РМИАЦ

Особенности защиты информации в ГИС Минздрава Удмуртии

Руководитель группы по обеспечению ИБ
БУЗ УР «РМИАЦ МЗ УР»
Соловьев Сергей Вениаминович

НПА, составляющие основу ИБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

Об информации, информационных технологиях и о защите информации

8 июля 2006 года

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

О персональных данных

Принят Государственной Думой 8 июля 20
Одобрен Советом Федерации 14 июля 2

Статья 1. Сфера действия настоящего Федерального закона

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

Об электронной подписи

Принят Государственной Думой 25 марта 2011 года
Одобрен Советом Федерации 30 марта 2011 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами. *(В редакции Федерального закона от 05.04.2013 № 60-ФЗ)*

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

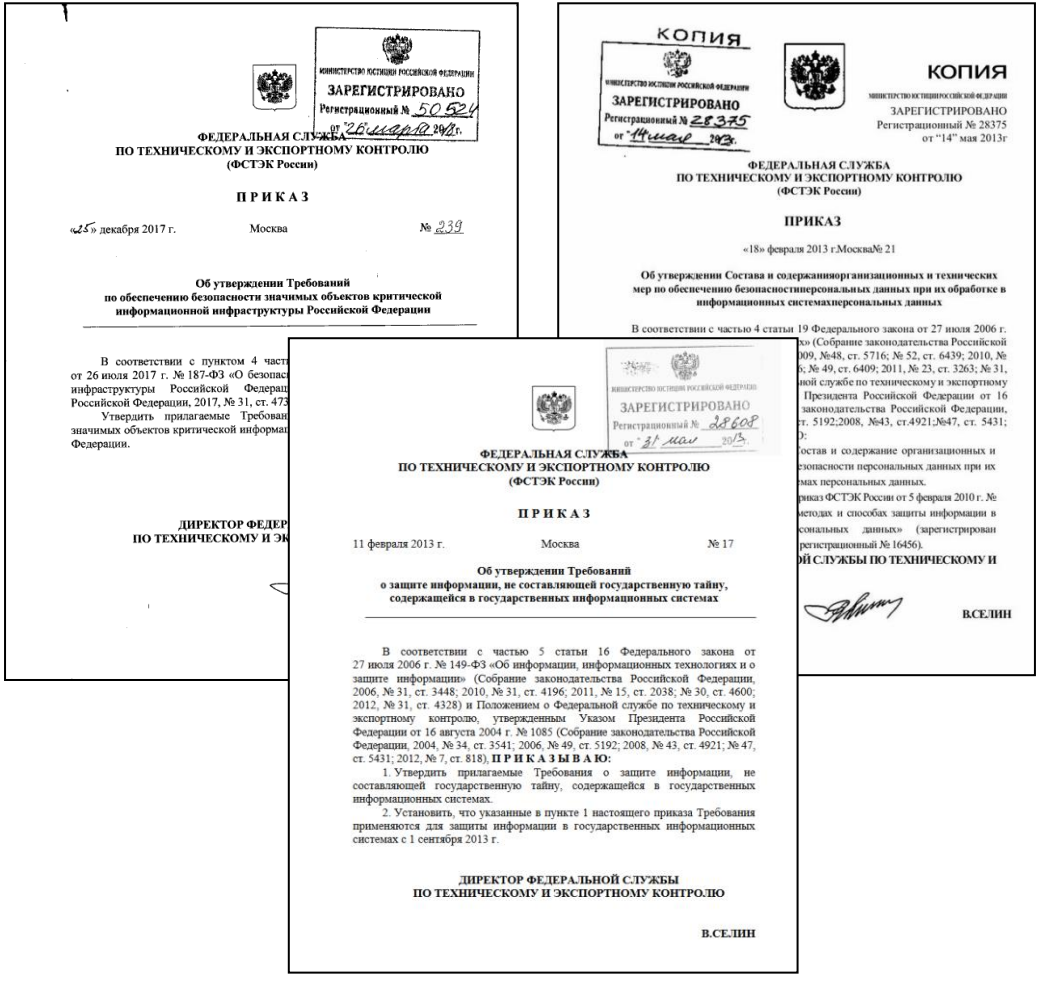
Для целей настоящего Федерального закона используются следующие основные понятия:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации;
- Федеральный закон от 06.04.2011 № 63 «Об электронной подписи».

