МИНИСТЕРСТВО
АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА
СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

«02» 04 2026 № 055-ОД

О внесении изменений в приказ Министерства архитектуры и строительства Смоленской области от 28.05.2025 № 082-ОД

п р и к а з ы в а ю :

Внести в приказ Министерства архитектуры и строительства Смоленской области от 28.05.2025 № 082-ОД «О реализации мер по защите информации в информационных системах Министерства архитектуры и строительства Смоленской области» следующие изменения:

1. в пункте 2 слова «оставляю за собой» заменить словами «возложить на уполномоченного по обеспечению информационной безопасности в Министерстве архитектуры и строительства Смоленской области»;

2. изложить в новой редакции приложение № 1, приложение № 2, приложение № 5, приложение 7.

Министр **К.Н. Ростовцев**

Приложение № 1
к приказу Министерства
архитектуры и строительства
Смоленской области
от «02»04 2026 г. №055-01

Регламент идентификации и аутентификации в информационных системах Министерства архитектуры и строительства Смоленской области

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления Министерством архитектуры и строительства Смоленской области (далее – Министерство) общих правил, требований и процедур идентификации и аутентификации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом к информационным системам (далее – ИС) Министерства.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

1.3. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИС Министерства.

1.4. Регламент предназначен для сотрудников Министерства:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

2. Термины и определения

2.1. Аутентификационная информация (информация аутентификации) – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной (автоматизированной) системе.

2.2. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной (автоматизированной) системе).

2.3. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной (автоматизированной) системе).

2.4. Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

2.5. Несанкционированный доступ (НСД) – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.6. Объект доступа – единица информационного ресурса информационной (автоматизированной) системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

2.7. Пароль – Идентификатор субъекта доступа, который является его (субъекта) секретом.

2.8. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной (автоматизированной) системе или использующее результаты ее функционирования.

2.9. Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

2.10. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

3. Цели и задачи реализации процессов идентификации и аутентификации

3.1. Целью реализации процессов идентификации и аутентификации в ИС Министерства является распознавание субъекта доступа с необходимой уверенностью в том, что он является именно тем, за кого себя выдает.

3.2. Реализация процессов идентификации и аутентификации достигается решением следующих задач:

– формированием и регистрацией информации о субъекте (объекте) доступа, а также присвоением субъекту (объекту) доступа идентификатора доступа и его регистрацией в перечне присвоенных идентификаторов;

– хранением и поддержанием в актуальном состоянии (обновлением) идентификационной и аутентификационной информации субъекта (объекта) доступа в соответствии с установленными правилами;

– опознаванием субъекта доступа, запросившего доступ к объекту доступа, по предъявленному идентификатору;

– аутентификацией, включающей проверку подлинности субъекта (объекта) доступа и принадлежности ему предъявленных идентификатора и аутентификационной информации.

4. Общие требования

4.1. Процессы идентификации и аутентификации в ИС Министерства подлежат реализации при управлении доступом к следующим частям информационной системы:

– автоматизированные рабочие места;

– серверы;

– прикладное программное обеспечение.

4.2. Идентификация и аутентификация должна осуществляться в отношении:

– пользователей ИС Министерства, являющихся сотрудниками Министерства;

– пользователей ИС Министерства, не являющихся сотрудниками Министерства;

– процессов, запускаемых от имени пользователей;

– процессов, запускаемых от имени системных учетных записей.

4.3. Процессы, запускаемые от имени пользователя, должны однозначно сопоставляться с идентификатором пользователя.

4.4. В качестве идентификатора пользователя при доступе должен использоваться набор буквенно-цифровых символов (логин).

4.5. В ИС Министерства должен использоваться механизм аутентификации на основе пароля.

5. Требования к созданию, присвоению и уничтожению идентификаторов

5.1. Создание, присвоение и уничтожение идентификатора должно осуществляться сотрудниками Министерства, назначенными ответственными за обеспечение безопасности персональных данных (далее – Ответственный).

5.2. Ответственный обеспечивает однозначную идентификацию пользователя и (или) устройства путем формирования уникального персонального идентификатора.

5.3. Повторное использование идентификатора пользователя не допускается в течение одного года со дня уничтожения.

5.4. Блокирование идентификатора пользователя должно осуществляться после 30 дней неиспользования.

