\МИНИСТЕРСТВО ЭКОНОМИЧЕСКОГО РАЗВИТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
(РОСПАТЕНТ)

ПРИКАЗ

13.10.2022 **№ 158**

Москва

О назначении лиц, ответственных за эксплуатацию и обеспечение безопасности информации в государственных информационных системах, создаваемых на основании Приказа Роспатента от 26.02.2019 № 24

В целях обеспечения защиты информации, обрабатываемой в государственных информационных системах, создаваемых на основании Приказа Роспатента от 26.02.2019 № 24 «О реализации мероприятий по обеспечению возможности получения правовой охраны и управления правами на результаты интеллектуальной деятельности в цифровой среде в рамках федерального проекта "информационная инфраструктура национальной программы "Цифровая экономика Российской Федерации",

п р и к а з ы в а ю:

1. Назначить ответственными за эксплуатацию государственных информационных систем:

1.1. в части эксплуатации компонент государственных информационных систем, относящихся к инфраструктурным – Миротворцева А.В. – ведущего эксперта отдела цифрового развития, управления организации финансово-административной деятельности и цифровой трансформации Роспатента;

1.2. в части эксплуатации компонент, относящихся к прикладному обеспечению государственных информационных систем:

- Миротворцева А.В. - ведущего эксперта отдела цифрового развития, управления организации финансово-административной деятельности и цифровой трансформации Роспатента:

- государственная информационная система интеграции и управления нормативно-справочной информацией;

- государственная информационная система контроля использования прав на результаты интеллектуальной деятельности;

- государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицам и в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных»;

2. Назначить ответственным за обеспечение безопасности информации,

обрабатываемой в государственных информационных системах (администратора безопасности информации):

- Миротворцева А.В. – ведущего эксперта отдела цифрового развития, управления организации финансово-административной деятельности и цифровой трансформации Роспатента.

- Соловцова А.И. - начальника отдела системного администрирования и технической поддержки пользователей ФГБУ «ФИПС».

3. Назначить ответственным за защиту информации, обрабатываемой в государственных информационных системах Балыгина Д.А. - главного специалиста сектора информационной безопасности ФГБУ «ФИПС».

4. Возложить на ответственного за защиту информации обязанности по организации работ по защите информации, обрабатываемой в государственных информационных системах.

5. Назначить ответственным за организацию обработки персональных данных в государственных информационных системах:

- Грищук А.А. – главный специалист-:эксперт Роспатента:

- государственная информационная система контроля использования прав на результаты интеллектуальной деятельности;

- Соловцова А.И. – начальника отдела системного администрирования и технической поддержки пользователей ФГБУ «ФИПС»:

- государственная информационная система интеграции и управления нормативно-справочной информацией;

- Стародубцева Ю.В. - начальника отдела системного администрирования и технической поддержки пользователей :

- государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицам и в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных»;

6. Разрешить ответственным за эксплуатацию государственных информационных систем и ответственному за обеспечение безопасности информации, обрабатываемой в государственных информационных системах (администратору безопасности информации) действия по внесению изменений в конфигурацию соответствующих государственных информационных систем и их систему защиты информации.

7. Утвердить следующие инструкции :

- Инструкция ответственного за эксплуатацию государственных информационных систем (Приложение № 1);

- Инструкция ответственного за обеспечение безопасности информации, обрабатываемой в государственных информационных системах (Приложение № 2);

- Инструкция пользователя по обеспечению безопасности при работе с государственными информационным и системами (Приложение № 3);

- Инструкция ответственного за защиту информации, обрабатываемой в государственных информационных системах (Приложение № 4);

- Инструкция ответственного за организацию обработки персональных данных в государственной информационной системе (Приложение № 5).

- Инструкция технического администратора ИС (Приложение № 6).

8. Ответственному за защиту информации, обрабатываемой в государственных информационных системах, в 2-недельный срок провести инструктаж указанных в

пп. 1, 2 настоящего приказа работников и ознакомить их под роспись с действующей организационно-распорядительной документацией по защите информации.

9. Указанным в пп. 1, 2, 3 настоящего приказа работникам неукоснительно соблюдать требования нормативных документов по защите информации.

10. Обеспечить подготовку и поддержание в актуальном состоянии перечня нормативно-правовых актов, которые должны быть использованы при обеспечении защиты информации, обрабатываемой в государственных информационных системах.

Ответственные:

- Миротворцев А.В. – ведущий эксперт отдела цифрового развития Управления организации финансово-административной деятельности и цифровой трансформации Роспатента;

- Соловцов А.И. – заведующий отделом системного администрирования и технической поддержки пользователей ФГБУ «ФИПС»

11. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Фролова В.Е.

Руководитель Ю.С.Зубов

.

Приложение № 1
УТВЕРЖДЕНО
приказом
от 13 10 **20**22 **№** 158

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ЭКСПЛУАТАЦИЮ
государственных информационных систем:

Государственная информационная система контроля использования прав на результаты интеллектуальной деятельности (ГИС Контроль РИД)

Государственная информационная система интеграции и управления нормативно-справочной информацией (ГИС НИС)

Государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (ГИС Онлайн Роспатент)

2022 г.

