



**МИНИСТЕРСТВО
АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА
СМОЛЕНСКОЙ ОБЛАСТИ**

П Р И К А З

«04» 08 2015

№ 141-02

Об утверждении документов в
области защиты информации в
Министерстве архитектуры и
строительства Смоленской области

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

п р и к а з ы в а ю :

1. Утвердить документы, необходимые для выполнения требований законодательства в области защиты информации:
 - План мероприятий по защите персональных данных (Приложение № 1);
 - Методику определения уровня защищенности персональных данных в информационных системах персональных данных (Приложение № 2);

- Правила работы с обезличенными персональными данными (Приложение № 3);
 - Правила обработки персональных данных без использования средств автоматизации (Приложение № 4);
 - Форму акта вскрытия АРМ (Приложение № 5);
 - Инструкцию о порядке действий во внештатных ситуациях и восстановлению после сбоя (Приложение № 6);
 - Инструкцию о порядке резервирования и восстановления после сбоя АРМ на базе автономной ПЭВМ (Приложение № 7);
 - Описание технологического процесса обработки персональных данных в ИСПДн «Бухгалтерия» Министерства архитектуры и строительства Смоленской области (Приложение № 8);
 - Описание технологического процесса обработки персональных данных в ИСПДн «Кадры» Министерства архитектуры и строительства Смоленской области (Приложение № 9);
 - Описание технологического процесса обработки персональных данных в ИС «Сайт» Министерства архитектуры и строительства Смоленской области (Приложение № 10);
2. Утвердить формы учетных журналов:
- Журнал инструктажа по защите ПДн (Приложение № 11);
 - Журнал учета процедур резервного копирования (Приложение № 12);
 - Журнал учета персональных паролей объектов вычислительной техники (Приложение № 13);
 - Журнал инструктажей по информационной безопасности (Приложение № 14);
 - Журнал учета мероприятий по контролю обеспечения защиты информации (Приложение № 15);
 - Журнал учета организационно-распорядительной документации по защите информации (Приложение № 16).
3. Ответственному за организацию обработки ПДн провести первичный инструктаж по утвержденным документам среди сотрудников Министерства архитектуры и строительства Смоленской области, участвующих в процессе обработки ПДн (с использованием и без использования средств автоматизации), под роспись в Журнале инструктажей по защите ПДн.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Министр



К.Н. Ростовцев

Приложение № 1

к приказу Министерства архитектуры и строительства Смоленской области

от «14» 08 2025 г. № 141-ОД

**План
мероприятий по обеспечению защиты персональных данных**

1. Настоящий План устанавливает порядок выполнения мероприятий по обеспечению защиты персональных данных (ПДн) Министерства архитектуры и строительства Смоленской области (далее по тексту – Министерство) и предназначен для описания комплекса действий, которые необходимо выполнить, чтобы определить, достигнуть и поддерживать уровень безопасности ПДн, в соответствии с действующим законодательством.

2. Данный процесс направлен на достижение следующих целей:

- Определение организационных мероприятий по защите ПДн;
- Определение технических мероприятий для защиты ИСПДн;
- Определение контролирующих мероприятий для поддержания уровня безопасности ПДн;
- Определение круга ответственных лиц, исполнителей и сроков проведения мероприятий по защите ПДн.

3. Настоящий документ обязаны знать и использовать в работе члены комиссии по проведению мероприятий по защите ПДн, назначенной приказом министра архитектуры и строительства Смоленской области.

4. Мероприятия:

№	Мероприятия	Срок выполнения Периодичность	Исполнитель
Организационные мероприятия			
1.	Разработка документов по защите ПДн, обрабатываемых с использованием средств автоматизации	Июль – август	Ответственный за обеспечение безопасности персональных данных
2.	Разработка документов по защите ПДн, обрабатываемых без использования средств автоматизации		
3.	Разработка форм учетных Журналов		
Технические мероприятия			
1.	Анализ моделей актуальных угроз с целью выявления необходимых средств защиты ПДн	Один раз в три месяца	Ответственный за обеспечение безопасности персональных данных
2.	Анализ рынка средств защиты ПДн	Один раз в полгода	

№	Мероприятия	Срок выполнения Периодичность	Исполнитель
	и их подбор под заданные требования		данных
3.	Внедрение системы защиты ПДн, выбранной на основании анализа модели угроз	По мере необходимости	
Контролирующие мероприятия			
1.	Контроль за работой пользователей с носителями ПДн	Один раз в три месяца	Ответственный за организацию обработки персональных данных
2.	Контроль над соблюдением парольной политики		
3.	Контроль над выполнением антивирусной защиты		
4.	Проверка знаний пользователями ИСПДн требований организационно-распорядительной документации Министерства	Один раз в полгода	
5.	Проверка знаний сотрудников Министерства, работающих с бумажными носителями ПДн, требований организационно-распорядительной документации		
7.	Организация пересмотра имеющихся угроз безопасности ПДн, а также анализа новых угроз	По мере необходимости	
8.	Поддержание в актуальном состоянии нормативно-организационных документов	Актуализация проводится в соответствии с изменениями законодательной базы	

5. Ответственность за выполнение организационных и технических мероприятий по защите ПДн несет ответственное лицо за обеспечение безопасности персональных данных в информационных системах Министерства, назначенный приказом министра архитектуры и строительства Смоленской области.

6. Ответственность за контролируемые мероприятия возлагается на ответственное лицо за организацию обработки ПДн, назначенное приказом министра архитектуры и строительства Смоленской области.

Методика
определения уровня защищенности персональных данных в информационных
системах персональных данных Министерства архитектуры и строительства
Смоленской области

1. Методика определения уровня защищенности персональных данных (ПДн) в информационных системах персональных данных (ИСПДн) Министерства архитектуры и строительства Смоленской области (далее по тексту – Министерство) предназначена для построения методики определения уровней защищенности ПДн в ИСПДн. Данный регламент может также использоваться в случаях переопределения уровня защищенности ПДн существующих и новых ИСПДн.

Настоящая Методика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О ПДн» и Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн».

Целью настоящего Регламента является определение уровня защищенности ПДн в ИСПДн.

Настоящий документ обязаны знать и использовать в работе члены комиссии по проведению мероприятий по защите ПДн, назначенной приказом министра архитектуры и строительства Смоленской области.

2. При обработке ПДн в информационных системах устанавливаются 4 уровня защищенности ПДн.

1-ый уровень защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории ПДн, либо биометрические ПДн, либо иные категории ПДн;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

2-ой уровень защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные ПДн;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории ПДн сотрудников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические ПДн;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

3-ий уровень защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные ПДн сотрудников оператора или общедоступные ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории ПДн сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории ПДн сотрудников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические ПДн;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

4-ый уровень защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные ПДн;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории ПДн сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

Определение типа информационных систем:

Информационная система является **информационной системой, обрабатывающей специальные категории ПДн**, если в ней обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн.