Руководящие документы ФСТЭК России

- Приказ ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
- Приказ ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»
- Приказ ФСТЭК от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»



ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" декабря 2017 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«25» декабря 2017 г. Москва № 239

Об утверждении Требований
по обеспечению безопасности значимых объектов критической
информационной инфраструктуры Российской Федерации

КОПИЯ

ЗАРЕГИСТРИРОВАНО
Регистрационный № 28375
от "14" мая 2013г

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«18» февраля 2013 г. Москва № 21

ЗАРЕГИСТРИРОВАНО
Регистрационный № 28608
от "21" мая 2013

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

11 февраля 2013 г. Москва № 17

Об утверждении Требований
о защите информации, не составляющей государственную тайну,
содержащейся в государственных информационных системах

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818), **ПРИКАЗЫВАЮ:**

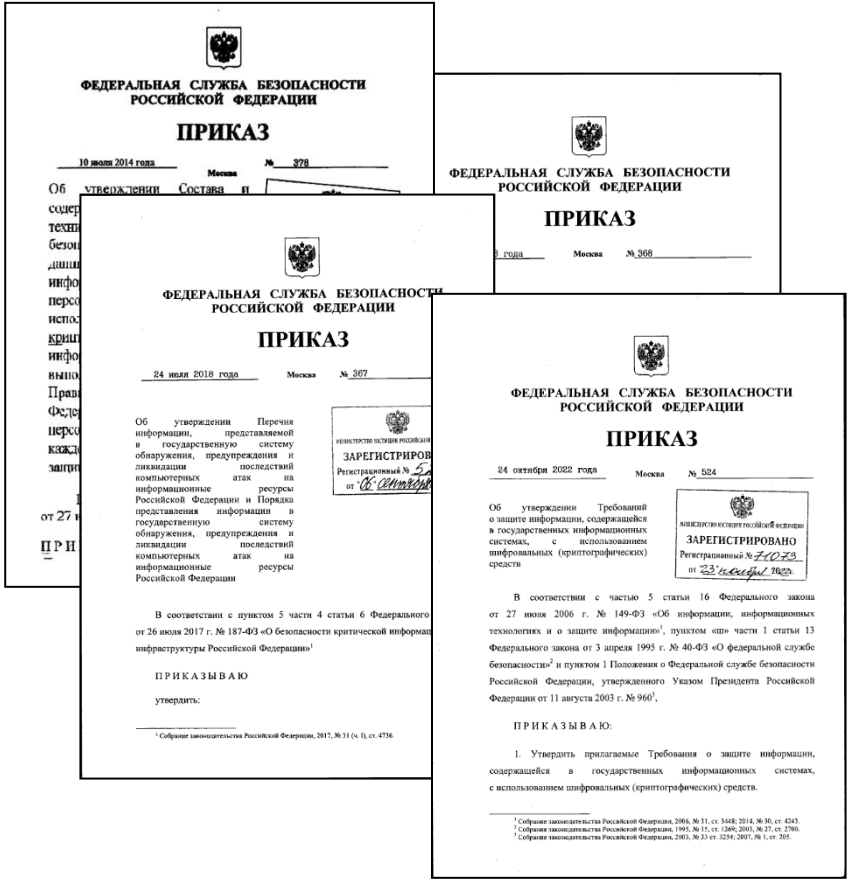
1. Утвердить прилагаемые Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

2. Установить, что указанные в пункте 1 настоящего приказа Требования применяются для защиты информации в государственных информационных системах с 1 сентября 2013 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Руководящие документы ФСБ России



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

10 июля 2014 года Москва № 378

Об утверждении Состава и

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

Москва № 368

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24 июля 2018 года Москва № 367

Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

ЗАРЕГИСТРИРОВ
Регистрационный № 5
от 6 сентября

В соответствии с пунктом 5 части 4 статьи 6 Федерального от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информ инфраструктуры Российской Федерации»[1]

П Р И К А З Ы В А Ю

утвердить:

[1] Собрание законодательства Российской Федерации, 2017, № 31 (ч. I), ст. 4736.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24 октября 2022 года Москва № 524

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств

ЗАРЕГИСТРИРОВАНО
Регистрационный № 71073
от 23 января 2023

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1], пунктом «пп» части 1 статьи 13 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»[2] и пунктом 1 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. № 960[3],

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Требования о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств.

[1] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2014, № 30, ст. 4243.
[2] Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2003, № 27, ст. 2700.
[3] Собрание законодательства Российской Федерации, 2003, № 33 ст. 3254; 2007, № 1, ст. 205.

