БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ
ЕР ҺӘМ МӨЛКӘТ МӨНӘСӘБӘТТӘРЕ
МИНИСТРЛЫҒЫ
450008, Өфө ҡалаһы, Цюрупа урамы, 13
тел. (347) 272-95-53

РЕСПУБЛИКА БАШКОРТОСТАН
МИНИСТЕРСТВО ЗЕМЕЛЬНЫХ
И ИМУЩЕСТВЕННЫХ ОТНОШЕНИЙ
450008, г. Уфа, ул. Цюрупы, 13
тел. (347) 272-95-53

ПРИКАЗ

«28» февраль 2013 й. № 464 «28» февраля 2013 г.

О защите конфиденциальной информации в Министерстве земельных и имущественных отношений Республики Башкортостан

Руководствуясь требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утверждёнными приказом Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002 г. № 282, в целях защиты конфиденциальной информации, обрабатываемой в Министерстве земельных и имущественных отношений Республики Башкортостан, ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые:

Порядок организации и проведения работ по защите конфиденциальной информации в Министерстве земельных и имущественных отношений Республики Башкортостан;

Перечень информационных систем персональных данных (ИСПДн), эксплуатируемых в Министерстве земельных и имущественных отношений Республики Башкортостан;

Перечень персональных данных, обрабатываемых в Министерстве земельных и имущественных отношений Республики Башкортостан;

Перечень должностей работников Министерства земельных и имущественных отношений Республики Башкортостан, уполномоченных на обработку персональных данных, имеющих право самостоятельного доступа к штатным средствам информационной системы персональных данных (ИСПДн).

2. Руководителям подразделений обеспечить ознакомление под подпись работников с Порядком организации и проведения работ по защите конфиденциальной информации в Министерстве земельных и имущественных отношений Республики Башкортостан, Перечнем персональных данных, обрабатываемых в Министерстве земельных и имущественных отношений Республики Башкортостан, мерами ответственности за неправомерное обращение с персональными данными

граждан.

3. Начальнику отдела информационных технологий обеспечить защиту конфиденциальной информации в соответствии с утверждённым Порядком организации и проведения работ по защите конфиденциальной информации в Министерстве земельных и имущественных отношений Республики Башкортостан.

4. Признать утратившим силу приказ Министерства земельных и имущественных отношений Республики Башкортостан от 22.08.2008 № 1845 «О защите конфиденциальной информации в Министерстве земельных и имущественных отношений Республики Башкортостан».

5. Контроль за исполнением настоящего приказа возложить на заместителя министра Ягафарова Р.Б.

Министр Р.К. Искужин

Утверждён
приказом Министерства
земельных и имущественных отношений
Республики Башкортостан
от «28» февраля 2013 г.
№ 464

ПОРЯДОК
организации и проведения работ по защите конфиденциальной информации в Министерстве земельных и имущественных отношений Республики Башкортостан

I. Общие положения

Настоящий Порядок организации и проведения работ по защите конфиденциальной информации (далее – Порядок) в Министерстве земельных и имущественных отношений Республики Башкортостан (далее – Минземимущество РБ) определяет основные принципы, организацию, порядок осуществления работ, основные требования и рекомендации, способы и средства защиты циркулирующей в Минземимуществе РБ конфиденциальной информации, не содержащей сведения, составляющие государственную тайну (далее – конфиденциальная информация).

1.1. Настоящий Порядок разработан в соответствии с Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 17.03.2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 г. № 282, постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и другими нормативно-методическими документами.

1.2. Контроль за обеспечением требований по технической защите конфиденциальной информации осуществляется заместителем министра земельных и имущественных отношений Республики Башкортостан.

1.3. Разработка мероприятий по защите информации в Минземимуществе РБ осуществляется специалистами отдела информационных технологий. Разработка и реализация мер защиты информации может осуществляться также организациями, имеющими

лицензии на право проведения соответствующих работ, привлекаемых в установленном порядке.

