

# Приложение № 1

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

## ПЕРЕЧЕНЬ

структурных подразделений главного управления ЗАГС Рязанской области

№ п/п	Структурные подразделения главного управления ЗАГС Рязанской области	Местонахождение (фактический адрес)
1	Главное управление ЗАГС Рязанской области	г. Рязань, ул. Полонского, д.1/54
2	Отдел накопления, хранения и выдачи документов	г. Рязань, ул. Ленина д.57
3	Территориальный отдел ЗАГС № 1 по г. Рязани	г. Рязань, Народный бульвар д.16
4	Территориальный отдел ЗАГС № 2 по г. Рязани	г. Рязань, ул. Семинарская д.35
5	Территориальный отдел ЗАГС № 3 по г. Рязани	г. Рязань, ул. Гагарина д.83а
6	Территориальный отдел ЗАГС № 4 по г. Рязани	г. Рязань, ул. Ленина д.57
7	Территориальный отдел ЗАГС № 5 по г. Рязани	г. Рязань, Скорбящинский проезд д.4
8	Территориальный отдел ЗАГС по Рязанскому району	г. Рязань, п. Соколовка, ул. Связи д.11
9	Территориальный отдел ЗАГС по г. Касимову и Касимовскому району	Рязанская область, г. Касимов, ул. Советская д.4
10	Территориальный отдел ЗАГС по Рязжскому району	Рязанская область, г. Рязжск, ул. Горького д.5
11	Территориальный отдел ЗАГС по г. Сасово и Сасовскому району	Рязанская область, г. Сасово, мкр. Северный, д.1
12	Территориальный отдел ЗАГС по г. Скопину и Скопинскому району	Рязанская область, г. Скопин, пл. Ленина д.1
13	Территориальный отдел по Ермишинскому району	Рязанская область, р.п. Ермишь, ул. Московская д.63
14	Территориальный отдел по Захаровскому району	Рязанская область, с. Захарово, ул. Центральная д.190
15	Территориальный отдел по Кадомскому району	Рязанская область, р.п. Кадом, ул. Ленина д.37
16	Территориальный отдел по Клепиковскому району	Рязанская область, г. Спас-Клепики, ул. Свободы д.3

№ п/п	Структурные подразделения главного управления ЗАГС Рязанской области	Местонахождение (фактический адрес)
17	Территориальный отдел по Кораблинскому району	Рязанская область, г. Кораблино, ул. К. Маркса, д.3
18	Территориальный отдел по Милославскому району	Рязанская область, р.п. Милославское, ул. Центральная д.49
19	Территориальный отдел по Михайловскому району	Рязанская область, г. Михайлов, ул. Победы, д.3
20	Территориальный отдел по Александро- Невскому району	Рязанская область, р.п. Александро-Невский, ул. Советская д.44
21	Территориальный отдел по Пителинскому району	Рязанская область, р.п. Пителино, пл. Советская д.8
22	Территориальный отдел по Пронскому району	Рязанская область, р.п. Пронск, ул. Первомайская д.32
23	Территориальный отдел по г. Новомичуринску	Рязанская область, Пронский район, г. Новомичуринск д.26д
24	Территориальный отдел по Путятинскому району	Рязанская область, с. Путятино, ул. Ворошилова д.36
25	Территориальный отдел по Рыбновскому району	Рязанская область, г. Рыбное, ул. Почтовая, д.8
26	Территориальный отдел по Сапожковскому району	Рязанская область, р.п. Сапожок, ул. Советская, д.8
27	Территориальный отдел по Сараевскому району	Рязанская область, р.п. Сарай, ул. Ленина, д.157
28	Территориальный отдел по Спасскому району	Рязанская область, г. Спасск-Рязанский, ул. Свердлова, д.63а
29	Территориальный отдел по Старожиловскому району	Рязанская область, р.п. Старожилово, ул. Толстого, д.41
30	Территориальный отдел по Ухоловскому району	Рязанская область, р.п. Ухолово, ул. Ленина, д.22
31	Территориальный отдел по Чучковскому району	Рязанская область, р.п. Чучково, ул. Ленина, д.10
32	Территориальный отдел по Шацкому району	Рязанская область, г. Шацк, ул. Интернациональная, д.14а
33	Территориальный отдел по Шиловскому району	Рязанская область, р.п. Шилово, пл. Советская д.11

## **ИНСТРУКЦИЯ**

### **администратора государственной информационной системы главного управления ЗАГС Рязанской области**

#### **1 Общие положения**

1.1 Инструкция Администратора государственной информационной системы (далее – ГИС) главного управления ЗАГС Рязанской области (далее – Инструкция) определяет функции, права и обязанности Администратора ГИС по вопросам обеспечения правильности использования и нормального функционирования ГИС.

1.2 Администратор ГИС назначается из числа сотрудников главного управления ЗАГС Рязанской области и отвечает за обеспечение устойчивой работоспособности элементов ГИС.

1.3 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима безопасности информации и не исключает обязательного выполнения их требований.

