

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СТАВРОПОЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

ПРИНЯТО

Решением Ученого совета университета
от 31 января 2018 г., протокол № 6



В.И. Кошель

Приказ от 31.01.2018 № 79-ОД

**ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОРГАНИЗАЦИИ ОХРАНЫ СПЕЦИАЛЬНЫХ ПОМЕЩЕНИЙ
И РАБОТЫ С ХРАНИЛИЩАМИ**

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о порядке организации охраны специальных помещений и работы с хранилищами (далее – Положение) разработано в соответствии со статьей 19 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», в целях исполнения требований постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 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».

1.2. Положение определяет требования к размещению, оборудованию, охране, организации режима в специальных помещениях (далее – спецпомещения) в федеральном государственном бюджетном образовательном учреждении высшего образования «Ставропольском государственном медицинском университете» Министерства здравоохранения Российской Федерации (далее – ФГБОУ ВО СтГМУ Минздрава России) и порядку доступа в такие помещения, а также обеспечению сохранности носителей информации конфиденциального характера, технических средств, средств защиты информации, средств криптографической защиты информации, в том числе ключевых документов.

1.3. Целями принятия настоящего Положения являются:

– исключение возможности неконтролируемого проникновения или пребывания в помещениях ФГБОУ ВО СтГМУ Минздрава России посторонних лиц, а также просмотра посторонними лицами ведущихся там работ;

– исключение несанкционированного доступа к носителям информации конфиденциального характера, подлежащей защите в ФГБОУ ВО СтГМУ Минздрава России, в хранилища индивидуального пользования, к средствам защиты информации, средствам криптографической защиты информации, в том числе к ключевым документам.

1.4. Действие настоящего Положения распространяется на всех работников ФГБОУ ВО СтГМУ Минздрава России.

1.5. Перечень сведений конфиденциального характера, подлежащих защите в ФГБОУ ВО СтГМУ Минздрава России утверждается приказом ректора.

1.6. Ответственным за организацию охраны спецпомещений и работы с хранилищами ФГБОУ ВО СтГМУ Минздрава России является отдел по обеспечению комплексной безопасности управления по стратегическому развитию (далее – Ответственное структурное подразделение).

1.7. Работники ФГБОУ ВО СтГМУ Минздрава России несут ответственность за соблюдение порядка доступа в спецпомещения, за обеспечение сохранности носителей информации конфиденциального характера, средств криптографической защиты информации, в том числе ключевых документов, и исключение несанкционированного доступа к таким носителям и средствам.

1.8. Во всех случаях, не урегулированных настоящим Положением или другими нормативными документами ФГБОУ ВО СтГМУ Минздрава России, необходимо руководствоваться действующим законодательством Российской Федерации.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Для целей настоящего Положения используются следующие термины и определения:

1) объект – помещения ФГБОУ ВО СтГМУ Минздрава России, в том числе специальные помещения ФГБОУ ВО СтГМУ Минздрава России;

2) пропускной режим – порядок, обеспечиваемый совокупностью мероприятий и правил, исключающих возможность бесконтрольного входа (выхода) лиц на объект (с объекта);

3) специальные помещения (спецпомещения) – помещения, в которых проводятся работы с информацией конфиденциального характера, подлежащей защите в ФГБОУ ВО СтГМУ Минздрава России, хранятся носители такой информации и обеспечивается ее сохранность, помещения, в которых установлены средства криптографической защиты информации или хранятся ключевые документы к ним, а также помещения, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, переговоров); архивы, места расположения серверного и коммутационного оборудования;

4) дежурная охрана – работники охранного предприятия, выполняющие обязательства по обеспечению безопасности ФГБОУ ВО СтГМУ Минздрава России на основании заключенного государственного контракта на оказание охранных услуг;

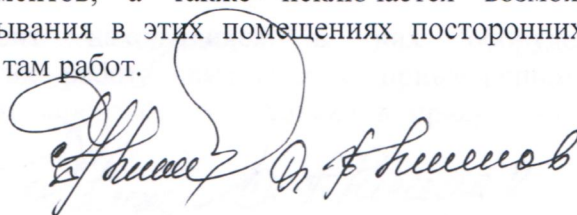
5) пост охраны – строго определенное рабочее место дежурного охранника и часть объекта, находящаяся в зоне его ответственности, включая участки, охраняемые при помощи технических средств;