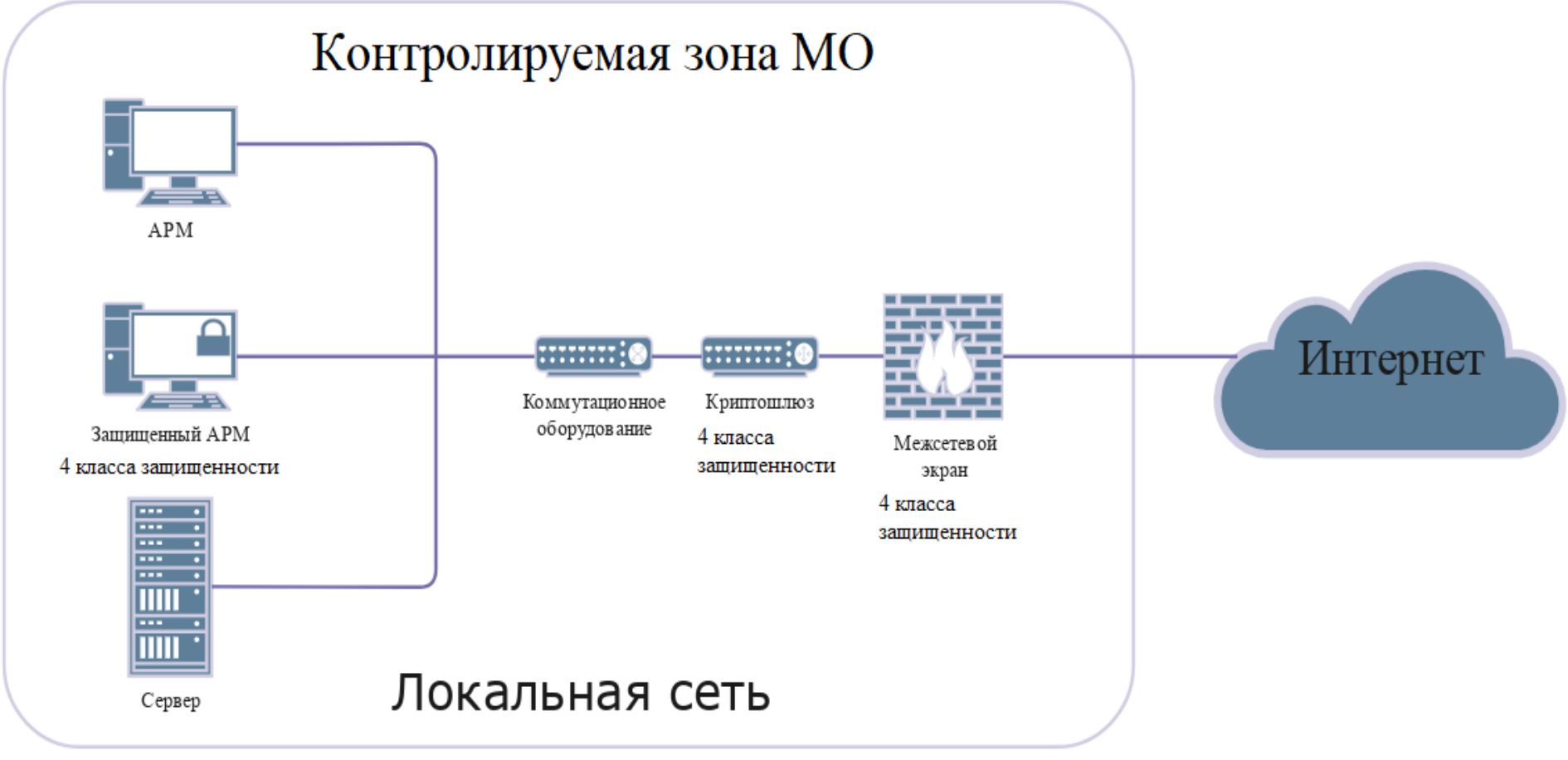
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для каждого из уровней защищенности»;

- Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»;

- Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

- Приказ ФСБ России от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в ГИС, с использованием шифровальных (криптографических) средств».