1.4. К обработке конфиденциальной информации допускаются лица, утверждённые приказом Министерства земельных и имущественных отношений Республики Башкортостан.

1.5. Сотрудники Минземимущества РБ, осуществляющие работы с использованием конфиденциальной информации, несут персональную ответственность за несоблюдение безопасности конфиденциальной информации.

II. Основные термины и понятия

В настоящем Порядке используются следующие основные понятия и термины:

объект защиты – материальный носитель конфиденциальной информации или место его нахождения, подлежащее защите;

утечка информации – несанкционированное и целенаправленное получение конфиденциальной информации третьими лицами, которые могут её использовать в своих интересах;

утрата информации – несанкционированное разглашение конфиденциальной информации или утрата её носителей субъектами, которым они были доверены;

защита информации – осуществление организационно-технических мероприятий, направленных на предотвращение утечки и утраты конфиденциальной информации;

пользователь – сотрудник Минземимущества, имеющий доступ к информационным ресурсам Минземимущества, содержащим конфиденциальную информацию;

автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

контролируемая зона (КЗ) – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами;

информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

электронные носители информации – материальные носители, используемые для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники.

III. Цели и задачи разработки и внедрения системы защиты информации

Основными целями и задачами разработки и внедрения системы защиты информации в Минземимуществе РБ являются:

– предотвращение утечки и утраты информации, а также её носителей;

– обеспечение условий быстрого, полного и всестороннего расследования случаев утечки информации;

– устранение негативных последствий и условий в случае несанкционированной утечки или утраты информации;

– обеспечение оптимальных условий накопления, хранения, обработки и использования информации.

IV. Объекты защиты информации

4.1. Защите в Минземимуществе РБ подлежит информация, обрабатываемая средствами вычислительной техники (СВТ), а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

Объектами защиты при этом являются:

– средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети, системы связи и передачи данных, технические средства приема, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической и видео-информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки конфиденциальной информации;

– технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещённые в помещениях, где она обрабатывается (циркулирует).

4.2. Перечень сведений конфиденциального характера, подлежащих защите, а также Перечень средств информатизации Минземимущества РБ, с использованием которых обрабатывается информация конфиденциального характера, разрабатывается специалистами отдела информационных технологий совместно с подразделениями, эксплуатирующими указанные средства вычислительной техники, и утверждаются приказом Министерства

земельных и имущественных отношений Республики Башкортостан.

4.3. Все сотрудники Минземимущества РБ должны быть ознакомлены с Перечнем сведений конфиденциального характера, в части, их касающейся.

4.4. Информационные системы персональных данных, используемые в подразделениях Минземимущества РБ с использованием СВТ, должны быть проклассифицированы в соответствии в приказом ФСБ России, Федеральной службы по техническому и экспортному контролю России и Министерства связи и информатизации России № 55/86/20 от 14.02.2008 г. Защита информационных систем персональных данных должна осуществляться в соответствии с требованиями методических документов, утверждённых Федеральной службой по техническому и экспортному контролю Российской Федерации 15.02.2008 г.

4.5. Порядок обращения со служебной информацией ограниченного доступа должен осуществляться в соответствии с требованиями Положения о порядке обращения со служебной информацией ограниченного распространения в республиканских органах исполнительной власти, утверждённого постановлением Кабинета Министров Республики Башкортостан от 26.12.1995 г. № 447.

4.6. В целях дифференцированного подхода к защите конфиденциальной информации должна производиться классификация автоматизированных систем по требованиям защищённости от несанкционированного доступа в соответствии с руководящими документами Государственной технической комиссии при Президенте Российской Федерации.