1. Назначение

Инструкция ответственного за эксплуатацию (далее - Администратора) государственной информационной системы контроля использования прав на результаты интеллектуальной деятельности, государственной информационной системы интеграции и управления нормативно-справочной информацией и государственной информационной системы «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (далее – Система) (далее – Инструкция) определяет функции, права, обязанности и ответственность Администратора Системы.

2. Общие положения

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

Администратор Системы назначается из числа работников Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности» (далее – ФИПС).

3. Задачи и функции Администратора Системы

Основными задачами Администратора Системы являются:

- обеспечение функционирования и настройка системного и прикладного программного обеспечения (далее – СПО и ППО, соответственно), технических средств (далее – ТС) и кабельной системы (далее – КС) Системы;
- управление привилегиями доступа пользователей к ресурсам СПО, ППО;
- мониторинг функционирования СПО, ППО, ТС и КС.

Для выполнения поставленных задач на Администратора Системы возлагаются следующие функции:

- обеспечение работоспособности СПО, ППО, ТС и КС;
- ведение организационно–технической документации Системы в рамках своих полномочий;
- обновление СПО, ППО;
- локализация, устранение сбоев и неисправностей в работе СПО, ППО, ТС и КС;
- обеспечение непрерывности процесса обработки информации в ППО, проведение резервного копирования СПО, ППО;
- настройка привилегий доступа пользователей к ресурсам СПО, ППО и ТС;

• практическая реализация мероприятий по защите информации в СПО, ППО, ТС и КС.

4. Обязанности Администратора Системы

Для реализации поставленных задач и возложенных функций Администратор Системы обязан:

• знать структуру и состав используемого в Системе СПО, ППО, ТС и КС;

• знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, правил и процедур по защите информации и распоряжений, регламентирующих порядок действий по защите информации;

• знать в совершенстве применяемые в Системе информационные технологии и соблюдать требования технологического процесса обработки информации в Системе;

• управлять (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

• осуществлять установку, настройку, обновление СПО, ППО, ТС Системы;

• контролировать работоспособность СПО, ППО, ТС и КС;

• осуществлять установку СПО и ППО в соответствии с Регламентом по ограничению программной среды в государственной информационной системе «Управление выполнением формальных проверок возможности совершения юридически значимых действий»;

• осуществлять регистрацию пользователей СПО, ППО, ТС и предоставление им прав доступа в соответствии с требованиями организационно–распорядительных документов ФИПС и служебными обязанностями сотрудников;

• проводить периодический контроль установленного в Системе ППО, СПО в соответствии с Регламентом по ограничению программной среды в государственной информационной системе «Управление выполнением формальных проверок возможности совершения юридически значимых действий»;

• осуществлять контроль состава СПО, ППО, ТС в соответствии с Регламентом контроля защищенности за обеспечением требуемого уровня защищенности информации в государственной информационной системе «Управление выполнением формальных проверок возможности совершения юридически значимых действий»;

• принимать меры по ликвидации последствий нарушений, ошибок в действиях пользователей при работе с СПО, ППО, ТС, сбоев работоспособности и неисправностей компонентов СПО, ППО, ТС;

• в случае отказа работоспособности технических средств и программного обеспечения элементов Системы, принимать действия по их

своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

• обеспечивать размещение стационарных технических средств, обрабатывающих информацию, а также средств обеспечения функционирования в пределах контролируемой зоны;

• обеспечивать размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра;

• в случае появления сведений или подозрений о фактах нарушения правил работы с СПО, ППО, ТС, фактах несанкционированного доступа к информации в СПО, ППО, ТС, конфигурационным настройкам серверов ППО, несанкционированного изменения привилегий пользователей СПО, ППО, ТС немедленно сообщать об этом ответственному за защиту информации, обрабатываемой в Системе для организации проведения последующего служебного расследования;

• требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования Системы или средств защиты;

• обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт;

• присутствовать при выполнении технического обслуживания элементов Системы сторонними физическими лицами и организациями;

• участвовать в проведении мероприятий по обеспечению защиты информации в Системе, предусмотренных утвержденным Планом мероприятий по защите информации, обрабатываемой в Системе;

• обеспечивать резервирование ТС и периодическое резервное копирование информации на резервные машинные носители в соответствии с Правилами и процедуры по обеспечению доступности государственной информационной системы «Управление выполнением формальных проверок возможности совершения юридически значимых действий».