Информационная система является **информационной системой, обрабатывающей биометрические ПДн**, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным категориям ПДн.

Информационная система является **информационной системой, обрабатывающей общедоступные ПДн**, если в ней обрабатываются ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 Федерального закона "О ПДн".

Информационная система является **информационной системой, обрабатывающей иные категории ПДн**, если в ней не обрабатываются ПДн, указанные в абзацах первом - третьем настоящего пункта.

Информационная система является **информационной системой, обрабатывающей ПДн сотрудников оператора**, если в ней обрабатываются ПДн только указанных сотрудников. В остальных случаях информационная система ПДн является информационной системой, обрабатывающей ПДн субъектов ПДн, не являющихся сотрудниками оператора.

Определение типов актуальных угроз:

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3. Исходные данные.

Министерство является оператором ПДн физических лиц, состоящих с ним в трудовых отношениях (далее по тексту – сотрудники) и физических лиц, имеющих отношения с Министерством (далее по тексту – граждане).

Обработка ПДн сотрудников определяется:

- Трудовым Кодексом РФ;
- Федеральным законом РФ от 27.07.2004 № 79-ФЗ «О государственной гражданской службе».

Обработка ПДн граждан происходит на основании:

- Федерального закона РФ от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан РФ».

4. Описание ИСПДн.

ЛВС Министерства является доменной, в её состав входят 1 файловый сервер, 1 проху-сервер, 1 контроллер домена, 1 сервер резервного копирования и 45 АРМ.

Доступ в сеть общего пользования Интернет осуществляется со всех АРМ и организован через проху-сервер от провайдера ОАО «Ростелеком».

В Министерстве по целям обработки ПДн и категориям субъектов ПДн выделены две ИСПДн и одна ИС.

Назначение ИСПДн «Бухгалтерия» – ведение персонифицированного учета.

ИСПДн «Бухгалтерия» представлена 4 АРМ и 1 сервером.

Средствами обработки ПДн является пакет офисных приложений Microsoft Office, 1С: Предприятие Конфигурация: КАМИН: Расчет заработной платы.

В ИСПДн «Бухгалтерия» осуществляется взаимодействие с системами других организаций: Сбербанк бизнес, ГИИС ПУД ЭБ, ВТБ бизнес Онлайн.

Передача ПДн осуществляется по мере необходимости по защищенному каналу, через сеть Интернет.

Назначение ИСПДн «Кадры» – ведение персонифицированного учета.

ИСПДн «Кадры» представлена 4 АРМ.

Средствами обработки ПДн является пакет офисных приложений Microsoft Office.

В ИСПДн «Кадры» осуществляется взаимодействие с системами других организаций: «Контур-Эксперт» (Пенсионный фонд Российской Федерации), портал государственной гражданской службы.

Передача ПДн осуществляется по мере необходимости по защищенному каналу, через сеть Интернет.

Назначение ИС «Сайт» – предоставление доступа пользователям к сервисам, информации и материалам на сайте. Улучшение обслуживания пользователей с учетом положений законодательства.

ИС «Сайт» представлена 3 АРМ.

К информационным ресурсам ИС «Сайт» осуществляется удаленный доступ с помощью подключения через браузер.

5. Доступ к ПДн и ИСПДн.

Доступ к ИСПДн и ИС имеют только сотрудники Министерства, в соответствии с Матрицей доступа. Обслуживание технических и программных средств осуществляется собственными специалистами Министерства.

Правила работы с обезличенными персональными данными

1. Настоящие Правила работы с обезличенными персональными данными (ПДн) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящие Правила определяют порядок работы с обезличенными ПДн в Министерстве архитектуры и строительства Смоленской области (далее по тексту – Министерство).

2. Обезличивание ПДн.

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

– ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

– обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

– обезличивание ПДн – действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн.

Обезличивание ПДн может быть проведено с целью снижения ущерба от разглашения защищаемых ПДн, снижения класса ИСПДн Министерства и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки ПДн:

– уменьшение перечня обрабатываемых сведений;

– замена части сведений идентификаторами;

– обобщение – понижение точности некоторых сведений;

– понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город)

– деление сведений на части и обработка в разных информационных системах;

– другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня ПДн.

Для обезличивания ПДн годятся любые способы, явно не запрещенные законодательно.

Перечень должностей Министерства, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн, приведен в Приложении к настоящим Правилам.

Министр архитектуры и строительства Смоленской области, по заявлению начальников подразделений, где обрабатываются ПДн, принимает решение о необходимости обезличивания ПДн, а ответственный за организацию обработки ПДн осуществляет непосредственное обезличивание выбранным способом.

3. Работа с обезличенными ПДн.

Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем;

При обработке обезличенных ПДн без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

Приложение
к Приложению № 3
Правил работы с
обезличенными
персональными данными

**Перечень
должностей, ответственных за проведение мероприятий по
обезличиванию обрабатываемых ПДн**

1. Министр архитектуры и строительства Смоленской области.
2. Заместитель министра.
3. Начальник отдела — главный бухгалтер отдела бухгалтерского учета, отчетности и планирования расходов.
4. Начальник отдела правового и кадрового обеспечения.
5. Начальник отдела цифровизации и информационных систем.

Правила обработки персональных данных без использования средств автоматизации

1. Общие положения.

1.1. Обработка персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если обработка персональных данных осуществляется без помощи средств вычислительной техники.

1.2. Категории обрабатываемых персональных данных и категории субъектов персональных данных, а также цели обработки персональных данных указаны в утвержденном положении о защите и обработке персональных данных.

1.3. В Министерстве архитектуры и строительства Смоленской области не обрабатываются биометрические и специальные категории персональных данных.

1.4. Обработка персональных данных без использования средств автоматизации осуществляется на законной и справедливой основе. Обработка персональных данных без использования средств автоматизации не может быть использована Министерством архитектуры и строительства Смоленской области или его работниками в целях причинения материального и морального вреда субъектам персональных данных, затруднения реализации их прав и свобод.

1.5. Настоящие правила обработки персональных данных без использования средств автоматизации (далее – Правила) разработаны и утверждены в целях обеспечения безопасности персональных данных, обрабатываемых в Министерстве архитектуры и строительства Смоленской области без использования средств автоматизации, и исполнения требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

1.6. Настоящие Правила являются внутренним локальным актом Министерства архитектуры и строительства, вступают в силу с момента их утверждения министра архитектуры и строительства Смоленской области и действуют бессрочно до их замены новым документом.