V. Порядок создания и ввода в действие объектов информатизации, на которых обрабатывается конфиденциальная информация

5.1. Организация работ по созданию и эксплуатации объектов информатизации и их средств защиты состоит из следующих этапов:

– предпроектное обследование объектов информатизации, на которых будет обрабатываться конфиденциальная информация;

– разработка аналитического обоснования необходимости создания средств защиты конфиденциальной информации и технического задания на их создание;

– проектирование объектов информатизации, включая разработку системы защиты информации в их составе;

– ввод в действие системы защиты информации, включая опытную эксплуатацию и приёмно-сдаточные испытания средств защиты информации, а также аттестацию объектов информатизации на соответствие требованиям безопасности информации.

5.2. Техническое задание на разработку системы защиты информации должно содержать:

– обоснование разработки;

– исходные данные создаваемого объекта информатизации;

– класс защищённости автоматизированной системы;

– перечень предполагаемых средств защиты информации;

– требования к средствам защиты информации на основе нормативно-методических документов и установленного класса защищённости автоматизированной системы.

5.3. На этапе ввода в действие объектов информатизации и системы защиты информации осуществляются:

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности;

– приёмно-сдаточные испытания средств защиты информации;

– аттестация объектов информатизации по требованиям безопасности информации.

Предпроектное обследование объектов информатизации осуществляется специалистами отдела информационных технологий, либо может быть поручено специализированной организации, имеющей соответствующую лицензию.

VI. Источники угроз безопасности информации

6.1. При использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

– несанкционированный доступ к обрабатываемой в АС информации и несанкционированные действия с ней;

–воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедрённых программных средств;

–побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи информации;

– наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

– радиоизлучения, модулирование информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;

– радиоизлучения или электрические сигналы от внедрённых в технические средства и защищаемые помещения специальных электронных устройств съёма речевой информации (закладочные устройства), модулированные информативным сигналом;

– радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключённых к каналам связи или техническим

средствам обработки информации;

– просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

– прослушивание телефонных и радиопереговоров;

– хищение технических средств с хранящейся в них информацией или носителей информации.

6.2. Перехват информации или воздействие на неё с использованием технических средств могут вестись:

– из-за границы КЗ из близлежащих строений и транспортных средств;

– из смежных помещений, принадлежащих другим организациям и расположенных в том же здании, что и объект защиты;

– при посещении организации посторонними лицами;

– за счёт несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через вычислительные сети.

6.3. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты, либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства съёма информации (закладочные устройства), размещаемые внутри или вне защищаемых помещений.

6.4. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ, например, за счёт некомпетентных или ошибочных действий пользователей и администраторов.

VII. Защита конфиденциальной информации, циркулирующей в информационно-коммуникационных системах

7.1. С целью обеспечения безопасности конфиденциальных данных в сетевых версиях автоматизированных систем, применяется система разграничения доступа к конфиденциальной информации с помощью программных средств используемой сетевой операционной системы (ОС). Для этого администратор базы данных должен выполнять следующие мероприятия:

– устанавливать права доступа пользователей к ресурсам сервера в соответствии с требованиями должностных регламентов;

– присваивать пользователям соответствующие имена и пароли для доступа к конфиденциальной информации, находящейся в локальных сетях, при этом в качестве паролей могут использоваться сочетания букв и цифр общей длиной не менее восьми знаков;

– назначать периодичность смены паролей.

7.2. Включение информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается конфиденциальная информация, к сетям общего пользования, в том числе Интернет, осуществляется в соответствии с требованиями Указа Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

7.3. Для обеспечения физической безопасности конфиденциальной информации, циркулирующей в ЛВС, осуществляются следующие мероприятия:

– ограничение доступа посторонних лиц к серверам, а также сетевому оборудованию;

– резервное копирование информации, представляющей особую ценность (базы данных);

– периодический контроль ресурсов файл-серверов;

– применение антивирусных средств;

– обеспечение файл-серверов и сетевого оборудования источниками бесперебойного питания;

– управление электронными носителями конфиденциальной информации (учёт, регистрация, передача, уничтожение).