#### **2 Должностные обязанности**

2.1 Администратор ГИС обязан:

2.1.1 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.1.2 Обеспечивать установку, настройку и своевременное обновление элементов ГИС:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.1.3 Обеспечивать работоспособность элементов ГИС и локальной вычислительной сети.

2.1.4 Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.1.5 Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.1.6 В случае отказа работоспособности технических средств и программного обеспечения элементов ГИС, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.1.7 Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

2.1.8 Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.1.9 Информировать Ответственного за организацию обработки информации о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ГИС главного управления ЗАГС Рязанской области.

2.1.10 Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ГИС главного управления ЗАГС Рязанской области или средств защиты.

2.1.11 Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.1.12 Присутствовать при выполнении технического обслуживания элементов ГИС главного управления ЗАГС Рязанской области, сторонними физическими людьми и организациями.

2.1.13 Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью ликвидации их последствий, в пределах возложенных на него функций.

2.1.14 Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных и аварийных ситуаций.

2.1.15 В кратчайшие сроки принимать меры по восстановлению работоспособности компонентов ГИС главного управления ЗАГС Рязанской области.

2.1.16 Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

### 3 Права

3.1 Администратор ГИС имеет право:

3.1.1 Участвовать в анализе ситуаций, касающихся функционирования ГИС главного управления ЗАГС Рязанской области и расследования фактов несанкционированного доступа.

3.1.2 Требовать прекращения обработки информации в случае нарушения установленного порядка работы или нарушения функционирования средств и систем защиты ГИС главного управления ЗАГС Рязанской области.

## 4 Ответственность

4.1 Администратор ГИС несет ответственность:

4.1.1 За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2 За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3 За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

## **ИНСТРУКЦИЯ**

### **администратора информационной безопасности государственной информационной системы главного управления ЗАГС Рязанской области**

#### **1 Общие положения**

1.1 Инструкция Администратора информационной безопасности государственной информационной системы (далее – ГИС) главного управления ЗАГС Рязанской области (далее – Инструкция) определяет функции, права и обязанности Администратора информационной безопасности (далее – Администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов на автоматизированных рабочих местах (далее – АРМ) ГИС главного управления ЗАГС Рязанской области.

1.2 Администратор ИБ назначается из числа сотрудников главного управления ЗАГС Рязанской области и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации (СЗИ).

1.3 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4 Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации на АРМ пользователей (за исключением информации, закрытой с использованием средств криптозащиты). Он несет ответственность за реализацию принятой в Администрации политики безопасности.

#### **2 Обязанности Администратора ИБ**

2.1 Администратор ИБ обязан:

2.1.1 Знать перечень установленных АРМ ГИС главного управления ЗАГС Рязанской области и перечень задач, решаемых с их использованием.

2.1.2 Осуществлять учет и периодический контроль за составом и полномочиями пользователей АРМ ГИС главного управления ЗАГС Рязанской области.

2.1.3 Осуществлять оперативный контроль за работой пользователей защищенных АРМ ГИС главного управления ЗАГС Рязанской области, анализировать содержимое системных журналов всех АРМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов АРМ и надлежащий режим хранения данных архивов.

2.1.4 Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на АРМ ГИС главного управления ЗАГС Рязанской области специальных технических средств защиты информации от несанкционированного доступа (далее – СЗИ от НСД).

2.1.5 Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, устанавливать и осуществлять настройку средств защиты на АРМ ГИС главного управления ЗАГС Рязанской области.

2.1.6 Периодически проверять состояние используемых СЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.7 Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.

2.1.8 Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ГИС и осуществления НСД к информации и техническим средствам АРМ.

2.1.9 Докладывать руководству главного управления ЗАГС Рязанской области обеспечения информационной безопасности об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ.

2.1.10 По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты информации от НСД, установленных на АРМ ГИС главного управления ЗАГС Рязанской области.

2.1.11 Проводить занятия с сотрудниками по правилам работы на АРМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

2.2 Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.3 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

2.4 Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций.

2.5 В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ГИС главного управления ЗАГС Рязанской области.

2.6 Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

### **3 Права Администратора ИБ**

**3.1** Администратор ИБ имеет право:

**3.1.1** Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ГИС главного управления ЗАГС Рязанской области.

**3.1.2** Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ГИС главного управления ЗАГС Рязанской области при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

**3.1.3** Вносить свои предложения по совершенствованию мер защиты в ГИС главного управления ЗАГС Рязанской области.

### **4 Ответственность Администратора ИБ**

**4.1** На Администратора ИБ возлагается персональная ответственность за программно-технические и шифровальные средства защиты информации, средства вычислительной техники, информационно-вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним приказом, и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

**4.2** Администратор ИБ несет ответственность по действующему законодательству за разглашение сведений, составляющих (государственную, банковскую, коммерческую) тайну, и сведений ограниченного распространения, ставших известными ему по роду работы.