6) СКЗИ – сертифицированные Федеральной службой безопасности Российской Федерации средства криптографической защиты конфиденциальной информации;

2.2. Конфиденциальная информация – информация (в т. ч. персональные данные), доступ к которой ограничен федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства, за исключением информации, составляющей государственную тайну, и в отношении которой обязательным является требование соблюдения конфиденциальности такой информации.

III. ОРГАНИЗАЦИЯ ОХРАНЫ СПЕЦПОМЕЩЕНИЙ

3.1. Для спецпомещений ФГБОУ ВО СтГМУ Минздрава России организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации конфиденциального характера, средств защиты информации, средств криптографической защиты информации и ключевых документов, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц, просмотра посторонними лицами ведущихся там работ.



3.2. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время.

3.3. Требования для спецпомещений, где установлены СКЗИ или хранятся ключевые документы к ним:

– окна, расположенные на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещение посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в эти спецпомещения;

– размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища;

– в спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, устанавливающих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

3.4. Конфиденциальная информация на бумажных носителях должна находиться в недоступном для посторонних лиц месте. Бумажные носители и электронные носители конфиденциальной информации хранятся в металлических шкафах, оборудованных опечатывающими устройствами.

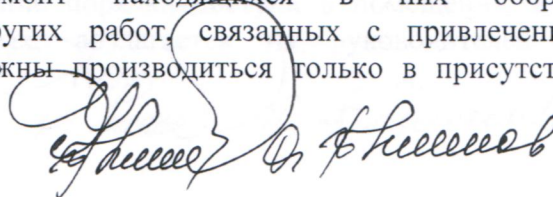
3.5. Ответственное структурное подразделение совместно с Уполномоченным по информационной безопасности и обеспечению защиты конфиденциальной информации осуществляет периодический контроль за состоянием технических средств охраны и общий контроль в рамках исполнения требований настоящего Положения.

3.6. При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Положение хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает: ответственный за организацию обработки персональных данных, ответственный пользователь СКЗИ.

3.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации. Ответственный пользователь СКЗИ и ответственный за организацию обработки персональных данных должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации.

3.8. Для предотвращения просмотра извне спецпомещений их окна должны быть защищены шторами (жалюзи). Двери спецпомещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода работников и посетителей.

3.9. Уборка спецпомещений, ремонт находящихся в них оборудования и технических средств, выполнение других работ, связанных с привлечением лиц, не имеющих доступа в помещения, должны производиться только в присутствии лиц,



допущенных в спецпомещения. Бесконтрольное нахождение в помещении посетителей, или работников не включенных в список лиц, допущенных в соответствующие помещения запрещено.

3.10. Перечень лиц, допущенных к работе в специальных помещениях утверждается приказом ректора университета.

3.11. Вскрытие и закрытие (опечатывание) спецпомещений производится работниками, имеющими право доступа в данные помещения.

3.12. Право самостоятельного входа в спецпомещения имеют только работники, непосредственно работающие в данном помещении. Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

3.13. Перед закрытием спецпомещений по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

- убрать бумажные носители и электронные носители конфиденциальной информации в шкафы/хранилища, закрыть и опечатать шкафы/хранилища;
- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;
- закрыть окна;
- подключить охранную сигнализацию (при наличии охранной сигнализации в спецпомещении).

3.14. Перед открытием спецпомещений, работники, имеющие право доступа в спецпомещения, обязаны:

- провести внешний осмотр с целью установления целостности двери, замка, пломбы или опечатывающего бланка;
- открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

3.15. В целях реализации требований по защите информации в ФГБОУ ВО СтГМУ Минздрава России утверждается комиссия.