7.4. С целью обеспечения безопасности конфиденциальной информации, обрабатываемой с использованием средств вычислительной техники, каждый пользователь обязан выполнять следующие требования:

7.4.1. Подключаться к ресурсам локальных сетей и автоматизированной системы только с закреплённого рабочего места.

7.4.2. При вводе пароля убеждаться, что при наборе гарантируется его конфиденциальность.

7.4.3. При временном убытии с рабочего места и в конце рабочего дня производить отключение от используемых ресурсов.

7.4.4. При использовании в работе электронных носителей информации проверять их перед началом работы средствами антивирусной защиты.

7.4.5. При обнаружении действий, грозящих безопасности информационной системы, немедленно докладывать об этом лицам, ответственным за эксплуатацию данной системы и своему непосредственному начальнику.

7.5. Пользователю автоматизированной системы обработки конфиденциальных данных запрещается:

– подключаться к ресурсам ЛВС и автоматизированной системе под чужим именем;

– сообщать кому-либо пароль;

– использовать ресурсы ЛВС для нужд, не связанных с её назначением;

– записывать и запускать игровые программы;

– отключать средства защиты и регистрации доступа к конфиденциальной информации;

– производить попытки несанкционированного доступа к конфиденциальной информации;

– использовать в работе электронные носители информации, компакт-диски без предварительной проверки антивирусными программами;

– пользоваться неучтёнными электронными носителями информации;

– устанавливать программное обеспечение, взаимодействующее с локальной компьютерной сетью, сетью Интернет и электронной почтой, в том числе:

– клиентского программного обеспечения, предназначенного для организации доступа к серверам баз данных;

– средств администрирования серверов баз данных, WEB-серверов или средств маршрутизации;

– программных или аппаратных систем маршрутизации пакетов, в том числе proxy-серверов;

– программных межсетевых экранов (FireWall);

– серверов WINS, DHCP и DNS;

– организовывать на базе рабочего компьютера серверов удалённого доступа, устанавливать дополнительное оборудование (модемы, сотовые телефоны, сетевые карты и т.п.) для доступа к другим сетям или компьютерам;

– устанавливать и использовать программное обеспечение, осуществляющее нестандартную передачу файлов или обмен информацией: так называемые чат-программы и интернет-пейджеры типа ICQ и т.п.;

– посещать конференции и сайты непроизводственного назначения;

– производить какое-либо переключение оборудования, без согласования со специалистом, ответственным за защиту информации.

VIII. Методы защиты информации

Защита информации на объектах информатизации Минземимущества РБ осуществляется по следующим направлениям:

– исключение или существенное затруднение возможности получения заинтересованными лицами на этапе эксплуатации объектов Минземимущества РБ охраняемых сведений;

– защита информации и критичных информационных процессов, в том числе от компьютерных вирусов и других программно-технических воздействий, от хищения технических средств с находящейся в них информацией или отдельных носителей информации.

В этих целях:

– ограничивается доступ посторонних лиц в помещения, в которых размещаются объекты защиты;

– ремонт ПЭВМ осуществляется в режиме, исключающем считывание записанной или восстановление стёртой на жёстком диске конфиденциальной информации;

– с учётом классификации автоматизированных систем реализуется

комплекс программно-технических мероприятий по управлению доступом к базам данных, регистрации и учёта доступа к ресурсам автоматизированных систем, протоколирование всех действий пользователей, выполняемых в автоматизированной системе;

– проводится аттестация объектов информатизации с оформлением «Аттестата соответствия».

IX. Планирование работ по защите информации и контролю защиты информации

9.1. Работа по защите информации в Минземимуществе РБ проводится в соответствии с годовым планом.

9.2. План должен содержать мероприятия по технической защите информации, выполняемые всеми структурными подразделениями Минземимущества РБ, эксплуатирующими объекты информатизации, и направленные на выявление и учёт факторов, которые воздействуют или могут воздействовать на конфиденциальную информацию.