Рекомендованная схема ЛВС МО для взаимодействия с ГИС Минздрава Удмуртии



Порядок действий при подключении к ГИС Минздрава Удмуртии

1. Заключить соглашения:

– об информационном взаимодействии, осуществляемом средствами ГИС «РС ЕГИСЗ» и обеспечивающим юридически значимый документооборот медицинскими документами в электронной форме с Минздравом Удмуртии;

– о подключении к ведомственной ЗСПД Минздрава Удмуртии с БУЗ УР «РМИАЦ МЗ УР» **или** об установлении защищенного межсетевого взаимодействия (в случае, если у организации есть своя ЗСПД)

– о конфиденциальности (соглашение заключается с каждым участником информационного взаимодействия, в случае если между участниками происходит обмен конфиденциальной информацией).

2. Разработать пакет организационно-распорядительной документации по ИБ;

3. Закупочные процедуры + настройка СЗИ:

– сертифицированный ФСБ России криптошлюз для доступа в ЗСПД Минздрава Удмуртии (ПО или ПАК) (4 класс защищенности);

– сертифицированный ФСТЭК России межсетевой экран (МЭ) (4 класс защищенности);

– сертифицированное ФСТЭК России антивирусное ПО (АВЗ) (2 уровню доверия, 2 класса защиты);

– сертифицированное ФСТЭК России и ФСБ России средство доверенной загрузки (СДЗ) (2 уровень доверия, применяется в ИСПДн до 1 уровня защищенности 1 включительно и в ГИС до 1-го класса защищенности включительно);

– сертифицированное ФСТЭК России средство от несанкционированного доступа (НСД) (4 уровню доверия, применяется в ИСПДн до 1 уровня защищенности включительно, ГИС до 1 класса включительно);

– сертифицированное ФСБ России средство проверки электронной подписи (ЭП) (СКЗИ КС2);

– сертифицированное ФСТЭК России и ФСБ России средство обнаружения вторжений (СОВ) (4 уровень доверия, 4 класс защиты СОВ).

Рекомендуемый перечень ОРД:

1. Политика в отношении обработки и защиты персональных данных;
2. Политика информационной безопасности;
3. Политика по организации парольной защиты;
4. Политика об организации антивирусной защиты;
5. Политика по организации резервного копирования;
6. Политика в отношении учета и хранения машинных носителей;
7. Регламент доступа в серверное помещение (приложение: перечень лиц, допущенных в серверное помещение);
8. Регламент технического обслуживания оборудования, размещенного в серверном помещении;
9. Техническое задание на создание системы защиты информации информационной системы персональных данных;
10. Модель угроз безопасности информации при ее обработке в информационной системе персональных данных;
11. Приказ о вводе в эксплуатацию информационной системы персональных данных;
12. Приказ о назначении комиссии по классификации информационной системы персональных данных;
13. Акт классификации информационной системы персональных данных;
14. Положение о разрешительной системе доступа пользователей к информационным ресурсам информационной системы персональных данных (матрица доступа);
15. Приказ о назначении структурного подразделения ответственного за реагирование на инциденты информационной безопасности (приложение: регламент реагирования на инциденты информационной безопасности);
16. Приказ о назначении ответственного за организацию обработки персональных данных;
17. Приказ о назначении ответственного за защиту персональных данных (приложение: Перечень конфиденциальной информации (персональных данных), подлежащей защите);
18. Приказ о назначении администратора безопасности (приложение: инструкция администратора безопасности);
19. Приказ о назначении системного администратора (приложение: инструкция системного администратора);
20. Приказ об утверждении инструкции пользователя (приложения: 1) инструкция пользователя, 2) перечень лиц, допущенных к обработке персональных данных);
21. Приказ об установлении границ контролируемой зоны (приложения: 1) Положение о контролируемой зоне; 2) Схемы помещений, которые входят в границы контролируемой зоны;
22. Приказ об утверждении перечня лиц, допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ) (приложения: 1) перечень лиц, допущенных к СКЗИ, инструкция пользователя СКЗИ);
23. Приказ об утверждении регламента доступа в помещения, в которых размещены, хранятся и используются средства криптографической защиты информации, носители ключевой, аутентифицирующей и парольной информации (приложения: 1) Перечень лиц, допущенных в защищаемые помещения, 2) Регламент доступа в защищаемые помещения).

Важно! Названия документов, приведенные в перечне, носят рекомендательный характер. Медицинская организация при разработке индивидуального перечня организационно-распорядительной документации вправе указывать иные названия документов. Существенным условием при разработке документов является смысловая нагрузка и концептуальность информации, которая будет изложена в приказах, инструкциях, регламентах, положениях и. т.д.

РМИАЦ

СПАСИБО ЗА ВНИМАНИЕ!

QR-визитка