Администратору Системы запрещается:

• самовольно осуществлять допуск пользователей Системы к ресурсам Системы и изменять расположение информационных ресурсов и прав доступа в нарушение действующей разрешительной системы доступа;

• использовать для работы в Системы чужую учётную запись;

• использовать в своих личных интересах ресурсы Системы и предоставлять такую возможность другим;

• подключать локальную вычислительную сеть Системы к любым сетям передачи данных, не входящим в состав Системы;

• вносить какие-либо изменения в аппаратную составляющую ТС Системы, заменять и удалять комплектующие ТС Системы, изменять месторасположение ТС Системы;

• передавать третьим лицам тем или иным способом сетевые адреса, информацию об учётных записях пользователей Системы, их привилегиях;

• производить в рабочее время действия, приводящие к сбоям, остановке, замедлению работы Системы, блокированию доступа к информационным ресурсам Системы, риску потери информации без санкции ответственного за защиту информации, обрабатываемой в Системе и заблаговременного предупреждения пользователей Системы;

• нарушать правила эксплуатации оборудования Системы;

• корректировать и удалять журналы аудита СПО, ППО, средств защиты информации Системы.

5. Права Администратора Системы

Администратор Системы имеет право:

• осуществлять оперативное вмешательство в работу пользователей Системы, а также останавливать процессы обработки данных при служебной необходимости;

• участвовать в анализе ситуаций, касающихся функционирования Системы, и расследовании фактов несанкционированного доступа;

• требовать прекращения обработки информации в случае нарушения установленного порядка работы или нарушения функционирования средств и систем защиты Системы.

6. Ответственность Администратора Системы

Администратор Системы несет ответственность за:

• реализацию установленной разрешительной системы доступа;

• бесперебойное функционирование СПО, ППО, ТС, КС Системы;

• соответствие настроек СПО, ППО, ТС Системы организационно–распорядительной и эксплуатационной документации Системы;

• разглашение сведений ограниченного распространения, ставших известными в ходе выполнения служебных обязанностей;

• соблюдение требований по обеспечению безопасности информации в Системе в части выполняемых функций и требований настоящей инструкции;

• за ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

Приложение № 2
УТВЕРЖДЕНО
приказом
от 13 10 **20**22 **№** 158

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, обрабатываемой в государственных информационных системах:

Государственная информационная система контроля использования прав на результаты интеллектуальной деятельности (ГИС Контроль РИД)

Государственная информационная система интеграции и управления нормативно-справочной информацией (ГИС НИС)

Государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (ГИС Онлайн Роспатент)

2022 г.

Содержание

1. Назначение

Инструкция ответственного за обеспечение безопасности информации, обрабатываемой в государственных информационных системах контроля использования прав на результаты интеллектуальной деятельности, государственной информационной системы интеграции и управления нормативно-справочной информацией и государственной информационной системы «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (далее – Система) (далее – Инструкция) определяет задачи, функции, обязанности, права и ответственность администратора безопасности информации (далее – Администратор БИ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в Федеральном государственном бюджетном учреждении «Федеральный институт промышленной собственности» (далее – ФИПС).

2. Общие положения

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

Администратор БИ назначается из числа работников Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности» (далее – ФИПС).

3. Задачи и функции Администратора БИ

Основными задачами Администратора БИ являются:

- организация разграничения доступа;
- обеспечение функционирования и настройка средств защиты информации (далее – СрЗИ);
- контроль эффективности организационных и технических мер по защите информации.

Для выполнения поставленных задач на Администратора БИ возлагаются следующие функции:

- участие в разработке технологии обработки информации ограниченного распространения по вопросам:
  - организации порядка учёта, хранения и обращения с документами и носителями информации;
  - подготовки, согласования, утверждения инструкций, определяющих задачи, функции, права, обязанности и ответственность администраторов и пользователей Системы по вопросам защиты информации.
- ведение организационно–технической документации СИСТЕМЫ в рамках своих полномочий;
- учёт используемых в Системе СрЗИ, ведение документации на СрЗИ;
- установка и настройка СрЗИ, контроль функционирования СрЗИ на стадии эксплуатации Системы;
- управление настройками СрЗИ;
- контроль целостности общесистемной программной среды и программных СрЗИ;
- контроль выполнения пользователями Системы и Ответственного за эксплуатацию Системы (далее - Администратором Системы) требований действующих нормативных и методических документов по защите информации в Системе;

- контроль действий Администратора Системы;
- контроль привилегий пользователей Системы;
- проведение инструктажей сотрудников ФИПС, допускаемых к работе в Системе, в части обеспечения безопасности информации;
- консультация Администратора Системы и пользователей Системы по вопросам защиты информации.
- участие в служебных расследованиях причин утечки защищаемой информации и нарушения работоспособности Системы;
- контроль и аудит действий сотрудников сторонних организаций, выполняющих работы по установке, настройке, сопровождению и обслуживанию программного обеспечения Системы.