9.3. В план включаются следующее разделы:

9.3.1. Мероприятия по выполнению решений Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России);

9.3.2. Обследование объектов информатизации:

– соответствие классов защищённости автоматизированных систем и данных, отражённых в технических паспортах объектов информатизации, условиям, сложившимся на момент проверки;

– проверка выполнения установленных норм и требований по защите информации;

– разработка (совершенствование) системы защиты информации.

9.3.3. Организационно-методическое обеспечение работ по технической защите информации:

– разработка, корректировка и согласование организационно методических документов, планов, отчетов;

– оценка эффективности принимаемых мер по защите информации на объектах информатизации.

9.3.4. Для каждого мероприятия по защите информации устанавливаются срок исполнения, материально-техническое обеспечение, ответственный за исполнение, ответственный за контроль, отметка о выполнении.

9.4. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

9.5. Контроль защиты информации в органе осуществляется в целях:

– предупреждения и пресечения возможности получения техническими средствами разведки охраняемых сведений об объектах информатизации Минземимущества РБ;

– выявления и предотвращения утечки информации по техническим

каналам;

– исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации;

– предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

9.6. Основными задачами контроля являются:

– проверка организации выполнения мероприятий по защите информации в подразделениях Минземимущества РБ, учёта требований по защите информации в разрабатываемых плановых и распорядительных документах;

– проверка выполнения установленных норм и требований по защите информации;

– оценка достаточности и эффективности мероприятий по защите информации;

– проверка выполнения требований по защите автоматизированных систем от несанкционированного доступа;

– проверка выполнения требований по антивирусной защите автоматизированных рабочих мест;

– проверка знаний должностных лиц по вопросам защиты информации и их соответствия необходимому уровню подготовки для конкретного рабочего места;

– оперативное принятие мер по пресечению нарушений требований (норм) защиты информации на объектах информатизации Минземимущества РБ.

9.7. Повседневный контроль выполнения мероприятий по защите информации осуществляет специалист, ответственный за защиту информации.

9.8. Периодический контроль выполнения мероприятий по защите информации проводится комиссией по категорированию и классификации объектов информатизации Минземимущества РБ не реже одного раза в год. Результаты обследования оформляются актом.

В ходе обследования проверяется:

– соответствие классов защищённости автоматизированных систем условиям, сложившимся на момент проверки;

– соблюдение организационно-режимных требований;

– выполнение требований по защите автоматизированных систем от несанкционированного доступа;

– выполнение требований по антивирусной защите автоматизированных систем и средств вычислительной техники.

9.9. Контроль эффективности мер защиты информации на объектах информатизации Минземимущества РБ с использованием технических средств осуществляется не реже 1 раза в год организацией, имеющей

лицензию ФСТЭК России на право осуществления мероприятий по защите конфиденциальной информации.

9.10. Периодический контроль состояния защиты информации осуществляется при проверке Минземимущества РБ комиссией Управления Федеральной службы по техническому и экспортному контролю Российской Федерации по Приволжскому Федеральному округу.

X. Аттестация объектов информатизации

10.1. Объекты информатизации Минземимущества РБ, предназначенные для обработки информации конфиденциального характера, подлежат обязательной аттестации по требованиям безопасности информации, либо требуют декларирования соответствия требованиям безопасности информации.

10.2. Аттестация объектов информатизации осуществляется организациями, имеющими лицензии ФСТЭК России на осуществление работ по защите конфиденциальной информации.

10.3. Декларирование соответствия объектов информатизации требованиям безопасности информации осуществляется самостоятельно силами сотрудников Минземимущества РБ на основании собственных доказательств.

10.4. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

10.5. В результате аттестационных испытаний оформляется «Аттестат соответствия», которым подтверждается, что объект соответствует требованиям стандартов или иных нормативных документов по защите конфиденциальной информации, утверждённых ФСТЭК России и другими органами государственного управления в пределах их компетенции.