В состав комиссии включаются:

ответственное лицо (при наличии);

руководитель соответствующего структурного подразделения;

ответственный пользователь СКЗИ (при наличии);

начальник отдела комплексной безопасности или должностное лицо его замещающее;

уполномоченный по информационной безопасности и обеспечению защиты конфиденциальной информации, ответственный за организацию обработки персональных данных.

3.16. При обнаружении признаков, указывающих на возможное проникновение посторонних лиц в спецпомещения, последние не вскрываются. О случившемся немедленно ставится в известность ректор ФГБОУ ВО СтГМУ Минздрава России. Одновременно принимаются меры по охране данного помещения. Специальной комиссией (п. 3.15 раздела III) составляется акт (приложение 1).

3.17. Вскрытие спецпомещений ФГБОУ ВО СтГМУ Минздрава России без лиц, допущенных в помещения производится комиссией, определенной в соответствии с п. 3.15 раздела III настоящего Положения, в составе не менее двух человек, которая составляет акт о вскрытии с указанием в нем должностей и фамилий лиц, вскрывших помещение, времени и причины (принятие экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещения и т.д.) вскрытия (приложение 2).

3.18. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей отделов, обрабатывающих персональные данные.

IV. ОРГАНИЗАЦИЯ И ПРЯДОК РАБОТЫ С ХРАНИЛИЩАМИ

4.1. Для хранения носителей информации конфиденциального характера, ключевых документов, эксплуатационной и технической документации, устанавливающих носителей средств криптографической защиты информации спецпомещения оборудуются надежно запираемыми хранилищами индивидуального пользования, оборудованными приспособлениями для опечатывания. Хранилища, находящиеся в помещениях ФГБОУ ВО СтГМУ Минздрава России, вносятся в Журнал учета (приложение 3).

4.2. На лицевой стороне хранилища по центру помещается бирка установленного образца (приложение 4). Она включает в себя номер хранилища, Ф.И.О. лица, за которым закреплено хранилище (ответственного за хранение), и номер его личной печати. Бирка удостоверяется личной подписью уполномоченного по информационной безопасности и обеспечению защиты конфиденциальной информации.

4.3. Рабочие ключи от хранилищ выдаются работникам ФГБОУ ВО СтГМУ Минздрава России под подпись в Журнале учета хранилищ (сейфов).

4.4. Дубликаты ключей от хранилищ передаются в опечатанной упаковке Ответственному лицу, который обеспечивает их сохранность и недоступность посторонним лицам. Дубликат ключа от хранилища Ответственного лица передается в опечатанной упаковке ректору ФГБОУ ВО СтГМУ Минздрава России, который обеспечивает его хранение в сейфе.

4.5. Все экземпляры ключей от хранилищ оснащаются бирками соответствующего образца, содержащими информацию, позволяющую однозначно идентифицировать ключи.

4.6. По окончании рабочего дня хранилища запираются и опечатываются таким образом, чтобы исключить возможность снятия печати без повреждения оттиска печати. Опечатывать и вскрывать хранилища вправе только работники, ответственные за соответствующие хранилища.

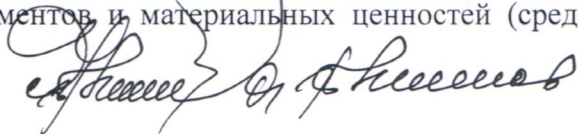
4.7. При вскрытии хранилища работник, ответственный за хранение, обязан убедиться в сохранности оттиска печати.

4.8. При обнаружении нарушения целостности оттисков или других признаков, указывающих на возможное проникновение посторонних лиц в хранилища, последние не вскрываются. О случившемся немедленно ставится в известность Ректор ФГБОУ ВО СтГМУ Минздрава России. Одновременно принимаются меры по охране места происшествия, на которое не допускаются посторонние лица. Комиссией, определенной в соответствии с п. 3.15 раздела III настоящего Положения, в составе не менее двух человек составляется акт (приложение 1).