## **ИНСТРУКЦИЯ**

### **пользователя государственной информационной системы главного управления ЗАГС Рязанской области**

#### **1 Общие положения**

1.1 Инструкция пользователя государственной информационной системы (далее – ГИС) главного управления ЗАГС Рязанской области (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей ГИС, в которой обрабатывается конфиденциальная информация.

1.2 Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации, обрабатываемой с использованием средств автоматизации.

1.3 В настоящей Инструкции используются следующие понятия и определения:

1.3.1 Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.3.2 База данных – объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

1.3.3 Информация – сведения (сообщения, данные) независимо от формы их представления.

1.3.4 Информационная система – совокупность содержащихся в базах данных информационных ресурсов и обеспечивающих их обработку информационных технологий и технических средств.

1.3.5 Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность защищаемой информации. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь) – несанкционированное сообщение пароля другому лицу; утеря бумажного или машинного носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется.

1.3.6 Конфиденциальность информации – обязательное для соблюдения лицом, получившим доступ к информации, требование не допускать ее распространение.

1.3.7 Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности информации, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.

1.3.8 Распространение информации – действия, направленные на раскрытие информации определенному лицу или определенному кругу лиц.

1.3.9 Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в ГИС.

1.3.10 Утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем.

1.3.11 Электронная вычислительная машина ГИС (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав ГИС. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.

## 2 Обязанности пользователя

2.1 Пользователь ГИС обязан:

2.1.1 Хранить в тайне информацию, ставшую ему известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать Ответственного за организацию обработки информации, Администратора ГИС или Администратора ИБ ГИС.

2.1.2 Знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах в соответствии с Инструкциями, требованиями, регламентирующими функционирование установленных средств защиты.

2.1.3 Хранить в тайне свой пароль доступа в ГИС главного управления ЗАГС Рязанской области, а также информацию о системе защиты, установленной в ГИС главного управления ЗАГС Рязанской области.

2.1.4 Сдавать средства аутентификации и идентификации средств защиты информации (iButton, токены и т.п.) Администратору ИБ ГИС после завершения работы на АРМ ГИС.

2.1.5 Использовать для работы, только учтенные съемные накопители информации (компакт диски, флеш-накопители и т.д.).

2.1.6 В случае необходимости сообщать о необходимости обновления антивирусных баз Администратору ИБ ГИС.

2.1.7 Немедленно ставить в известность Администратора ГИС и/или Администратора ИБ ГИС:

– в случае утери носителя с конфиденциальной информацией (в том числе персональными данными) и/или при подозрении компрометации личных почтой и паролей;

- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к ГИС;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ГИС.

2.1.8 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в ГИС главного управления ЗАГС Рязанской области технических средств защиты ставить в известность Администратора ГИС и/или Администратора ИБ ГИС.

2.2 В случае увольнения пользователь ГИС обязан вернуть все документы и материалы, относящиеся к ГИС главного управления ЗАГС Рязанской области. В том числе: отчеты, инструкции, служебную переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к ГИС главного управления ЗАГС Рязанской области, полученные в течение срока работы.

2.3 Уборка помещений должна производиться под контролем пользователя ГИС, имеющего доступ в помещение и постоянно в нем работающего.

2.3.1 Вынос технических средств ГИС главного управления ЗАГС Рязанской области, на которых проводилась обработка конфиденциальной, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с Администратором ГИС или Ответственным за организацию обработки информации запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.3.2 АРМ, используемые для работы с ГИС, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора.

2.4 Пользователю категорически запрещается:

- передавать, кому бы то ни было, устно или письменно, конфиденциальную информацию, в том числе персональные данные;
- использовать конфиденциальную информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами, содержащими конфиденциальную информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного за организацию обработки информации;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие конфиденциальную информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и ящики с документами, содержащими конфиденциальную информацию;

- использовать компоненты программного и аппаратного обеспечения ГИС в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (компакт диски, флеш-накопители и т.д.);
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Администратора ГИС или Администратора ИБ ГИС.

2.5 Принимать меры по реагированию, в случае возникновения внештатных ситуации и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

2.6 Оперативно докладывать Администратору ГИС и Администратору ИБ ГИС о случаях возникновения внештатных ситуаций и аварийных ситуаций.

2.7 В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ГИС.

2.8 Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

### **3 Права пользователя**

3.1 Пользователь имеет право:

3.1.1 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

### **4 Ответственность пользователя**

4.1 Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации. За разглашение конфиденциальной информации, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

## **ИНСТРУКЦИЯ**

**по порядку обращения с техническими средствами защиты информации,  
предназначенными для защиты информации, обрабатываемой в  
государственной информационной системе  
главного управления ЗАГС Рязанской области**

### **1 Общие положения**

1.1 Инструкция по порядку обращения с техническими средствами защиты информации, предназначенными для защиты информации, обрабатываемой в государственной информационной системе (далее – ГИС) главного управления ЗАГС Рязанской области (далее – Инструкция) регламентирует порядок обращения с техническими средствами защиты информации в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты конфиденциальной информации, обрабатываемой с использованием средств автоматизации.