10.6. На основании выданного специализированной организацией аттестата соответствия министр земельных и имущественных отношений Республики Башкортостан издаёт приказ о разрешении обработки конфиденциальной информации на объекте информатизации и назначении лиц, ответственных за обеспечение защиты информации при его эксплуатации.

XI. Порядок взаимодействия подразделений Минземимущества РБ, специализированных сторонних организаций при разработке и эксплуатации объектов информатизации и системы защиты информации

11.1. В процессе создания (модернизации) и эксплуатации объектов информатизации взаимодействие подразделений Минземимущества РБ

направлено на обеспечение надёжного и бесперебойного его функционирования. Тем самым создаются условия выполнения Минземимуществом РБ функций по своему предназначению. Распределение полномочий определяется приказами и распоряжениями министра земельных и имущественных отношений РБ, распоряжениями заместителей министра земельных и имущественных отношений РБ и положениями о подразделениях (отдельных специалистах).

11.2. С целью выполнения отдельных видов работ по технической защите информации Минземимущество РБ в установленном порядке заключает договоры на оказание услуг с организациями-лицензиатами ФСТЭК России и ФСБ России, имеющими лицензии на оказание услуг в области технической защиты конфиденциальной информации.

Порядок взаимодействия по вопросам защиты информации, применяемые совместные организационные и технологические мероприятия, ответственность, права и обязанности взаимодействующих сторон определяются соответствующими договорами.

11.3. Структурная схема взаимодействия приведена на рис. 1.