4.9. Вскрытие хранилищ без лиц, ответственных за них, производится комиссией определенной в соответствии с п. 3.15 раздела III настоящего Положения, в составе не менее двух человек, которая составляет акт о вскрытии с указанием в нем должностей и фамилий лиц, вскрывших хранилища, номера помещения, времени и причины вскрытия (принятие экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещения и т.д.) номеров печатей, которыми ранее были опечатаны и вновь опечатаны хранилища (приложение 2).

4.10. Все носители информации конфиденциального характера, ключевые документы, эксплуатационная и техническая документации, устанавливающие носители средств криптографической защиты информации в обязательном порядке заносятся во внутреннюю опись документов и материальных ценностей (средств), находящихся в хранилище (приложение 5).

4.11. При необходимости временной выдачи документов и материальных ценностей (средств), находящихся в хранилище, другому работнику факт такой выдачи должен фиксироваться в реестре учета выдачи документов и материальных ценностей (средств), находящихся в хранилище (приложение 6).

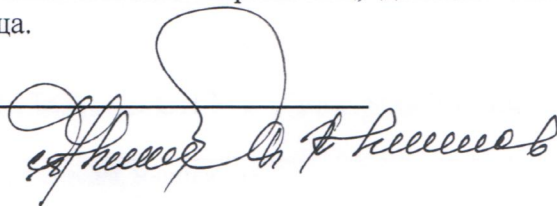


4.12. Об утрате ключей от хранилищ, личных номерных печатей работники немедленно официально уведомляют Уполномоченного по информационной безопасности и обеспечению защиты конфиденциальной информации ФГБОУ ВО СтГМУ Минздрава России.

4.13. При утрате ключа от хранилища до замены замка или смены секрета замка хранить документы и материальные ценности (средства) в нем запрещено.

4.14. При увольнении, уходе в отпуск, убытии в командировку, а также в случае отсутствия по другой причине, работник ФГБОУ ВО СтГМУ Минздрава России передает находящиеся у него ключи от хранилища, находящиеся в нем носители информации конфиденциального характера, ключевые документы, эксплуатационную и техническую документацию, устанавливающие носители средств криптографической защиты информации, материальные ценности по указанию ректора ФГБОУ ВО СтГМУ Минздрава России, другому работнику университета или сдает их на хранение Уполномоченному по информационной безопасности и обеспечению защиты конфиденциальной информации по акту приема-передачи.

4.15. Печати, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за эти хранилища.



Приложение № 1
к Положению о порядке организации
охраны специальных помещений и работы
с хранилищами

ФГБОУ ВО СтГМУ Минздрава России

ОКУД

Код
Код
01962907

Форма по

по ОКПО

АКТ

Номер документа	Дата составления

ИБ

Об обнаружении несанкционированного
проникновения в специальное помещение

Мы, нижеподписавшиеся, работники ФГБОУ ВО СтГМУ Минздрава России

(должность, фамилия, инициалы)

(должность, фамилия, инициалы)

(должность, фамилия, инициалы)

в соответствии с п. 15 раздела II Положения о порядке организации охраны специальных помещений и работы с хранилищами составили настоящий акт о том, что в (на) специальном помещении (хранилище):

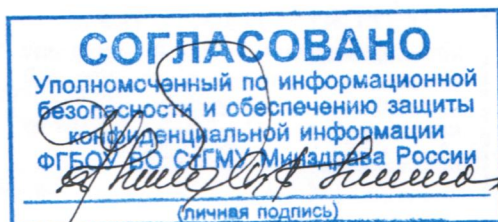
(номер помещения, хранилища)

ФГБОУ ВО СтГМУ Минздрава России обнаружены признаки проникновения (нарушена целостность оттиска печати, иные следы проникновения).