4. Обязанности Администратора БИ

Администратор БИ обязан:

- знать перечень установленных в Системе основных технических средств и систем (далее – ОТСС), СрЗИ, перечень задач, решаемых с их использованием, и пользователей, допущенных к их решению;
- осуществлять учет и периодический контроль за составом и полномочиями пользователей Системы;
- осуществлять контроль за работой пользователей Системы, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и реагировать на возникающие нештатные ситуации в рамках своей деятельности. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов;
- осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в Системе СрЗИ;
- присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СрЗИ;
- осуществлять периодическую проверку состояния используемых СрЗИ, осуществлять проверку правильности их настройки (выборочное тестирование);
- осуществлять контроль за управлением идентификаторами и средствами аутентификации (аутентификационной информацией) внутренних пользователей в Системе;
- осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием действий в случае утраты и (или) компрометации средств аутентификации в соответствии с Регламентом идентификации и аутентификации пользователей в Системе;
- осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в Системы программного обеспечения в соответствии с Регламентом по ограничению программной среды в Системе
- настраивать параметры журналов регистрации событий безопасности в соответствии с Регламентом мониторинга и регистрации событий информационной безопасности в Системе
- проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование;
- осуществлять контроль уровня защищенности информации, обрабатываемой в Системе, в соответствии с Регламентом контроля защищенности за обеспечением требуемого уровня защищенности информации в Системе;
- осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СрЗИ и принятие процедур, направленных на устранение выявленных недостатков;

• обеспечивать сохранность СрЗИ, эксплуатационной и технической документации к СрЗИ, а также порядок обращения со СрЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой в Системе с учетом с Правил и процедур по порядку обращения со средствами защиты информации в Системе;

• своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СрЗИ, установленных на СВТ Системы;

• осуществлять поэкземплярный учет в соответствующем журнале:

– СрЗИ (носителей дистрибутивов, системных блоков с установленными СрЗИ);

– эксплуатационной и технической документации к СрЗИ.

• осуществлять хранение:

– носителей дистрибутивов СрЗИ;

– лицензий и сертификатов на СрЗИ.

• осуществлять периодические проверки:

– состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);

– состояния линейно-кабельного оборудования локально-вычислительных сетей.

• проводить первоначальный, плановый и внеплановый инструктаж пользователей Системы по вопросам работы со СрЗИ;

• осуществлять взаимодействие с пользователями Системы по вопросам в рамках своих обязанностей;

• составлять инструкции по работе со СрЗИ;

• участвовать в выявлении инцидентов информационной безопасности и реагировании на них;

• управлять конфигурацией Системы и ее системой защиты информации;

• в случае возникновения нештатных ситуаций и аварийных ситуаций принимать действия по реагированию в пределах функций и полномочий с целью ликвидации последствий. Докладывать ответственному за защиту информации, обрабатываемой в Системе о случаях возникновения внештатных ситуаций и аварийных ситуаций. Принимать меры по восстановлению работоспособности элементов Системы;

Администратору БИ запрещается:

• использовать для работы в Системы чужую учётную запись;

• вносить изменения в программно–аппаратную часть Системы, не связанные с администрированием СрЗИ;

• отключать СрЗИ;

• использовать для обеспечения безопасности информации СрЗИ, не сертифицированные по требованиям безопасности информации (не прошедших в установленном порядке процедуру оценки соответствия СрЗИ);

• разглашать информацию о средствах и методах обеспечения безопасности информации в Системе;

• совершать действия, способствующие нарушению технологии обработки информации в Системе;

• производить в рабочее время действия, приводящие к сбоям, остановке, замедлению работы Системы, блокированию доступа к информационным ресурсам Системы, риску потери информации без санкции ответственного за защиту информации, обрабатываемой в ИС и заблаговременного предупреждения пользователей Системы;

• нарушать правила эксплуатации программных и технических средств Системы;

• корректировать, подменять и удалять журналы аудита СрЗИ;

• использовать не учтённые установленным порядком машинные носители информации.

5. Права администратора информационной безопасности

Администратор БИ имеет право:

- получать информацию обо всех проводимых и планируемых работах по обслуживанию программного обеспечения и технических средств Системы;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи, обрабатываемой в Системе и технических компонентов Системы;
- осуществлять вмешательство в работу пользователя Системы при выявлении угрозы безопасности информации, либо нарушения технологии обработки защищаемой информации;
- по согласованию с Администратором Системы производить анализ защищённости Системы путём применения программных средств контроля защищённости и имитации попыток несанкционированного доступа;
- непосредственно обращаться к пользователям Системы с требованием прекращения работы при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;
- в пределах своей компетенции сообщать ответственному за защиту информации, обрабатываемой в ИС обо всех недостатках в работе Системы и её системы защиты;
- вносить свои предложения по совершенствованию процедур защиты информации в Системе.

6. Ответственность Администратора БИ

Администратор БИ несет ответственность за:

- актуальность организационно–технической документации Системы;
- бесперебойную работу СрЗИ;
- соответствие настроек СрЗИ требованиям организационно–распорядительной и эксплуатационной документации Системы;
- разглашение сведений ограниченного распространения, ставших известными в ходе выполнения служебных обязанностей;
- соблюдение требований по обеспечению безопасности информации в Системе в части выполняемых функций и требований настоящей инструкции;
- за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

Приложение № 3
УТВЕРЖДЕНО
приказом
от 13 10 **20**22 **№** 158

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С государственными информационными системами:

Государственная информационная система контроля использования прав на результаты интеллектуальной деятельности (ГИС Контроль РИД)

Государственная информационная система интеграции и управления нормативно-справочной информацией (ГИС НИС)

Государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (ГИС Онлайн Роспатент)

2022 г.