1.7. Ответственность за актуализацию настоящих Правил и контроль над выполнением настоящих Правил возлагаются на ответственное лицо за организацию обработки персональных данных.

2. Особенности организации обработки персональных данных, осуществляемых без использования средств автоматизации.

2.1. В Министерстве архитектуры и строительства Смоленской области без использования средств автоматизации обрабатываются персональные данные работников, соискателей и контрагентов.

2.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

2.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. К обработке персональных данных без использования средств автоматизации допущены только те работники, которые указаны в утвержденных в перечнях лиц, допущенных к обработке персональных данных.

2.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, подписывают соглашение о неразглашении персональных данных.

2.6. При использовании типовых форм документов характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

2.7. Журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию Министерства архитектуры и строительства Смоленской области, не ведутся.

2.8. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

2.9. Для уничтожения персональных данных на материальных носителях в Министерстве архитектуры и строительства Смоленской области утвержден состав комиссии по уничтожению персональных данных, а также утверждена форма уничтожения персональных данных.

2.10. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. С целью обеспечения безопасности персональных данных при их обработке без использования средств автоматизации приказом министра архитектуры и строительства Смоленской области определены места хранения персональных данных, а также назначены ответственные за обеспечение конфиденциальности персональных данных при их хранении.

3.2. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях (разные места хранения для разных категорий субъектов персональных данных).

3.3. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, определены в Положении о защите и обработке персональных данных в Министерстве архитектуры и строительства Смоленской области.

Приложение № 5
к приказу Министерства
архитектуры и строительства
Смоленской области
от «04» 08 2025 г. № 141-ОД

АКТ № _____
от _____ 202_ г.
вскрытия автоматизированного рабочего места

№ п/п	Инвентарный номер автоматизирова нного рабочего места	Местонахождение автоматизированн ого рабочего места (подразделение, номер кабинета)	Причина вскрытия автоматизированн ого рабочего места	Ф.И.О. ответственного за снятие пломбы с автоматизированно го рабочего места

До вскрытия автоматизированного рабочего места, установлена полная сохранность пломбы серийный номер _____.

(должность)

(подпись)

(Ф.И.О.)

Инструкция

о порядке действий во внештатных ситуациях и восстановлению после сбоя

1. Настоящая Инструкция устанавливает порядок действий во внештатных ситуациях и действий сотрудников Министерства архитектуры и строительства Смоленской области.

Целью настоящей Инструкции является определение основных мер, методов и средств сохранения (поддержания) работоспособности ИСПДн при возникновении различных внештатных ситуаций, а также способов и средств восстановления информации и процессов ее обработки в случае нарушения работоспособности ИСПДн и ее основных компонентов.

2. Общие требования.

Источники информации о возникновении внештатной ситуации:

- пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
- средства защиты, обнаружившие кризисную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной внештатной ситуации, должны немедленно информировать в устной форме ответственным за организацию обработки персональных данных (ПДн). Дальнейшие действия по устранению причин нарушения работоспособности информационной системы персональных данных (ИСПДн), возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая внештатная ситуация должна анализироваться ответственным за организацию обработки ПДн. По результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости должно проводиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Серьезная и угрожающая внештатная ситуация может требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или

угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Все программные средства, используемые в системе, должны иметь эталонные (дистрибутивные) копии.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала – системные администраторы и ответственный за организацию обработки ПДн.

3. Меры обеспечения непрерывной работы и восстановления.

Технические меры:

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения внештатных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. Д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;

– технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

Организационные меры:

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых ПДн – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведении процедуры резервного копирования, должны отражаться в Журнале учета процедур резервного копирования, который ведет ответственный за организацию обработки ПДн.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4. Действия персонала при возникновении внештатных ситуаций.

Сотрудник обнаруживший сбой в работе ИСПДн в результате внештатной ситуации должен незамедлительно поставить в известность ответственного за организацию обработки ПДн.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за организацию обработки ПДн предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

Инструкция **о порядке резервирования и восстановления после сбоя** **автоматизированного рабочего места на базе автономной ПЭВМ**

1. Общие положения.

1.1. Настоящая Инструкция устанавливает порядок резервирования и восстановления после сбоев АРМ.

1.2. Целью настоящей Инструкции является определение основных мер, методов и средств сохранения (поддержания) работоспособности АРМ, а также способов и средств восстановления информации и процессов ее обработки в случае нарушения работоспособности АРМ и его основных компонентов.

2. Общие требования.

2.1. Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

2.2. Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

2.3. Все программные средства, используемые в системе, должны иметь эталонные (дистрибутивные) копии.

2.4. Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

3. Меры обеспечения непрерывной работы и восстановления.

3.1. Технические меры:

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения внештатных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.1.2. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств АРМ в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.3. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АРМ, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.1.4. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

3.1.5. Для обеспечения отказоустойчивости критичных компонентов АРМ при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов АРМ должны использоваться территориально удаленные системы кластеров.

3.1.6. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.1.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2. Организационные меры:

3.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемой конфиденциальной информации – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы АРМ – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведении процедуры резервного копирования, должны отражаться в Журнале учета процедур резервного копирования.

3.2. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.3. Носители должны храниться в негорючем шкафу или помещении, оборудованном системой пожаротушения.

3.4. Носители должны храниться не менее года, для возможности восстановления данных.

**Описание технологического процесса
обработки персональных данных в ИСПДн «Бухгалтерия» Министерства
архитектуры и строительства Смоленской области**

1. Общие положения.

1.1. Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1.2. Технологический процесс обработки информации предназначен для обеспечения защиты информации, носителя информации или информационного процесса, в отношении которых необходимо обеспечивать защиту.

1.3. Под технологией обработки информации понимаются информационные процессы, т.е. процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

1.4. В процессе обработки информации на АС участвуют пользователи, имеющие доступ к АС, в соответствии с утвержденной разрешительной системой доступа.

1.5. Субъекты доступа в ИСПДн «Бухгалтерия» указаны в Перечне сотрудников, осуществляющих обработку персональных данных и имеющих доступ к персональным данным, обрабатываемым в ИСПДн «Бухгалтерия» и на бумажных носителях в Министерстве архитектуры и строительства Смоленской области. Все пользователи, допущенные к обработке защищаемой информации зарегистрированы в установленной системе защиты информации от несанкционированного доступа (далее – НСД).

2. Описание входной информации.