1.2 Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов ФСТЭК России и ФСБ России по защите информации.

1.3 Под техническим средством защиты информации (далее – ТСЗИ) в настоящей Инструкции понимается средство защиты информации, не являющееся криптосредством.

1.4 В настоящей Инструкции используются следующие понятия и определения:

1.4.1 Доступ к информации - возможность получения информации и ее использования.

1.4.2 Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.4.3 Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, защищаемого помещения.

1.4.4 Обработка информации - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств

34

автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

1.4.5 Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.5 Для обеспечения безопасности информации при ее обработке в государственной информационной системе главного управления ЗАГС Рязанской области должны использоваться сертифицированные в системе сертификации ФСТЭК России и/или ФСБ России ТСЗИ (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

## 2 Учет ТСЗИ

2.1 Инсталлирующие ТСЗИ носители и установленные ТСЗИ подлежат поэкземпляруму учету.

2.2 Программные ТСЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные ТСЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие ТСЗИ учитываются также совместно с соответствующими аппаратными средствами.

2.3 Эксплуатационная и техническая документация к ТСЗИ подлежит поэкземпляруму учету.

2.4 ТСЗИ, а так же эксплуатационная и техническая документация к ТСЗИ должны быть упакованы в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия.

2.5 Полученные упаковки с ТСЗИ, а так же с эксплуатационной и технической документацией к ним, вскрываются Администратором ИБ ГИС. Администратор ИБ ГИС проверяет целостность упаковки и содержимого.

### 2.6 Уничтожение ТСЗИ:

2.6.1 ТСЗИ уничтожаются (утилизируются) по решению Ответственного за обработку информации в ГИС главного управления ЗАГС Рязанской области, и с уведомлением Администратора ИБ ГИС, ответственного за организацию поэкземпляруму учета ТСЗИ.

2.6.2 Намеченные к уничтожению (утилизации) ТСЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом ТСЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к ТСЗИ процедура удаления программного обеспечения ТСЗИ и они полностью отсоединены от аппаратных средств.

2.6.3 Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения ТСЗИ без ограничений.

2.7 Эксплуатационная и техническая документация к ТСЗИ уничтожается путем сжигания или с помощью любых бумагорезательных машин.

### **3 Организация режима помещений с ТСЗИ**

3.1 Размещение, специальное оборудование, охрана и организация режима в помещении, где установлены ТСЗИ (далее - режимные помещения), должны обеспечивать сохранность защищаемой информации, ТСЗИ, исключать возможность неконтролируемого проникновения или пребывания в режимном помещении посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.2 Режимное помещение выделяется с учетом размеров контролируемых зон. Помещение должно иметь прочные входные двери с замками, гарантирующими надежное закрытие помещения в нерабочее время.

3.3 Режим охраны помещения, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается Ответственным за организацию обработки информации в ГИС главного управления ЗАГС Рязанской области.

3.4 Во время отсутствия в помещении лиц, имеющих право находиться в помещении, дверь режимного помещения должна быть постоянно закрыта на замок и может открываться только для санкционированного прохода сотрудников и посетителей.

3.5 Для предотвращения просмотра извне режимных помещений их окна должны быть защищены шторами или жалюзи.

### **4 Эксплуатация хранилищ с ТСЗИ**

4.1 Инсталлирующие ТСЗИ носители, эксплуатационная и техническая документация к ТСЗИ должна храниться в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

### **5 Контроль безопасности ТСЗИ**

5.1 Текущий контроль за организацией и обеспечением функционирования ТСЗИ возлагается на Ответственного за организацию обработки информации в пределах его полномочий.

### **6 Модификация ПО и ТС**

6.1 Все изменения конфигурации технических, программных и программно-аппаратных средств защиты АРМ и серверов баз данных (БД) ГИС главного управления ЗАГС Рязанской области должны производиться только на основании заявок пользователей ГИС, согласованных с Ответственным за организацию обработки информации, на имя Администратора ГИС и/или Администратора ИБ ГИС.

6.2 Право внесения изменений в конфигурацию программно-аппаратных средств защиты ГИС предоставляется:

- в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – уполномоченному Администратору ГИС;
- в отношении программно-аппаратных средств защиты – уполномоченному Администратору ИБ ГИС.

6.3 Изменение конфигурации программно-аппаратных средств защиты АРМ и серверов БД, кроме уполномоченных сотрудников запрещено.

6.4 Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Администратором ГИС. Если АРМ или сервер относится к защищаемым рабочим станциям, то установка, снятие, и внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на АРМ осуществляется Администратором ИБ ГИС.

6.5 Подготовка модификаций программного обеспечения защищенных серверов и АРМ, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в архив эталонных дистрибутивов, и другие необходимые действия производятся Администратором ИБ ГИС.

6.6 Модификация ПО на сервере осуществляется Администратором ИБ ГИС. После установки модифицированных модулей на сервер, Администратор ИБ ГИС устанавливает защиту целостности модулей на сервере, после чего на рабочих станциях проводит антивирусный контроль.