Содержание

1. Назначение

Инструкция пользователя по обеспечению безопасности в государственной информационной системы контроля использования прав на результаты интеллектуальной деятельности, государственной информационной системы интеграции и управления нормативно-справочной информацией и государственной информационной системы «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (далее – Система) (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей Системы.

2. Общие положения

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

3. Обязанности пользователя

Пользователь Системы обязан:

- знать и выполнять требования:
  - настоящей Инструкции;
  - внутренних распорядительных документов по режиму обработки информации, учету, хранению и пересылке носителей информации, обеспечению безопасности информации, обрабатываемой в Системе»;
  - нормативных правовых актов действующего законодательства в области защиты информации.
- 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;
- хранить в тайне свой пароль доступа в Систему, а также информацию о системе защиты информации в Системе;
- в срок не позднее восьми часов предпринимать действия по информированию ответственного за эксплуатацию Системы (далее – администратор ИС) и/или администратора безопасности информации Системы (далее – Администратор БИ) в случае:
  - утраты носителя с информацией и/или при подозрении компрометации личных ключей и паролей;
  - нарушения целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах автоматизированного рабочего места пользователя (далее – АРМ) или иных фактов совершения попыток несанкционированного доступа к Системе;
  - несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств Системы.
- покидать рабочее место только после блокировки АРМ;
- 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 Системе программно-аппаратных средств защиты информации ставить в известность ответственного за эксплуатацию Системы (далее - администратора Системы).

Для получения консультаций по вопросам информационной безопасности и по использованию средств защиты информации (далее — СрЗИ) пользователь обращается к Администратору БИ.

Уборка помещений должна производиться в присутствии пользователя, имеющего доступ в помещение и постоянно в нем работающего.

Пользователю запрещается:

- передавать кому бы то ни было, устно или письменно, информацию, а также личные ключи и атрибуты доступа к ресурсам Системы, открыто осуществлять ввод персонального пароля в присутствии других лиц;
- использовать компоненты программного и аппаратного обеспечения Системы в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства (в том числе отключать (блокировать) СрЗИ);
- подключать к АРМ и корпоративной информационной сети неучтенные внешние машинные носители информации (далее — МНИ), мобильные и иные устройства;
- записывать и хранить информацию, обрабатываемую в Системе на неучтенных МНИ;
- оставлять включенным без присмотра АРМ, не активировав средства защиты информации от несанкционированного доступа (временную блокировку экрана);
- умышленно использовать недокументированные возможности 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 Системы и/или Администратора БИ;
- выносить технические средства Системы, на которых проводилась обработка информации, за пределы контролируемой зоны;
- перемещать АРМ, используемые для работы с Системе.

4. Права пользователя

Пользователь имеет право:

- получать доступ к информации, материалам, необходимым для безопасной эксплуатации системного программного обеспечения, прикладного программного обеспечения, аппаратной части АРМ;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи обрабатываемой в Системе и технических компонентов Системы;
- вносить свои предложения по совершенствованию процедур защиты информации в Системе.

5. Ответственность пользователя

Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации.

Пользователь несет ответственность за нарушения в работе Системы, вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей инструкцией.

Пользователь отвечает за правильность включения и выключения Системы и всех действий при работе с ним.

За нарушение порядка работы с документами или машинными носителями информации, пользователь Системы может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

Приложение № 4
УТВЕРЖДЕНО
приказом
от 13 10 **20**22 **№** 158

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ЗАЩИТУ ИНФОРМАЦИИ,
обрабатываемой в государственных информационных системах:

Государственная информационная система контроля использования прав на результаты интеллектуальной деятельности (ГИС Контроль РИД)

Государственная информационная система интеграции и управления нормативно-справочной информацией (ГИС НИС)

Государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (ГИС Онлайн Роспатент)

2022 г.

Оглавление

1. Назначение

Инструкция Ответственного за защиту информации, обрабатываемой в государственной информационной системе контроля использования прав на результаты интеллектуальной деятельности, государственной информационной системы интеграции и управления нормативно-справочной информацией и государственной информационной системы «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (далее – Система) (далее – Инструкция) определяет основные права и обязанности Ответственного за защиту информации, обрабатываемой в Системе (далее – Ответственный за защиту информации).

2. Общие положения

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

Ответственный за защиту информации назначается приказом числа работников Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности» (далее – ФИПС).

3. Задачи и функции Ответственного за защиту информации

Основной задачей Ответственного за защиту информации, обрабатываемой в Системе является организация работ по защите информации в Системе.

Для выполнения поставленных задач на Ответственного за защиту информации, обрабатываемой в Системе возлагаются следующие функции:

- организация подготовки Системы к аттестации по требованиям безопасности информации, периодическому контролю защищённости;
- организация контроля выполнения требований по безопасности информации в Системе.