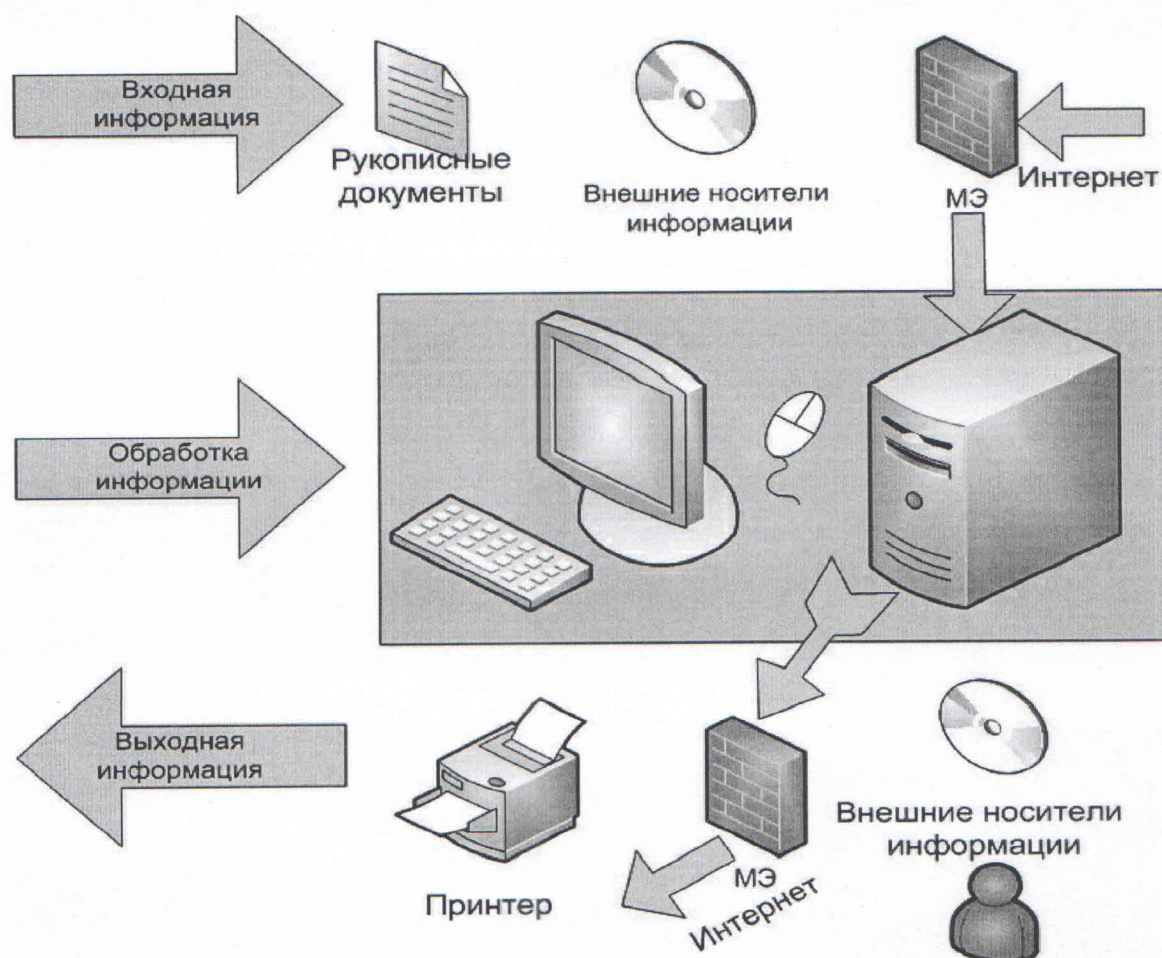
Входная информация может:

- поступать от сторонней организации на бумажных, оптических носителях, по защищенным каналам связи, через Интернет.
- подготавливаться на других аттестованных АС данной организации и передаваться в АС на бумажных или цифровых носителях.

3. Описание выходной информации.

Выходная информация может:

- хранится на НЖМД;
- передаваться на учтенных цифровых носителях;
- распечатываться на принтере;
- передаваться по защищенным каналам связи, через Интернет.



4. Перечень используемого программного обеспечения:

1.	Общесистемное программное обеспечение	- Windows 10 Pro; Windows Server 2012 R2; Server 2008 SP2 Datacenter
2.	Прикладное программное обеспечение	- 1С: Предприятие Конфигурация: КАМИН: Расчет заработной платы; - Пакет офисных приложений Microsoft Office; - 1С: Предприятие Конфигурация: 1С: Бухгалтерия
3.	Средства защиты информации	Криптографическая защита: - «КриптоПро CSP» версия 4.0 R4 (исполнение 1-Base) (Сертифицирующий орган ФСБ России № СФ/114-4716 от 15.01.2024 действителен до 15.01.2026) Межсетевое экранирование: - средство защиты информации Secret Net Studio (Сертифицирующий орган ФСТЭК России № 3745 от 16.05.2017 действителен до 16.05.2025) Антивирусная защита: - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСБ России № СФ/СЗИ-0523 от 15.12.2021 действителен до 15.12.2022)

	01.11.2026; Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029) Контроль съемных машинных носителей информации: - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029)
--	---

Работа с программными средствами производится в соответствии с эксплуатационной документацией на данные средства.

5. В технологическом процессе обработки информации задействованы следующие средства вычислительной техники:

АРМ 1:

Имя компьютера	OC-108-ZK-D10.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz
Материнская плата:	Asus H110M-K
ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-60WN4A1 CT480BX500SSD1
Видео карта:	Intel (R) HD Graphics 530
Звуковой адаптер:	Realtek Digital Output (Realtek High Definition Audio)
CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340074
Монитор (инв. или сер. номер)	23,6 ЛОС инв. 1101340074
МФУ (инв. или сер. номер)	HP LaserJet Pro MFPro M4289fdn инв. 1101340277 HP LaserJet M236sdn инв. 1101340321
Сетевая плата	Realtek PCIe GbE Family Controller

АРМ 2:

Имя компьютера	OC-108-ZK-D11.admin-smolensk.ru
ЦП:	11th Gen Intel(R) Core(TM) i5-11400 @ 2.60 GHz
Материнская плата:	Asus H610
ОЗУ:	16,00 ГБ
Жесткий диск:	FOXLINE FLSSD512X5SE
Видео карта:	Intel (R) UHD Graphics 730
Звуковой адаптер:	HDMI (HD Audio Driver for Display Audio)
CD-ROM:	MATSHITA DVD-RAM UJ8E2
Моноблок (инв. или сер. номер)	NERPA Saimaa 27 инв. 1101340330
МФУ (инв. или сер. номер)	HP LaserJet Pro 400MFP m425dn инв. 1101340039
Сетевая плата	Realtek PCIe GbE Family Controller

АРМ 3:

Имя компьютера	OC-108-ZK-D08.admin-smolensk.ru
ЦП:	11th Gen Intel(R) Core(TM) i5-11400 @ 2.60 GHz
Материнская плата:	Asus H610
ОЗУ:	16,00 ГБ
Жесткий диск:	FOXLINE FLSSD512X5SE
Видео карта:	Intel (R) UHD Graphics 730
Звуковой адаптер:	HDMI (HD Audio Driver for Display Audio)
CD-ROM:	MATSHITA DVD-RAM UJ8E2
Моноблок (инв. или сер. номер)	NERPA Saimaa 27 инв. 1101340329
Принтер (инв. или сер. номер)	Canon i-sensys LBP-6000 инв. 1101040138
Сетевая плата	Realtek PCIe GBE Family Controller

АРМ 4:

Имя компьютера	OC-104-ZK-D08.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i3-9100 CPU @ 3.60GHz
Материнская плата:	ASUS H110M-K
ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-22MFCA0
Видео карта:	Intel (R) UHD Graphics 630
Звуковой адаптер:	Realtek ® Audio
CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340074
Монитор (инв. или сер. номер)	LG24MK430H 23.8" инв. 1101340302
Сетевая плата	Realtek PCIe GbE Family Controller

Сервер:

Имя компьютера	OC-RDP1C-03
ЦП:	Intel(R) Xeon(R) E-2236 CPU @ 3.40 GHz 3.40GHz
Материнская плата:	Supermicro X11SCZ-F
ОЗУ:	64,0
Жесткий диск:	Intel Raid 1 Volume
Видео карта:	Базовый видеоадаптер (Майкрасофт)
Системный блок (инв. или сер. номер)	1101340326
Сетевая плата	Intel® I210 Gigabit Network Connection

6. Порядок работы.

6.1. Для работы в АС пользователь должен получить у ответственного лица за обеспечение безопасности персональных данных в ИС:

- персональный идентификатор или персональный логин и пароль для начальной идентификации и аутентификации;
- изучить организационно-распорядительную документацию.

6.2. Перед началом каждого сеанса работы пользователь должен удостовериться, что на корпусе АРМ отсутствуют следы вскрытия;

6.3. Подготовка персонального компьютера (далее – ПК) к работе:

включить источник бесперебойного питания, включить системный блок и монитор;

после загрузки операционной системы необходимо ввести логин и пароль для входа. При отсутствии НСД произойдет загрузка операционной системы. При нарушении или сбое системы защиты от НСД и при отказе загрузки операционной системы – прекратить работу и пригласить ответственное лицо за обеспечение безопасности персональных данных в ИС.

6.4. На АС разрешается обрабатывать информацию с меткой ДСП начальнику отдела – главному бухгалтеру (или лицу, исполняющему обязанности начальника отдела) и не конфиденциальную информацию всем пользователям ИСПДн «Бухгалтерия».

6.5. Пользователь, используя штатные средства доступа АРМ, выполняет ввод, обработку, вывод информации на учтенные носители (обрабатываемые файлы должны размещаться только в папках пользователей, список папок и права по доступу для каждого пользователя описаны в разрешительной системе доступа). Документы с меткой «ДСП» могут размещаться только в папках с меткой «ДСП».

6.6. Если во время работы на ПК появилась необходимость временно покинуть рабочее место, исполнитель обязан заблокировать ПК, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование ПК производится набором пароля разблокировки, который был создан при настройке системы блокировки.

7. Описание реализованных правил разграничения доступа.

7.1. Обработка информации осуществляется только на предварительно учтенных носителях информации (защищаемых ресурсах – ЖМД), прошедших антивирусный контроль.

7.2. Исполнителю запрещается:

- обрабатывать информацию в присутствии посторонних лиц;
- записывать информацию на неучтенных в специальной части носителях информации, листах бумаги и т. д.;
- использовать в работе пароли, если есть подозрение на их компрометацию;
- разглашать сведения о применяемой системе защиты и содержании информации;
- изменять и тиражировать программное обеспечение.

8. Порядок работы ответственного лица за обеспечение безопасности персональных данных в ИС.

8.1. Ответственное лицо за обеспечение безопасности персональных данных в ИС регистрирует факт выдачи персональных идентификаторов, имена пользователей и пароли в соответствующем журнале учета.

8.2. Ответственное лицо за обеспечение безопасности персональных данных в ИС безопасности проводит контроль защиты от несанкционированного доступа в соответствии с инструкцией безопасности и эксплуатационной документацией на соответствующие элементы системы защиты.

9. Режим технического обслуживания и ремонта.

9.1. При выходе из строя ОТСС АС, обработка персональных данных на данном ОТСС прекращается. Если вышедшее из строя ОТСС является составной частью АРМ (клавиатура, монитор и т.д.), то прекращается обработка информации на АРМ.

О случившемся ставится в известность ответственное лицо за обеспечение безопасности персональных данных в ИС. При необходимости вскрытия корпуса ОТСС составляется Акт о вскрытии по установленной в организации форме. Ремонт и (или) техническое обслуживание производится специалистами в присутствии ответственных лиц.

9.2. В случае передачи технических средств сторонним организациям, ОТСС АС после ремонта проходят дополнительные мероприятия по защите (в этом случае передача носителей информации «НЖМД» запрещена и не производится).

10. Отклонения от штатного режима технологического процесса.

В случае возникновения режима функционирования АС, не предусмотренного представленной технологией, обработка информации прекращается, и ставятся в известность ответственное лицо за обеспечение безопасности персональных данных в ИС для принятия соответствующих мер.

**Описание технологического процесса
обработки персональных данных в ИСПДн «Кадры» Министерства
архитектуры и строительства Смоленской области**

1. Общие положения.

1.1. Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1.2. Технологический процесс обработки информации предназначен для обеспечения защиты информации, носителя информации или информационного процесса, в отношении которых необходимо обеспечивать защиту.

1.3. Под технологией обработки информации понимаются информационные процессы, т.е. процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

1.4. В процессе обработки информации на АС участвуют пользователи, имеющие доступ к АС, в соответствии с утвержденной разрешительной системой доступа.

1.5. Субъекты доступа в ИСПДн «Кадры» указаны в Перечне сотрудников, осуществляющих обработку персональных данных и имеющих доступ к персональным данным, обрабатываемым в ИСПДн «Кадры» и на бумажных носителях в Министерстве архитектуры и строительства Смоленской области. Все пользователи, допущенные к обработке защищаемой информации зарегистрированы в установленной системе защиты информации от несанкционированного доступа (далее – НСД).

2. Описание входной информации.

Входная информация может:

- поступать от сторонней организации на бумажных, оптических носителях, по защищенным каналам связи, через Интернет.
- подготавливаться на других аттестованных АС данной организации и передаваться в АС на бумажных или цифровых носителях.