6.7 Установка и обновление общего ПО (системного, тестового и т.п.) на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств.

6.8 Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

6.9 После установки (обновления) ПО Администратор ГИС должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с ее (его) формуляром, Администратор ИБ ГИС должен проверить работоспособность ПО и правильность настройки средств защиты.

6.10 После завершения работ по внесению изменений в состав аппаратных средств защищенного АРМ ее системный блок должен закрываться на ключ (при наличии штатных механических замков) и опечатываться (пломбироваться, защищаться специальной наклейкой) Администратором ИБ ГИС.

6.11 При изъятии АРМ из состава ГИС главного управления ЗАГС Рязанской области ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор ИБ ГИС снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках



компьютера. Факт уничтожения данных, находившихся на диске компьютера оформляется актом за подписью Администратора ИБ ГИС.

## **7 Экстренная модификация (обстоятельства форс-мажор)**

7.1 В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на АРМ. Факт внесения изменений в ПО АРМ фиксируется актом за подписями Администратора ГИС, Администратора ИБ ГИС и пользователя данной АРМ. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается сотрудник, проводивший изменения. При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, Администратор ИБ ГИС вносит необходимые корректировки в настройки системы контроля целостности ПО АРМ и сервера.

7.2 В течение следующего дня после составления акта Администратором ГИС, Администратором ИБ ГИС при участии пользователей ГИС главного управления ЗАГС Рязанской области выясняются причины и состав проведенных экстренных изменений и принимается решение о необходимости подготовки исправительной модификации ПО или восстановления ПО АРМ (сервера) с эталонной копии. Необходимость участия в разбирательстве пользователя ГИС главного управления ЗАГС Рязанской области определяется руководством. Результат разбирательства оформляется в виде согласованного решения и хранится у Администратора ГИС, копии передаются Администратору ИБ ГИС.

## **8 Ответственность**

8.1 Пользователи ГИС главного управления ЗАГС Рязанской области несут персональную ответственность за сохранность полученных ТСЗИ, эксплуатационной и технической документации к ТСЗИ, за соблюдение положений настоящей Инструкции.

8.2 Ответственный за организацию обработки информации в ГИС главного управления ЗАГС Рязанской области несет ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки информации с использованием ТСЗИ лицензионным требованиям и условиям, эксплуатационной и технической документации к ТСЗИ, а также настоящей Инструкции.

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

## ИНСТРУКЦИЯ

по обращению с сертифицированными криптосредствами,  
предназначенными для защиты информации, обрабатываемой в  
государственной информационной системе  
главного управления ЗАГС Рязанской области, и криптоключам к ним

### 1 Общие положения

Инструкция по обращению с сертифицированными криптосредствами, предназначенными для защиты информации, обрабатываемой в государственной информационной системе (далее - ГИС) главного управления ЗАГС Рязанской области, и криптоключам к ним регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, внедрения в прикладные системы, тестирования в целях защиты конфиденциальной информации.

Под криптосредством в настоящей Инструкции понимается специальное (криптографическое) средство, предназначенное для защиты информации.

К криптосредствам (шифровальным, криптографическим средствам)

Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от ложной информации.

Средства электронной цифровой подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

1.3.4 Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.3.5 Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

1.3.6 Ключевые документы (независимо от вида носителя ключевой информации).

1.4 В настоящей Инструкции используются следующие понятия и определения:

1.4.1 Доступ к информации - возможность получения информации и ее использования.

1.4.2 Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

1.4.3 Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих их обработку информационных технологий и технических средств.

1.4.4 Ключевой документ – физический носитель определенной структуры, содержащий криптоключи.

1.4.5 Компрометация криптоключа – утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

1.4.6 Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

1.4.7 Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

1.4.8 Пользователь криптосредства - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.4.9 Распространение информации - действия, направленные на раскрытие конфиденциальной информации неопределённому кругу лиц.

1.4.10 Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

1.4.11 Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.5 Для обеспечения безопасности информации при ее обработке в ГИС главного управления ЗАГС Рязанской области должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.6 Класс криптосредства определяется в соответствии с «Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах

персональных данных с использованием средств автоматизации», утв. руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/54-144.

## **2 Организационная структура**

2.1 Безопасность обработки информации в ГИС главного управления ЗАГС Рязанской области с использованием криптосредств организует и обеспечивает Ответственный за эксплуатацию СКЗИ главного управления ЗАГС Рязанской области.

## **3 Обязанности пользователей криптосредств**

3.1 Пользователи криптосредств допускаются к работе с ними только после ознакомления под роспись с настоящей Инструкцией, Типовыми требованиями, другими документами, регламентирующими организацию и обеспечение безопасности информации при ее обработке в ГИС главного управления ЗАГС Рязанской области.

3.2 При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

3.3 Ответственный за эксплуатацию СКЗИ обязан:

3.3.1 Осуществлять поэкземплярный учет используемых оператором криптосредств, эксплуатационной и технической документации к ним.