4. Обязанности Ответственного за защиту информации

Ответственный за защиту информации обязан:

- знать и соблюдать требования действующих нормативных правовых актов, а также внутренних инструкций, правил и положений, регламентирующих порядок действий по защите информации при ее обработке в Системе;
- планировать мероприятия по защите информации в Системе;
- организовывать работы по аттестации Системы по требованиям безопасности информации;
- организовывать разработку организационно-распорядительных и технических документов на Систему;
- знать перечень задач, решаемых с использованием Системы, степень конфиденциальности и лиц, допущенных к решению этих задач;
- организовывать проведение с пользователями Системы занятий по изучению нормативных правовых и руководящих документов по вопросам защиты информации в Системе;
- организовывать контроль выполнения комплекса организационно–технических мероприятий по защите информации в Системе;

- организовывать работы по контролю эффективности мероприятий по защите информации в Системе;
- организовывать контроль учёта машинных носителей информации в Системе, их хранения и обращения с ними;
- контролировать правильность ведения технической документации на Систему;
- организовывать работы по устранению выявленных в результате контроля нарушений требований безопасности информации, обрабатываемой с использованием Системы;
- обеспечивать проведение служебных расследований по фактам и попыткам несанкционированного доступа к информации, обрабатываемой с использованием Системы;
- проводить анализ причин выявленных нарушений и недостатков в организации защиты информации в Системе;
- участвовать в проведении аттестационных испытаний;
- осуществлять организацию специальной подготовки (в том числе в системе дополнительного профессионального образования), Администратора информационной безопасности Системы (далее – Администратор БИ) по вопросам обеспечения безопасности информации;
- определять порядок эксплуатации средств защиты информации Системе;
- организовывать периодический контроль работоспособности средств защиты информации, применяемых в Системе.

Ответственному за защиту информации запрещается:

- выполнять функции по администрированию Системы;
- разглашать информацию о средствах и методах обеспечения безопасности информации в Системе;
- совершать действия, способствующие нарушению технологии обработки информации в Системе.

5. Права Ответственного за защиту информации

Ответственный за защиту информации имеет право:

- получать полный доступ ко всем информационным ресурсам, программным, аппаратным и техническим средствам Системы;
- участвовать в служебных расследованиях причин утечки защищаемой информации и нарушения работоспособности Системы.

6. Ответственность Ответственного за защиту информации

Ответственный за защиту информации несет ответственность за:

- разглашение сведений ограниченного распространения, ставших известными в ходе выполнения служебных обязанностей;
- соблюдение требований по обеспечению безопасности информации в Системе в части выполняемых функций и требований настоящей инструкции.

Приложение № 5
УТВЕРЖДЕНО
приказом
от 13 10 **20**22 **№** 158

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в государственных информационных системах:

Государственная информационная система контроля использования прав на результаты интеллектуальной деятельности (ГИС Контроль РИД)

Государственная информационная система интеграции и управления нормативно-справочной информацией (ГИС НИС)

Государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (ГИС Онлайн Роспатент)

2022 г.

Содержание

1. Назначение

Настоящая Инструкция определяет основные права и обязанности ответственного за организацию обработки персональных данных (далее – Информация), в государственной информационной системе контроля использования прав на результаты интеллектуальной деятельности, государственной информационной системы интеграции и управления нормативно-справочной информацией и государственной информационной системы «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (далее – Система).

2. Общие положения

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

Ответственный за организацию обработки персональных данных в Системе назначается приказом из числа работников Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности» (далее – ФИПС).

Ответственный за организацию обработки персональных данных в Системе получает указания непосредственно от руководителя ФИПС или иного уполномоченного лица и подотчетно ему.

3. Обязанности ответственного за организацию обработки персональных данных в Системе

Знать и соблюдать требования действующих нормативных правовых актов, а также внутренних инструкций, правил и положений, регламентирующих порядок действий по защите персональных данных при обработке в Системе.

Доводить до сведения работников ФИПС положения законодательства Российской Федерации о персональных данных, локальных актов ФИПС по вопросам обработки персональных данных, требований к защите персональных данных.

Проводить оценку вреда в ФИПС, который может быть причинен субъектам персональных данных в случае нарушения требований федерального законодательства по защите персональных данных.

Осуществлять внутренний контроль (проверки) за соблюдением ФИПС и его работников законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

Организовать прием и обработку обращений и запросов субъектов персональных данных (далее – ПДн) или их представителей и осуществлять контроль над приемом и обработкой таких обращений и запросов.

Осуществлять ведение Журнала учета обращений субъектов ПДн по вопросам обработки их ПДн в Системе (Приложение №1-3 к настоящей Инструкции).

4. Порядок проведения внутреннего контроля соответствия обработки информации требованиям законодательства

Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности персональных данных требованиям положений, указанных в п.3 настоящей Инструкции законов и принятых в соответствии с ними нормативно-правовых

актов, Политики по обработке персональных данных в Федеральном государственном бюджетном учреждении «Федеральный институт промышленной собственности», локальных актов ФИПС, регламентирующих обработку и защиту персональных данных.