3. Описание выходной информации.

Выходная информация может:

- хранится на НЖМД;
- передаваться на учтенных цифровых носителях;
- распечатываться на принтере;
- передаваться по защищенным каналам связи, через Интернет.



4. Перечень используемого программного обеспечения:

1.	Общесистемное программное обеспечение	- Windows 7 Профессиональная; Windows 10 Pro
2.	Прикладное программное обеспечение	- Пакет офисных приложений Microsoft Office
3.	Средства защиты информации	Криптографическая защита: - «КриптоПро CSP» версия 4.0 R4 (исполнение 1-Base) (Сертифицирующий орган ФСБ России № СФ/114-4716 от 15.01.2024 действителен до 15.01.2026) Средство защиты информации: - ViPNet Client 4 версии 4.5 (Сертифицирующий орган ФСБ России № СФ/124-4778 от 05.03.2024 действителен до 28.02.2026) Антивирусная защита: - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСБ России № СФ/СЗИ-0523 от 15.12.2021 действителен до 01.11.2026; Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029)

	Контроль съемных машинных носителей информации: - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029)
--	--

Работа с программными средствами производится в соответствии с эксплуатационной документацией на данные средства.

5. В технологическом процессе обработки информации задействованы следующие средства вычислительной техники:

АРМ 1:

Имя компьютера	OC-407-ZK-D14.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz
Материнская плата:	ASUS TUF GAMING B560-PLUS WIFI
ОЗУ:	32,00 ГБ
Жесткий диск:	WDC WD10EZEX-00BBHA0
Видео карта:	Intel (R) UHD Graphics 630
Звуковой адаптер:	Realtek Digital Output (Realtek (R) Audio)
CD-ROM:	ATA DRW-24D5MT
Системный блок (инв. или сер. номер)	инв. 1101340317
Монитор (инв. или сер. номер)	MSI PRO MP 271 s/n PA2T542804722
МФУ (инв. или сер. номер)	HP инв. 1101340033
Сетевая плата	Realtek Gamig 2.5GbE Family Controller

АРМ 2:

Имя компьютера	OC-407-ZK-D11.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz
Материнская плата:	ASUS PRIME H510M-K
ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-00BBHA0 CT250MX500SSD1
Видео карта:	Intel (R) UHD Graphics 630
Звуковой адаптер:	Realtek Digital Output (Realtek (R) Audio)
CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340077
Монитор (инв. или сер. номер)	23,6 ViewSonic инв. 1101340077 s/n UG0162223268
МФУ (инв. или сер. номер)	Brother MFC-L2700DNR инв. 101340309
Сетевая плата	Intel(R) Ethernet Connection (14) I219-V

АРМ 3:

Имя компьютера	OC-407-ZK-D01.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i3-9100 CPU @ 3.60GHz
Материнская плата:	GIGABYTE B365M D3H

ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-22MFCA0
Видео карта:	Intel(R) UHD Graphics 630
Звуковой адаптер:	Realtek Digital Output (Realtek (R) Audio)
CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340304
Монитор (инв. или сер. номер)	LG 24MK430H 23.8" инв. 1101340304 s/n 009NTZN7S093
МФУ (инв. или сер. номер)	HP LaserJet Pro 4103dw s/n CNCRS6R5DF
Сетевая плата	Intel(R) Ethernet Connection (2) I219-V

АРМ 4:

Имя компьютера	OC-407-ZK-D12.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz
Материнская плата:	ASUS H110M-A/M.2
ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-60WN4A0 SCSI Disk Device
Видео карта:	Intel(R) HD Graphics 530
Звуковой адаптер:	Realtek High Definition Audio
CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340076
Монитор (инв. или сер. номер)	23,6 ViewSonic инв. 1101340076
Принтер (инв. или сер. номер)	Canon i-sensys LBP 6000 инв. 1101340025
Операционная система	Windows 7 Профессиональная
Сетевая плата	Intel(R) Ethernet Connection (2) I219-V

6. Порядок работы.

6.1. Для работы в АС пользователь должен получить у ответственного лица за обеспечение безопасности персональных данных в ИС:

- персональный идентификатор или персональный логин и пароль для начальной идентификации и аутентификации;
- изучить организационно-распорядительную документацию.

6.2. Перед началом каждого сеанса работы пользователь должен удостовериться, что на корпусе АРМ отсутствуют следы вскрытия;

6.3. Подготовка персонального компьютера (далее – ПК) к работе:

включить источник бесперебойного питания, включить системный блок и монитор;

после загрузки операционной системы необходимо ввести логин и пароль для входа. При отсутствии НСД произойдет загрузка операционной системы. При нарушении или сбое системы защиты от НСД и при отказе загрузки операционной системы – прекратить работу и пригласить ответственное лицо за обеспечение безопасности персональных данных в ИС.

6.4. На АС разрешается обрабатывать информацию с меткой ДСП начальнику отдела (или лицу, исполняющему обязанности начальника отдела) и не конфиденциальную информацию всем пользователям ИСПДн «Кадры».

6.5. Пользователь, используя штатные средства доступа АРМ, выполняет ввод, обработку, вывод информации на учетные носители (обрабатываемые файлы должны размещаться только в папках пользователей, список папок и права по доступу для каждого пользователя описаны в разрешительной системе доступа). Документы с меткой «ДСП» могут размещаться только в папках с меткой «ДСП».

6.6. Если во время работы на ПК появилась необходимость временно покинуть рабочее место, исполнитель обязан заблокировать ПК, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование ПК производится набором пароля разблокировки, который был создан при настройке системы блокировки.

7. Описание реализованных правил разграничения доступа.

7.1. Обработка информации осуществляется только на предварительно учетных носителях информации (защищаемых ресурсах – ЖМД), прошедших антивирусный контроль.

7.2. Исполнителю запрещается:

- обрабатывать информацию в присутствии посторонних лиц;
- записывать информацию на неучтенных в специальной части носителях информации, листах бумаги и т. д.;
- использовать в работе пароли, если есть подозрение на их компрометацию;
- разглашать сведения о применяемой системе защиты и содержании информации;
- изменять и тиражировать программное обеспечение.

8. Порядок работы ответственного лица за обеспечение безопасности персональных данных в ИС.

8.1. Ответственное лицо за обеспечение безопасности персональных данных в ИС регистрирует факт выдачи персональных идентификаторов, имена пользователей и пароли в соответствующем журнале учета.

8.2. Ответственное лицо за обеспечение безопасности персональных данных в ИС безопасности проводит контроль защиты от несанкционированного доступа в соответствии с инструкцией безопасности и эксплуатационной документацией на соответствующие элементы системы защиты.