При вскрытии указанного помещения (хранилища) установлено, что

(указываются выявленные недостатки)

Члены комиссии:



Приложение № 2
к Положению о порядке организации охраны
специальных помещений и работы
с хранилищами

ОКУД	Код	Форма по
	Код	по ОКПО
	01962907	

ФГБОУ ВО СтГМУ Минздрава России

АКТ

Номер документа	Дата составления

ИБ

О вскрытии специального помещения

Мы, нижеподписавшиеся, работники ФГБОУ ВО СтГМУ Минздрава России

_____ (должность, фамилия, инициалы)

_____ (должность, фамилия, инициалы)

_____ (должность, фамилия, инициалы)

в соответствии с п. 16 раздела II Положения о порядке организации охраны специальных помещений и работы с хранилищами составили настоящий акт о том, что специальное помещение (хранилище):

_____ (номер помещения, хранилища)

ФГБОУ ВО СтГМУ Минздрава России было вскрыто

_____ (указать время и причины вскрытия)

Вскрытое помещение (хранилище) было вновь опечатано:

_____ (указать номер личной печати или бланка)

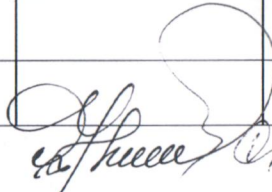
Члены комиссии:



Приложение № 3
к Порядку организации охраны
специальных помещений и работы
с хранилищами, утвержденному
приказом от 31.01.2018 № 49-08

Ж У Р Н А Л
УЧЕТА ХРАНИЛИЩ (СЕЙФОВ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО
ОБРАЗОВАНИЯ «СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Регист рацион ный номер	Наименование хранилища (сейф, металлический шкаф, кладовая, спец. хранилище)	Заводской, инвентарный номер хранилища	Местонахож дение хранилища (подразделе ние, номер комнаты)	Фамилия, инициалы ответственного за хранилище	Количество комплектов ключей и их номера	Расписка ответственного за хранилище в получении ключа и дата	Расписка в обратном приеме ключа и дата	Примечание
1	2	3	4	5	6	7	8	9


С. С. Шенников

Ф О Р М А
БИРКИ НА ХРАНИЛИЩЕ (СЕЙФ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ХРАНИЛИЩЕ (СЕЙФ) N _____

Ответственное должностное лицо (Ф.И.О., должность, структурное
подразделение):

Опечатывается (пломбируется) печатью N _____
Дата постановки на учет « ____ » _____ 20__ г.

Уполномоченный по информационной
безопасности и обеспечению защиты
конфиденциальной информации

Ф.И.О.

М.П.



Форма	Код	по ОКУД
	Код	по ОКПО
	01962907	

ФГБОУ ВО СтГМУ Минздрава России

ВНУТРЕННЯЯ ОПИСЬ
ДОКУМЕНТОВ И МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ (СРЕДСТВ) НАХОДЯЩИХСЯ
В ХРАНИЛИЩЕ (СЕЙФЕ)

Регистрац ионный номер	Дата постановки на учет

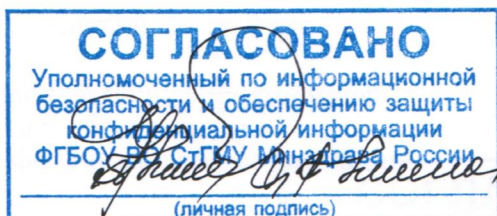
№ п/п	Наименование	Инвентарный (заводской номер)	Отметка об изъятии документа и его местонахождение	Примечание
1	2	3	4	5

Ответственное должностное лицо

Ф.И.О.

Уполномоченный по информационной
безопасности и обеспечению
защиты конфиденциальной информации

Ф.И.О.



Приложение № 6
к Положению о порядке организации охраны
специальных помещений и работы
с хранилищами

Форма

Код
Код
01962907

по ОКУД

по ОКПО

ФГБОУ ВО СтГМУ Минздрава России

РЕЕСТР

УЧЕТА ВЫДАЧИ ДОКУМЕНТОВ И МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ (СРЕДСТВ)
НАХОДЯЩИХСЯ В ХРАНИЛИЩЕ (СЕЙФЕ)

Регистрационный номер	Дата постановки на учет

Дата выдачи	Кому выдан (подразделение, фамилия исполнителя)	Название документа, средства (учетный номер)	Расписка в получении или ознакомлении, дата	Расписка в обратном приеме, дата
1	2	3	4	5

Ответственное должностное лицо

Ф.И.О.

Уполномоченный по информационной
безопасности и обеспечению
защиты конфиденциальной информации

Ф.И.О.