Основными целями контроля обеспечения безопасности персональных данных являются сбор, анализ и обработка данных, необходимых для:

- контроля над реализацией положений законодательной базы и внутренних нормативных актов по обеспечению безопасности персональных данных в Системе;
- выявления нештатных (или злоумышленных) действий с персональными данными;
- обнаружения фактов несанкционированного доступа к Системе.

При проведении контроля должны использоваться стандартные процедуры документальной проверки, опрос и интервью с пользователями Системы. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего контроля в качестве дополнительного способа может применяться «проверка на месте», которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

5. Порядок работы с обращениями и запросами субъектов персональных данных

Ответственный за организацию обработки персональных данных в Системе организует прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществляет контроль над приемом и обработкой таких обращений и запросов в соответствии с Политикой по обработке персональных данных Системе.

6. Права ответственного за организацию обработки персональных данных в Системе

Ответственный за организацию обработки персональных данных в Системе имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач;
- проходить обучение (переподготовку) по защите персональных данных в учебных центрах и на курсах повышения квалификации;
- требовать от пользователей Системы знания и выполнения требований законодательства по защите персональных данных, локальных актов ФИПС по вопросам обработки персональных данных, требований по защите персональных данных;
- инициировать разбирательство и составление заключений по фактам нарушения пользователями Системы законодательства Российской Федерации о защите персональных данных;
- требовать прекращения обработки персональных данных в случае нарушения требований по защите персональных данных;
- участвовать в анализе ситуаций, касающихся нарушения требований по защите персональных данных и расследования фактов несанкционированного доступа к персональным данным.

7. Ответственность

Ответственный за организацию обработки персональных данных в Системе несет материальную, дисциплинарную, административную и уголовную ответственность:

- за неисполнение либо ненадлежащее исполнение должностных обязанностей;
- за нарушение законодательства, приказов, распоряжений руководства ФИПС, действующих нормативных документов по защите информации, в том числе персональных данных;
- за превышение должностных полномочий и злоупотребление ими;

- за разглашение информации, к которой он допущен в рамках выполнения своих функциональных обязанностей, посторонним лицам.

Приложение № 6
УТВЕРЖДЕНО
приказом
от 13 10 **20**22 **№** 158

ИНСТРУКЦИЯ ТЕХНИЧЕСКОГО АДМИНИСТРАТОРА
государственных информационных систем:

Государственная информационная система контроля использования прав на результаты интеллектуальной деятельности (ГИС Контроль РИД)

Государственная информационная система интеграции и управления нормативно-справочной информацией (ГИС НИС)

Государственная информационная система «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (ГИС Онлайн Роспатент)

2022 г.

Содержание

1. Назначение

Инструкция Технического администратора государственной информационной системы контроля использования прав на результаты интеллектуальной деятельности, государственной информационной системы интеграции и управления нормативно-справочной информацией и государственной информационной системы «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных» (далее – Система) (далее – Инструкция) определяет функции, права, обязанности и ответственность технического администратора Системы.

2. Общие положения

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

Технический администратор Системы назначается из числа работников Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности» (далее – ФИПС).

3. Задачи и функции Технический администратора Системы

Основными задачами Технического администратора Системы являются:

- обеспечение функционирования и настройка технических средств (далее – ТС) и кабельной системы (далее – КС) Системы;
- мониторинг функционирования ТС и КС.

Для выполнения поставленных задач на Технического администратора Системы возлагаются следующие функции:

- обеспечение работоспособности ТС и КС;
- ведение организационно-технической документации Системы в рамках своих полномочий;
- локализация, устранение сбоев и неисправностей в работе ТС и КС;
- настройка привилегий доступа пользователей к ресурсам ТС;
- практическая реализация мероприятий по защите информации в ТС и КС.

4. Обязанности Технического администратора Системы

Для реализации поставленных задач и возложенных функций Технический администратор Системы обязан:

- знать структуру и состав используемого в Системе ТС и КС;
- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, правил и процедур по защите информации и распоряжений, регламентирующих порядок действий по защите информации;
- знать в совершенстве применяемые в Системе информационные технологии и соблюдать требования технологического процесса обработки информации в Системе;
- осуществлять установку, настройку ТС Системы;
- контролировать работоспособность ТС и КС;
- осуществлять регистрацию пользователей ТС и предоставление им прав доступа в соответствии с требованиями организационно-распорядительных документов ФИПС и служебными обязанностями сотрудников;

• осуществлять контроль состава ТС в соответствии с Регламентом контроля защищенности за обеспечением требуемого уровня защищенности информации в Системе;

• принимать меры по ликвидации последствий нарушений, ошибок в действиях пользователей при работе с ТС, сбоев работоспособности и неисправностей компонентов ТС;

• в случае отказа работоспособности технических средств Системы, принимать действия по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

• обеспечивать размещение стационарных технических средств, обрабатывающих информацию, а также средств обеспечения функционирования в пределах контролируемой зоны;

• обеспечивать размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра;

• в случае появления сведений или подозрений о фактах нарушения правил работы с ТС, фактах несанкционированного доступа к информации в ТС, несанкционированного изменения привилегий пользователей ТС немедленно сообщать об этом ответственному за защиту информации, обрабатываемой в Системе для организации проведения последующего служебного расследования;

• требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования Системы или средств защиты;

• обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт;

• присутствовать при выполнении технического обслуживания элементов Системы сторонними физическими лицами и организациями;

• участвовать в проведении мероприятий по обеспечению защиты информации в Системе, предусмотренных утвержденным Планом мероприятий по защите информации, обрабатываемой в Системе;

• обеспечивать резервирование ТС и периодическое резервное копирование информации на резервные машинные носители в соответствии с Правилами и процедуры по обеспечению доступности Системы.