9. Режим технического обслуживания и ремонта.

9.1. При выходе из строя ОТСС АС, обработка персональных данных на данном ОТСС прекращается. Если вышедшее из строя ОТСС является составной частью АРМ (клавиатура, монитор и т.д.), то прекращается обработка информации на АРМ.

О случившемся ставится в известность ответственное лицо за обеспечение безопасности персональных данных в ИС. При необходимости вскрытия корпуса ОТСС составляется Акт о вскрытии по установленной в организации форме. Ремонт и (или) техническое обслуживание производится специалистами в присутствии ответственных лиц.

9.2. В случае передачи технических средств сторонним организациям, ОТСС АС после ремонта проходят дополнительные мероприятия по защите (в этом случае передача носителей информации «НЖМД» запрещена и не производится).

10. Отклонения от штатного режима технологического процесса.

В случае возникновения режима функционирования АС, не предусмотренного представленной технологией, обработка информации прекращается, и ставятся в известность ответственное лицо за обеспечение безопасности персональных данных в ИС для принятия соответствующих мер.

**Описание технологического процесса
обработки персональных данных в ИС «Сайт» Министерства архитектуры и
строительства Смоленской области**

1. Общие положения.

1.1. Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1.2. Технологический процесс обработки информации предназначен для обеспечения защиты информации, носителя информации или информационного процесса, в отношении которых необходимо обеспечивать защиту.

1.3. Под технологией обработки информации понимаются информационные процессы, т.е. процессы создания, обработки, хранения, защиты от внутренних и внешних угроз, передачи, получения, использования и уничтожения информации.

1.4. В процессе обработки информации на АС участвуют пользователи, имеющие доступ к АС, в соответствии с утвержденной разрешительной системой доступа.

1.5. Субъекты доступа в ИС «Сайт» указаны в Перечне сотрудников, осуществляющих обработку персональных данных и имеющих доступ к персональным данным, обрабатываемым в ИС «Сайт» и на бумажных носителях в Министерстве архитектуры и строительства Смоленской области. Все пользователи, допущенные к обработке защищаемой информации зарегистрированы в установленной системе защиты информации от несанкционированного доступа (далее – НСД).

2. Описание входной информации.

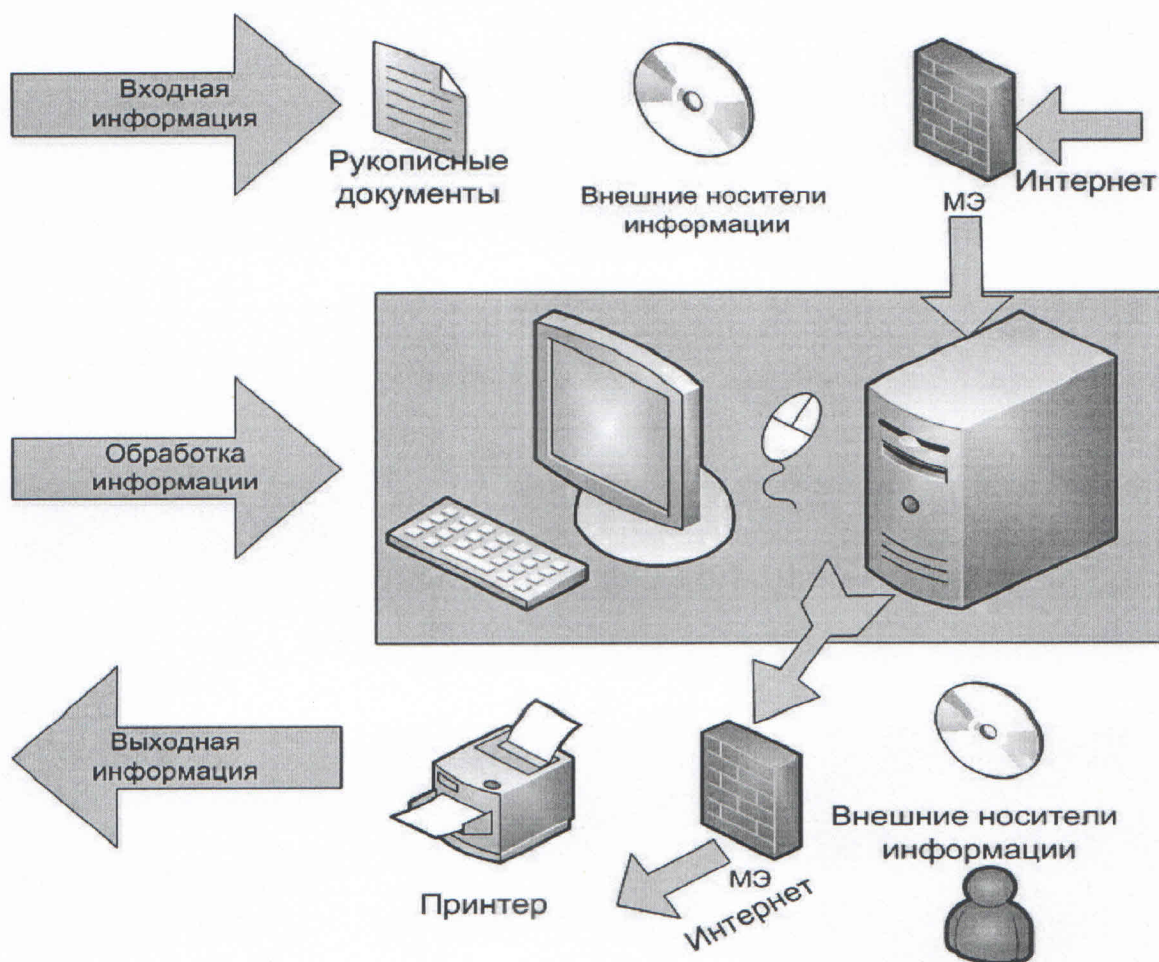
Входная информация может:

- поступать от сторонней организации на бумажных, оптических носителях, по защищенным каналам связи, через Интернет.
- подготавливаться на других аттестованных АС данной организации и передаваться в АС на бумажных или цифровых носителях.

3. Описание выходной информации.

Выходная информация может:

- хранится на НЖМД;
- передаваться на учетных цифровых носителях;
- распечатываться на принтере;
- передаваться по защищенным каналам связи, через Интернет.