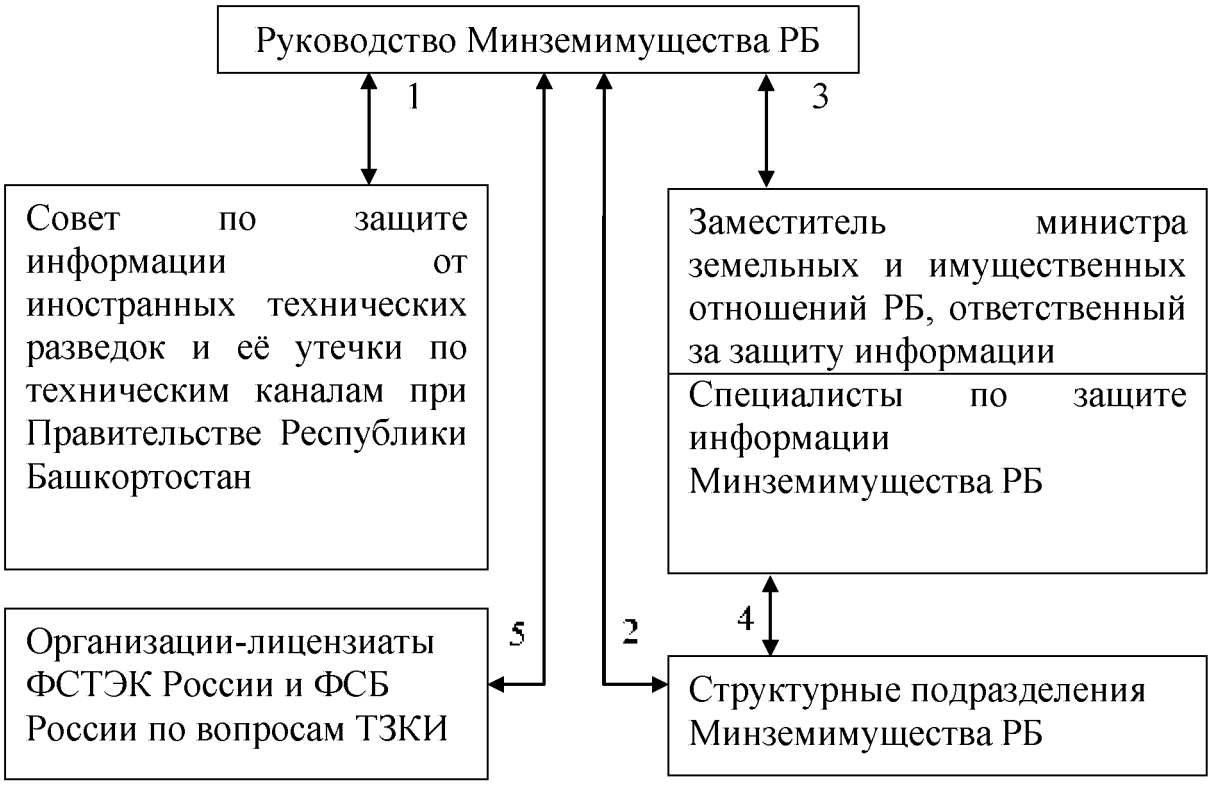

Рис. 1

1 – Координация работ по технической защите конфиденциальной информации, а также контроль состояния работ в данной области.

2 – Взаимодействие в процессе определения необходимости создания объекта информатизации, его создания, определения необходимости и создания системы защиты информации объекта информатизации, а также в процессе эксплуатации.

3 – Взаимодействие в процессе определения необходимости разработки системы защиты информации объекта информатизации, её создания. Организация контроля достаточности и эффективности мер защиты информации в процессе разработки и эксплуатации.

4 – Выполнение работ по созданию объекта информатизации, а также технической защите конфиденциальной информации.

5 – Аттестация объектов информатизации на договорной основе.

Утверждён
приказом Министерства
земельных и имущественных отношений
Республики Башкортостан
от «28» февраля 2013 г.
№ 464

Перечень информационных систем персональных данных (ИСПДн), эксплуатируемых в Министерстве земельных и имущественных отношений Республики Башкортостан

1. Реестр государственных гражданских служащих аппарата Минземимущества РБ (ИСПДн «Реестр ГГС Минземимущества РБ»);
2. Реестр государственных гражданских служащих территориальных органов Минземимущества РБ (ИСПДн «Реестр ГГС ТО Минземимущества РБ»);
3. Программа для автоматизации расчёта и учёта заработной платы государственных гражданских служащих (ИСПДн «Зарплата»);
4. Программа для подготовки данных персонифицированного учёта для предоставления в органы Пенсионного фонда Российской Федерации (ИСПДн «ПФР»);
5. Программа автоматизации бухгалтерского учёта «1С Бухгалтерия» (ИСПДн «1С Бухгалтерия»)
6. Автоматизированная система ведения имущественного кадастра «Имущество» (ИСПДн «Имущество»).

Утверждён
приказом Министерства
земельных и имущественных отношений
Республики Башкортостан
от «28» февраля 2013 г.
№ 464

Перечень персональных данных, обрабатываемых в Министерстве земельных и имущественных отношений Республики Башкортостан

№ п/п	Основания для обработки	Содержание сведений	Срок хранения, условия прекращения обработки
1	Глава 14 Трудового кодекса Российской Федерации, статья 42 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации", Положение о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела (утв. Указом Президента Российской Федерации от 30.05.2005 № 609) и др.	- Сведения, предусмотренные унифицированными формами № Т-2 ГС, Т-2 - Сведения о заработной плате и о денежном содержании государственного гражданского служащего - Иные сведения, определённые действующим законодательством	75 лет ЭПК[1]
2	Заключаемые договора аренды, купли-продажи и т.п.	- Фамилия, имя, отчество - Адрес места жительства или регистрации, дата регистрации - Номер паспорта, дата и место его выдачи - Дата рождения - ИНН - Расчётный счёт - Иные сведения, определённые действующим законодательством и заключаемыми договорами	До окончания действия договора или отзыва согласия субъекта персональных данных

[1] ЭПК означает, что часть таких документов может иметь научно-историческое значение и в установленном порядке должна передаваться в государственные, муниципальные архивы или храниться в организации (В соответствии с Перечнем типовых управленческих документов, сопровождающих деятельность организаций с указанием сроков хранения, утверждённом Росархивом 06.10.2000 г.)