Администратору Системы запрещается:

• самовольно осуществлять допуск пользователей Системы к ресурсам Системы и изменять расположение информационных ресурсов и прав доступа в нарушение действующей разрешительной системы доступа;

• использовать в своих личных интересах ресурсы Системы и предоставлять такую возможность другим;

• подключать локальную вычислительную сеть Системы к любым сетям передачи данных, не входящим в состав Системы;

• вносить какие-либо изменения в аппаратную составляющую ТС Системы, заменять и удалять комплектующие ТС Системы, изменять месторасположение ТС Системы;

• передавать третьим лицам тем или иным способом сетевые адреса, информацию об учётных записях пользователей Системы, их привилегиях;

• производить в рабочее время действия, приводящие к сбоям, остановке, замедлению работы Системы, блокированию доступа к информационным ресурсам Системы, риску потери информации без санкции ответственного за защиту информации, обрабатываемой в Системе и заблаговременного предупреждения пользователей Системы;

- нарушать правила эксплуатации оборудования Системы;

5. Права Технического администратора Системы

Технический администратор Системы имеет право:

- осуществлять оперативное вмешательство в работу пользователей Системы, а также останавливать процессы обработки данных при служебной необходимости;
- участвовать в анализе ситуаций, касающихся функционирования Системы, и расследовании фактов несанкционированного доступа;
- требовать прекращения обработки информации в случае нарушения установленного порядка работы или нарушения функционирования средств и систем защиты Системы.

6. Ответственность Технического администратора Системы

Технический администратор Системы несет ответственность за:

- бесперебойное функционирование ТС, КС Системы;
- соответствие настроек ТС Системы организационно–распорядительной и эксплуатационной документации Системы;
- разглашение сведений ограниченного распространения, ставших известными в ходе выполнения служебных обязанностей;
- соблюдение требований по обеспечению безопасности информации в Системе в части выполняемых функций и требований настоящей инструкции;
- за ненадлежащее исполнение или неисполнение своих служебных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

Приложение № 1

к Инструкции ответственного за организацию обработки персональных данных в государственной информационной системе контроля использования прав на результаты интеллектуальной деятельности

ФОРМА

ЖУРНАЛ №____

учета обращений субъектов персональных данных по вопросам обработки их персональных данных в государственной информационной системе «контроля использования прав на результаты интеллектуальной деятельности

Начат ___ _____ 20___ г. На ____ листах

Окончен ___ _____ 20___ г.

_____ _____

(ФИО ответственного лица за ведение журнала) (подпись)

№ п/п	Дата обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении или отказе в предоставлении персональных данных (предоставлено/отказано)	Дата передачи/отказа в предоставлении персональных данных	Подпись запрашивающего лица	Подпись ответственного работника
1	2	3	4	5	6	7	8

Приложение № 2

к Инструкции ответственного за организацию обработки персональных данных в государственной информационной системе интеграции и управления нормативно-справочной информацией

ФОРМА

ЖУРНАЛ №____

учета обращений субъектов персональных данных по вопросам обработки их персональных данных в государственной информационной системе интеграции и управления нормативно-справочной информацией

Начат ___ _____ 20___ г. На ____ листах

Окончен ___ _____ 20___ г.

_____ _____

(ФИО ответственного лица за ведение журнала) (подпись)

№ п/п	Дата обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении или отказе в предоставлении персональных данных (предоставлено/отказано)	Дата передачи/отказа в предоставлении персональных данных	Подпись запрашивающего лица	Подпись ответственного работника
1	2	3	4	5	6	7	8

Приложение № 3

к Инструкции ответственного за организацию обработки персональных данных в государственной информационной системе «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных»

ФОРМА

ЖУРНАЛ №____

учета обращений субъектов персональных данных по вопросам обработки их персональных данных в государственной информационной системе «Омниканальное взаимодействие Роспатента с заинтересованными лицами в ходе предоставления государственных услуг, услуг в рамках международных соглашений и договоров, публикации общедоступной информации о деятельности в сфере регистрации и охраны объектов интеллектуальной собственности в формате открытых данных»

Начат ___ _____ 20___ г. На ____ листах

Окончен ___ _____ 20___ г.

_____ _____

(ФИО ответственного лица за ведение журнала) (подпись)

№ п/п	Дата обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении или отказе в предоставлении персональных данных (предоставлено/отказано)	Дата передачи/отказа в предоставлении персональных данных	Подпись запрашивающего лица	Подпись ответственного работника
1	2	3	4	5	6	7	8