3.3.2 Осуществлять контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией.

3.3.3 Осуществлять учет Пользователей криптосредств.

3.3.4 Надежно хранить эксплуатационную и техническую документацию к криптосредствам, ключевые документы, носители дистрибутивов криптосредств, бумажные и машинные носители конфиденциальной информации.

3.3.5 Проводить расследования и составлять заключения по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации.

3.3.6 Осуществлять разработку и принимать меры по предотвращению возможных негативных последствий нарушений.

3.4 Пользователи криптосредств обязаны:

3.4.1 Не нарушать конфиденциальность закрытых ключей.

3.4.2 Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

3.4.3 Не допускать вывод закрытых ключей на дисплей (монитор) ПЭВМ или принтер.

3.4.4 Не допускать записи на ключевой документ посторонней информации.

3.4.5 Не допускать установки ключевых документов в другие ПЭВМ.

3.4.6 Обеспечить конфиденциальность информации о крипто средствах, других мерах защиты.

3.4.7 Не нарушать конфиденциальность защищаемой информации.

3.4.8 Точно соблюдать требования к обеспечению безопасности защищаемой информации, требования к обеспечению безопасности крипто средств и ключевых документов к ним.

3.4.9 Хранить ключевые документы к крипто средствам в защищаемых хранилищах.

3.4.10 Сдавать ключевые документы к крипто средствам при увольнении или отстранении от исполнения обязанностей.

3.4.11 Своевременно выявлять и сообщать Ответственному за эксплуатацию СКЗИ и Ответственному за организацию обработки информации в ГИС о ставших им известными попытках посторонних лиц получить сведения об используемых крипто средствах или ключевых документах к ним, защищаемой информации.

3.4.12 Немедленно уведомлять Ответственного за эксплуатацию СКЗИ и Ответственного за организацию обработки информации в ГИС главного управления ЗАГС Рязанской области и принимать меры по предупреждению нарушения конфиденциальности защищаемой информации при утрате или недостачи крипто средств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности информации.

#### 4 Учет ключевых документов

4.1 Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

4.2 Все экземпляры ключевых документов выдаются пользователям крипто средств под роспись в соответствующем журнале поэкземплярного учета.

4.3 Передача ключевых документов допускается только между пользователями крипто средств и Ответственным за эксплуатацию СКЗИ под роспись в соответствующем Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями крипто средств осуществляется с санкции Ответственного за эксплуатацию СКЗИ.

4.4 Для исключения компрометации ключевых документов, на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища (сейфы, железные ящики), которые, в свою очередь, закрываются на ключ и опечатываются.

4.5 Учет эксплуатационной и технической документации к крипто средствам:

4.5.1 Эксплуатационная и техническая документация к крипто средствам подлежит поэкземплярному учету.

4.5.2 Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под роспись.

4.5.3 Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под роспись. Аналогичная передача между пользователями криптосредств осуществляется с санкции Ответственного за эксплуатацию СКЗИ.

4.6 Распространение ключевых документов:

4.6.1 Ключевые документы получают лично владельцем криптографического ключа в удостоверяющем центре.

4.7 Плановая смена ключевых документов:

4.7.1 Заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

4.8 Внеплановая смена ключевых документов:

4.8.1 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

4.9 Уничтожение ключевых документов:

4.9.1 Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются Ответственному за эксплуатацию СКЗИ, или по его указанию уничтожаются на месте пользователями криптосредств.

4.9.2 Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

4.9.3 Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

4.9.4 Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 суток после вывода их из действия (окончания срока действия).

4.9.5 Пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Ответственного за эксплуатацию СКЗИ главного управления ЗАГС Рязанской области.

4.10 Уничтожение эксплуатационной и технической документации к криптосредствам:

4.10.1 Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.

## 5 Техническое обслуживание криптосредств

5.1 Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

5.2 На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

## **6 Опечатывание аппаратных средств**

6.1 Системные блоки АРМ, на которых установлены криптосредства, должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

## **7 Организация режима помещений**

7.1 Охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность защищаемой информации, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.2 При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

7.3 Перечисленные в настоящей Инструкции требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

7.4 Режимные помещения выделяются с учетом размеров контролируемых зон. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. 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, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

7.5 Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается ответственным за организацию обработки информации в ГИС главного управления ЗАГС Рязанской области.

7.6 Двери режимных помещений должны закрываться на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

7.7 Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

## 8 Порядок доступа к хранилищам

### 8.1 Эксплуатация хранилищ:

8.1.1 Пользователи криптосредств хранят, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

8.1.2 Металлические хранилища должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

8.1.3 Должно быть предусмотрено отдельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

8.2 При необходимости доступа к содержимому хранилища сотрудник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

8.3 По окончании работы сотрудник закрывает и опечатывает хранилище, за которое он ответственен.

8.4 Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за данные хранилища.

8.5 Порядок предоставления сотрудникам ключей для доступа к хранилищам:

8.5.1 Рабочий ключ от хранилища предоставляется сотруднику, ответственному за данное хранилище, под роспись в соответствующем журнале ответственным за эксплуатацию хранилищ.