Утверждён
приказом Министерства
земельных и имущественных отношений
Республики Башкортостан
от «28» февраля 2013 г.
№ 464

Перечень должностей работников Министерства земельных и имущественных отношений Республики Башкортостан, уполномоченных на обработку персональных данных, имеющих право самостоятельного доступа к штатным средствам информационной системы персональных данных (ИСПДн)

Должность	Номер кабинета	Инв. № системного блока
1. ИСПДн «Имущество»		
Отдел учета и ведения реестра государственного имущества		
Начальник отдела	120	101043298
Зам. начальника отдела	124	101043274
Зав. сектором	109	101043286
Зав. сектором	121	101043291
Главный спец.-эксперт	116	101043292
Главный спец.-эксперт	122	101043265
Ведущий спец.-эксперт	328	101043287
Ведущий спец.-эксперт	423	101043275
Ведущий спец.-эксперт	113	101043285
Ведущий спец.-эксперт	118	101043293
Ведущий спец.-эксперт	122	101041793
Ведущий спец.-эксперт	423	101043281
Ведущий спец.-эксперт	118	101043286
Ведущий спец.-эксперт	118	101042663
Специалист 1 разряда	118	101043285
Специалист 1 разряда	204	101043288
Отдел контроля и управления государственным имуществом		
Начальник отдела	326	101041307
Зам. начальника отдела	300	101042593
Зав. сектором	306	101043025
Зав. сектором	309	101043026
Главный спец.-эксперт	306	101041270
Главный спец.-эксперт	328	101043077
Ведущий спец.-эксперт	328	101041303
Ведущий спец.-эксперт	304	101041269

Ведущий спец.-эксперт	328	101041230
Ведущий спец.-эксперт	304	101041250
Ведущий спец.-эксперт	306	101042178
Ведущий спец.-эксперт	309	101041239
Отдел землеустройства, разграничения и распоряжения земельными участками		
Начальник отдела	433	101041315
Зам. начальника отдела	435	101043271
Зав. сектором	418	101041260
Зав. сектором	432	101043261
Главный спец.-эксперт	424	101041263
Ведущий спец.-эксперт	432	101043262
Ведущий спец.-эксперт	432	101041266
Ведущий спец.-эксперт	432	101041263
Ведущий спец.-эксперт	414	101041025
Специалист-эксперт	414	101041283
Отдел контроля и управления земельными участками		
Начальник отдела	421	101043276
Зам. начальника отдела	415	101043264
Главный спец.-эксперт	406	101041261
Ведущий спец.-эксперт	406	101042729
Ведущий спец.-эксперт	412	101041251
Ведущий спец.-эксперт	406	101042668
Ведущий спец.-эксперт	422	101042591
Ведущий спец.-эксперт	412	101043278
Ведущий спец.-эксперт	412	101043277
2. ИСПДн «Реестр ГГС Минземимущества РБ»		
Отдел кадров и государственной службы		
Заместитель начальника отдела	219	101041750
3. ИСПДн «Реестр ГГС ТО Минземимущества РБ»		
Отдел кадров и государственной службы		
Советник	317	101041277
4. ИСПДн «Зарплата»		
Бюджетный отдел		
Старший бухгалтер	404	01360718
5. ИСПДн «ПФР»		
Бюджетный отдел		
Старший бухгалтер	404	01360718
6. ИСПДн «1С Бухгалтерия»		
Бюджетный отдел		
Начальник отдела - главный бухгалтер	402	101043138М

Зам. начальника отдела	400/б	101043137М
Зам. начальника отдела	404	101043078
Главный экономист	404	101043193
Главный экономист	400/в	101042586
Главный экономист	400/а	101043071
Главный экономист	400/а	101043076
Ведущий бухг.-ревизор	400/в	101042587
Ведущий экономист	409	101042179
Старший бухгалтер	400/а	101042595
Ведущий экономист	409	101043070
Сектор административно-хозяйственной деятельности		
Старший специалист 2 разряда	105	101043072