4. Перечень используемого программного обеспечения:

1.	Общесистемное программное обеспечение	- Windows 7 Профессиональная, 10 Pro;
2.	Прикладное программное обеспечение	- Веб-сервер Apache
3.	Средства защиты информации	Криптографическая защита: - «КриптоПро CSP» версия 4.0 R4 (исполнение 1-Base) (Сертифицирующий орган ФСБ России № СФ/114-4716 от 15.01.2024 действителен до 15.01.2026) Антивирусная защита: - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган ФСБ России № СФ/СЗИ-0523 от 15.12.2021 действителен до 01.11.2026; Сертифицирующий орган ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029) Контроль съемных машинных носителей информации: - Kaspersky Endpoint Security для Windows (версия 11.6.0.394) (Сертифицирующий орган

	ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2029)
--	--

Работа с программными средствами производится в соответствии с эксплуатационной документацией на данные средства.

5. В технологическом процессе обработки информации задействованы следующие средства вычислительной техники:

АРМ 1:

Имя компьютера	OC-407-ZK-D09.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz
Материнская плата:	Asus H110M-D
ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-08WN4A0 SCSI Disk Device
Видео карта:	Стандартный VGA графический адаптер
Звуковой адаптер:	Realtek High Definition Audio
CD-ROM:	HL-DT-ST DVDROM GH24NSD1 SCSI CdRom Device
Системный блок (инв. или сер. номер)	s/n OP20180024
Монитор (инв. или сер. номер)	BenQ LCD s/n ETG6H03762019
Принтер (инв. или сер. номер)	Epson Stylus Phpto L110 инв. 1101340035
МФУ (инв. или сер. номер)	Canon i-sensys MF6140dn s/n QPX40356
Сетевая плата	Realtek PCIe GBE Family Controller

АРМ 2:

Имя компьютера	OC-111-ZK-D04.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i3-4150 CPU @ 3.50GHz
Материнская плата:	GA-H81-M
ОЗУ:	4,00 ГБ
Жесткий диск:	ST500DM002-1BD142
Видео карта:	Intel(R) HD Graphics 4400
Звуковой адаптер:	High Definition Audio
CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340037
Монитор (инв. или сер. номер)	23,6 BenQ инв. 1101340230
Принтер (инв. или сер. номер)	HP LaserJet P2055d инв. 1101090022
Сетевая плата	Realtek PCIe GBE Family Controller

АРМ 3:

Имя компьютера	OC-101-ZK-D10.admin-smolensk.ru
ЦП:	Intel(R) Core(TM) i3-7100 CPU @ 3.90 GHz
Материнская плата:	Asus H110M
ОЗУ:	8,00 ГБ
Жесткий диск:	WDC WD10EZEX-75WN4A0 SCSI Disk Device
Видео карта:	Стандартный VGA графический адаптер
Звуковой адаптер:	Realtek High Definition Audio

CD-ROM:	-
Системный блок (инв. или сер. номер)	инв. 1101340234
Монитор (инв. или сер. номер)	BenQ GW2470 s/n ETG6H03758019
МФУ (инв. или сер. номер)	HP LaserJet M1212nf MFP инв. 1101340019
Сетевая плата	Realtek PCIe GBE Family Controller

6. Порядок работы.

6.1. Для работы в АС пользователь должен получить у ответственного лица за обеспечение безопасности персональных данных в ИС:

- персональный идентификатор или персональный логин и пароль для начальной идентификации и аутентификации;
- изучить организационно-распорядительную документацию.

6.2. Перед началом каждого сеанса работы пользователь должен удостовериться, что на корпусе АРМ отсутствуют следы вскрытия;

6.3. Подготовка персонального компьютера (далее – ПК) к работе:

включить источник бесперебойного питания, включить системный блок и монитор;

после загрузки операционной системы необходимо ввести логин и пароль для входа. При отсутствии НСД произойдет загрузка операционной системы. При нарушении или сбое системы защиты от НСД и при отказе загрузки операционной системы – прекратить работу и пригласить ответственное лицо за обеспечение безопасности персональных данных в ИС.

6.4. На АС разрешается обрабатывать информацию не конфиденциальную информацию всем пользователям ИС «Сайт».

6.5. Пользователь, используя штатные средства доступа АРМ, выполняет ввод, обработку, вывод информации на учтенные носители (обрабатываемые файлы должны размещаться только в папках пользователей, список папок и права по доступу для каждого пользователя описаны в разрешительной системе доступа).

6.6. Если во время работы на ПК появилась необходимость временно покинуть рабочее место, исполнитель обязан заблокировать ПК, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование ПК производится набором пароля разблокировки, который был создан при настройке системы блокировки.

7. Описание реализованных правил разграничения доступа.

7.1. Обработка информации осуществляется только на предварительно учтенных носителях информации (защищаемых ресурсах – ЖМД), прошедших антивирусный контроль.

7.2. Исполнителю запрещается:

- обрабатывать информацию в присутствии посторонних лиц;
- записывать информацию на неучтенных в специальной части носителях информации, листах бумаги и т. д.;
- использовать в работе пароли, если есть подозрение на их компрометацию;
- разглашать сведения о применяемой системе защиты и содержании информации;
- изменять и тиражировать программное обеспечение.

8. Порядок работы ответственного лица за обеспечение безопасности персональных данных в ИС.

8.1. Ответственное лицо за обеспечение безопасности персональных данных в ИС регистрирует факт выдачи персональных идентификаторов, имена пользователей и пароли в соответствующем журнале учета.

8.2. Ответственное лицо за обеспечение безопасности персональных данных в ИС безопасности проводит контроль защиты от несанкционированного доступа в соответствии с инструкцией безопасности и эксплуатационной документацией на соответствующие элементы системы защиты.

9. Режим технического обслуживания и ремонта.

9.1. При выходе из строя ОТСС АС, обработка персональных данных на данном ОТСС прекращается. Если вышедшее из строя ОТСС является составной частью АРМ (клавиатура, монитор и т.д.), то прекращается обработка информации на АРМ.

О случившемся ставится в известность ответственное лицо за обеспечение безопасности персональных данных в ИС. При необходимости вскрытия корпуса ОТСС составляется Акт о вскрытии по установленной в организации форме. Ремонт и (или) техническое обслуживание производится специалистами в присутствии ответственных лиц.

9.2. В случае передачи технических средств сторонним организациям, ОТСС АС после ремонта проходят дополнительные мероприятия по защите (в этом случае передача носителей информации «НЖМД» запрещена и не производится).

10. Отклонения от штатного режима технологического процесса.

В случае возникновения режима функционирования АС, не предусмотренного представленной технологией, обработка информации прекращается, и ставятся в известность ответственное лицо за обеспечение безопасности персональных данных в ИС для принятия соответствующих мер.

ОТ «04» 08 2025 г. № 141-08

Журнал

[illegible]

ОТ «04» 08 2025 г. № 44-08

учета процедур резервного копирования

[illegible]

ОТ «04» 08 2025 г. № 141-02

**Журнал
проведения инструктажей по информационной безопасности**

[illegible]