8.5.2 Запасные экземпляры ключей от хранилищ хранятся в сейфе (хранилище) ответственного за эксплуатацию хранилищ.

8.5.3 Запасные экземпляры ключей от сейфа ответственного за эксплуатацию хранилищ передаются в опечатанном пенале под роспись в соответствующем журнале.

8.5.4 Ключи от хранилища не должны предоставляться сотрудникам, не ответственным за данные хранилища.

8.5.5 Изготавливать ключи от механического замка хранилищ имеет право только ответственный за эксплуатацию хранилищ.

8.5.6 Ключи от механических замков хранилищ должны быть пронумерованы, учтены в соответствующем журнале.

8.5.7 При увольнении сотрудника, либо при назначении другого лица ответственным за хранилище данного сотрудника, сотрудник обязан сдать



имеющиеся у него ключи от механического замка хранилища ответственному за эксплуатацию хранилищ.

8.5.8 Сотрудникам запрещено передавать кому-либо ключи от хранилищ кроме как в случаях, предусмотренных настоящей Инструкцией.

8.6 Действия при несанкционированном проникновении или утрате ключей от хранилища:

8.6.1 При утрате ключа от хранилища замок данного хранилища 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. Об утрате ключа сотрудник должен немедленно оповестить Ответственного за хранилища и ключи от них. Порядок хранения документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает Ответственный за хранилища и ключи от них.

8.6.2 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию хранилищ. Ответственный за хранилища и ключи от них должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств, составить акт и принять, при необходимости, меры к локализации последствий.

## **9 Контроль безопасности криптосредств**

9.1 Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на Ответственного за эксплуатацию СКЗИ в пределах его полномочий.

## **10 Ответственность за нарушение требований**

10.1 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

10.2 Ответственный за эксплуатацию СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки информации с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Приложение № 7

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

**ПЕРЕЧЕНЬ**

должностей сотрудников главного управления ЗАГС Рязанской области,  
замещение которых предусматривает осуществление работ с  
сертифицированными СКЗИ, предназначенными для защиты информации

Наименование должности
Начальник главного управления
Первый заместитель начальника главного управления
Заместитель начальника главного управления
Начальник управления
Начальник отдела
Консультант отдела
Консультант по правовым вопросам отдела
Главный специалист отдела
Ведущий специалист отдела
Специалист 1 категории отдела
Начальник территориального отдела
Консультант территориального отдела
Главный специалист территориального отдела
Ведущий специалист территориального отдела
Специалист 1 категории территориального отдела
Ведущий эксперт
Эксперт

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

## **ИНСТРУКЦИЯ**

**по организации антивирусной защиты в государственной информационной системе главного управления ЗАГС Рязанской области**

### **1 Общие положения**

1.1 Настоящая Инструкция предназначена для Администратора ИБ государственной информационной системы (далее – ГИС) главного управления ЗАГС Рязанской области, Ответственного за организацию обработки информации в ГИС, и пользователей, эксплуатирующих ГИС.

1.2 Инструкция устанавливает требования и ответственность администраторов и пользователей ГИС при организации защиты конфиденциальной информации от воздействия вредоносных компьютерных вирусов.

1.3 Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля при работе в ГИС главного управления ЗАГС Рязанской области.

### **2 Требования по обеспечению антивирусной защиты**

2.1 Требования к порядку организации антивирусной защиты.

2.1.1 Для организации антивирусной защиты ГИС главного управления ЗАГС Рязанской области допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2 Приобретение и установка (обновление) антивирусных программных средств осуществляется в установленном порядке. Не реже чем два раза в месяц Администратор ИБ ГИС должен производить обновление антивирусных баз, получая их из официальных источников. Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется Ответственным за организацию обработки информации в ГИС с привлечением (при необходимости) Администратора ИБ ГИС и/или специалистов лицензированной организации.

2.1.3 Должностные лица не должны допускать использования в ГИС программного обеспечения (ПО) и данных, не связанных с выполнением должностных обязанностей.

## 2.2 Требования к порядку проведения антивирусного контроля.

2.2.1 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором ИБ ГИС на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

- на защищаемых серверах и АРМ – Администратором ИБ ГИС;
- на других серверах и АРМ не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, - в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

2.2.2 При загрузке компьютера должен проводиться антивирусный контроль в автоматическом режиме. Порядок и периодичность расширенного антивирусного контроля и других необходимых антивирусных проверок определяется Администратором ИБ ГИС на этапе планирования мероприятий установленным порядком (не реже одного раза в месяц и при необходимости, в случае появления подозрений в заражении вирусной программой).

2.2.3 Обязательному дополнительному антивирусному контролю подлежит любая информация на съемных машинных носителях информации, поступающая для обработки в ГИС. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель информации).

2.2.4 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ГИС самостоятельно или вместе с Администратором ИБ ГИС должен провести внеочередной антивирусный контроль своей рабочей станции для определения ими факта наличия или отсутствия компьютерного вируса.

