лицами

г. _____ «__» _____ 201_ г.

Заказчик: Исполнитель:

Адрес: Адрес:

Настоящий акт составлен о том, что в период с «__» _____ 201_ г. по «__» _____ 201_ г. представителем исполнителя _____ была произведена установка и настройка средств криптографической защиты информации далее – СКЗИ, согласно Таблице 1

№ п/п	Наименование и тип продукции	Рег. № СКЗИ (номер экземпляра)	Сведения о сертификате	Место установки
1.				

ФИО ответственного пользователя СКЗИ: _____

Размещение СКЗИ, хранение ключевых носителей, охрана помещений организованы установленным порядком;

Обучение правилам работы с СКЗИ и проверка знаний нормативно правовых актов и эксплуатационной и технической документации к ним проведены.

Условия для использования СКЗИ, установленные эксплуатационной и технической документацией к СКЗИ созданы.

Установленное и настроенное СКЗИ находится в работоспособном состоянии.

Формуляр выведен на бумажный носитель, все разделы Формуляра заполнены установленным порядком.

Формуляр передан на ответственное хранение пользователю СКЗИ.

Пользователь СКЗИ обязуется:

- не распространять конфиденциальную информацию, к которой он допущен, в том числе криптоключи и сведения о ключевой информации;
- соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сдать установочный комплект СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранения от исполнения обязанностей, связанных с использованием СКЗИ;
- сообщать ответственному за организацию защиты информации и обработки персональных данных о попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним,
- немедленно уведомлять ответственного за организацию защиты информации и обработки персональных данных о фактах утраты или недостачи СКЗИ, ключевых документов к ним.

Акт составлен в двух экземплярах.

Исполнитель _____ / _____ /

(подпись) (Фамилия И.О.)

Заказчик _____

(подпись) (Фамилия И.О.)

Приложение №2.2 к Положению о безопасной эксплуатации средств криптографической защиты информации в автоматизированной системе Государственного бюджетного учреждения Ростовской области «Детская городская больница №1» в г. Ростове-на-Дону

Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные - номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств			Примечание	
				От кого получены	Дата и № сопроводит. док.	Ф.И.О пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников произведших установку	Дата установки	Инв. № аппаратн. редств, к которым подключены СКЗИ	Дата изъятия	Ф.И.О. сотрудников производивших изъятие	№ акта (расписка) об уничтож.	Сфера применения	№ комнаты
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Приложение №2.3. к Положению о безопасной эксплуатации средств криптографической защиты информации в автоматизированной системе Государственного бюджетного учреждения Ростовской области «Детская городская больница №1» в г. Ростове-на-Дону

Аппаратный журнал СКЗИ

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	