2.2.5 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ГИС обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и Администратора ИБ ГИС, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске Администратору ИБ ГИС для дальнейшей передачи в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИБ ГИС, в которой необходимо указать предполагаемый источник (отправителя, владельца и т.д.) зараженного файла,

тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

### **3 Ответственность при организации антивирусной защиты**

3.1 Ответственность за организацию антивирусной защиты ГИС и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на Администратора ИБ ГИС.

3.2 Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Ответственного за организацию обработки информации в ГИС и пользователей ГИС.

## **ИНСТРУКЦИЯ**

### **по организации парольной защиты в государственной информационной системе главного управления ЗАГС Рязанской области**

#### **1 Общие положения**

1.1 Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в государственной информационной системе (далее – ГИС) главного управления ЗАГС Рязанской области, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

#### **2 Требования по организации парольной защиты**

2.1 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ГИС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на Администратора ГИС и Администратора информационной безопасности ГИС (далее – Администратор ИБ ГИС), содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2.2 Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ГИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, \*, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

2.3 Владельцы паролей должны быть ознакомлены под роспись с

перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

**2.4** В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора ГИС и Администратора ИБ ГИС. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников главного управления ЗАГС Рязанской области.

**2.5** Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 90 дней.

**2.6** Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри главного управления ЗАГС Рязанской области и т.п.) должна производиться Администратором ГИС немедленно после окончания последнего сеанса работы данного пользователя с системой.

**2.7** Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри главного управления ЗАГС Рязанской области и другие обстоятельства) Администратора ГИС и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ГИС.

**2.8** В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.2.6 или п.2.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

### **3 Ответственность при организации парольной защиты**

**3.1** Ответственность за организацию парольной защиты ГИС и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на Администратора ИБ ГИС.

**3.2** Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Ответственного за организацию обработки информации в ГИС и пользователей (операторов) ГИС.

**3.3** Периодический контроль за выполнением всех требований настоящей Инструкции, и состоянием антивирусной защиты осуществляется  
Администратором ИБ ГИС.

# ЖУРНАЛ

## поземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним главного управления ЗАГС Рязанской области

На \_\_\_\_\_ листах

Начат «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончен «\_\_» \_\_\_\_\_ 20\_\_ г.

(ФИО ответственного лица за ведение журнала)

\_\_\_\_\_ подпись

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
				Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16



к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

## ЖУРНАЛ

позземплярного учета ключевых документов  
главного управления ЗАГС Рязанской области

На \_\_\_\_\_ листах

Начат «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончен «\_\_» \_\_\_\_\_ 20\_\_ г.

(ФИО ответственного лица за ведение журнала)

подпись

№ п/п	Наименование ключевых документов	Серийные номера ключевых документов	От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата изготовления ключевых документов и расписка в изготовлении	Дата и номер подтверждения или расписка в получении	Дата уничтожения	Подпись Администратора ИБ
1	2	3	4	5	6	7	8

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

# ЖУРНАЛ

**регистрации, учета и установли средств защиты информации  
главного управления ЗАГС Рязанской области**

На \_\_\_\_\_ листах

Начат «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончен «\_\_» \_\_\_\_\_ 20\_\_ г.

(ФИО ответственного лица за ведение журнала)

**ПОДПИСЬ**

[illegible]

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

## ЖУРНАЛ

учета дистрибутивов ключевой информации сети ViPNet № 1679  
главного управления ЗАГС Рязанской области

На \_\_\_\_\_ листах

Начат «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончен «\_\_» \_\_\_\_\_ 20\_\_ г.

(ФИО ответственного лица за ведение журнала)

подпись

№ п/п	Наименование дистрибутива ключевой информации	Дата формирования дистрибутива	Место установки	Подпись ответственного за формирование дистрибутива	Подпись Администратора ИБ	Примечание
1	2	3	4	5	6	7

**регистрации, учета и выдачи носителей конфиденциальной информации и резервных копий конфиденциальной информации главного управления ЗАГС Рязанской области**

Начат «\_\_» \_\_\_\_\_ 20\_\_ г.  
Окончен «\_\_» \_\_\_\_\_ 20\_\_ г.

**ПОДПИСЬ**

[illegible]

Приложение № 15

к приказу главного управления  
ЗАГС Рязанской области  
от 11 августа 2014 г. № 118-д

ЖУРНАЛ

учета хранилищ для хранения бумажных и электронных носителей конфиденциальной информации, СКЗИ и  
эксплуатационной документации к ним, ключевых документов  
главного управления ЗАГС Рязанской области

На \_\_\_\_\_ листах

Начат « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.  
Окончен « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

\_\_\_\_\_ подписать

\_\_\_\_\_ (ФИО ответственного лица за ведение журнала)

Дата регистрации	Адрес структурного подразделения	Номер помещения	Вид хранилища	Номер хранилища	Ответственный за хранилище	Подпись ответственного	Примечание
1	2	3	4	5	6	7	8