5.5. Уничтожение идентификатора пользователя, являющегося сотрудником Министерства, производится при прекращении полномочий (увольнении) сотрудника.

5.6. Уничтожение идентификатора пользователя, не являющегося сотрудником Министерства, производится в случаях, установленных требованиями по подключению внешних пользователей.

6. Управление средствами аутентификации

6.1. Генерация (назначение) паролей

6.1.1. Генерация и выдача начальной аутентификационной информации (пароля) пользователю осуществляется Ответственным.

6.1.2. Средства, реализующие идентификацию и аутентификацию пользователей, должны обеспечивать настройку характеристик паролей, представленных в таблице 2.

Таблица 2 – Требования к настройкам характеристик паролей

№ п/п	Характеристика	Значение	Примечание
1.	Соответствие требованиям к сложности пароля	Включено	Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков. Содержать знаки минимум трех из четырех перечисленных ниже категорий: - латинские заглавные буквы (от A до Z); - латинские строчные буквы (от a до z); - цифры (от 0 до 9)

№ п/п	Характеристика	Значение	Примечание
			- специальные символы (например, !, $, #, %).

6.2. Хранение паролей

6.2.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать защиту аутентификационной информации от несанкционированного доступа к ней и ее модификации.

6.3. Порядок смены аутентификационной информации

6.3.1. Смена паролей производится на плановой и внеплановой основе.

6.3.2. Плановая смена паролей осуществляется:

– при истечении максимального срока действия пароля;

– при поставках нового оборудования с предустановленной аутентификационной информацией (средств аутентификации), при внедрении системы защиты информации информационной системы;

– после внедрения системы защиты информации информационной системы.

6.3.3. Внеплановая смена паролей осуществляется в следующих случаях:

– компрометация или подозрение в компрометации пароля;

– прекращение полномочий (увольнение, изменение обязанностей и другие обстоятельства) сотрудников Министерства;

– по указанию сотрудника Министерства, назначенного ответственным за обеспечение безопасности персональных данных.

7. Защита обратной связи при вводе аутентификационной информации

7.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля должны отображаться условными знаками: «*», «●» или иными знаками.

8. Действия при компрометации аутентификационной информации

8.1. Компрометация действующих паролей является внештатной ситуацией.

8.2. Обо всех фактах компрометации паролей следует немедленно уведомить ответственного за обеспечение безопасности персональных данных.

8.3. Скомпрометированные пароли и связанные с ними персональные идентификаторы (логины) пользователей должны блокироваться при обнаружении факта компрометации.

9. Ответственность

9.1. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 2
к приказу Министерства
архитектуры и строительства
Смоленской области
от «02» 04 2026 г. № 055-ОД

Регламент управления доступом в информационных системах Министерства архитектуры и строительства Смоленской области

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления Министерством архитектуры и строительства Смоленской области (далее – Министерство) общих правил, требований и процедур управления доступом в информационных системах (далее – ИС) Министерства.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов

Условное обозначение и номер меры	Меры защиты информации
	доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

1.3. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИС Министерства.

1.4. Правила и процедуры управления информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами описаны в рамках Регламента защиты информационной системы, ее средств, систем связи и передачи данных.

1.5. Регламент предназначен для сотрудников Министерства:

1.5.1. Назначенных ответственными за обеспечение безопасности персональных данных.

2. Термины и определения

2.1. Аутентификационная информация (информация аутентификации) – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной (автоматизированной) системе.

2.2. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной (автоматизированной) системе).

2.3. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной (автоматизированной) системе).

2.4. Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

2.5. Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.6. Объект доступа – единица информационного ресурса информационной (автоматизированной) системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

2.7. Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

2.8. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной (автоматизированной) системе или использующее результаты ее функционирования.

2.9. Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

2.10. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной (автоматизированной) системе в соответствии с установленными правилами разграничения доступа.

3. Требование к системе управления доступом

3.1. Управление доступом должно быть направлено на недопущение несанкционированного доступа к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен.

3.2. Доступ пользователей к информационным ресурсам ИС Министерства предоставляется сотрудниками Министерства, назначенными ответственными за обеспечение безопасности персональных данных, исходя из следующих условий:

– доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своей должностной инструкцией;

– доступ необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) руководителя соответствующего подразделения;

– доступ необходим для выполнения пользователем обязанностей другого пользователя по письменному указанию Министра архитектуры и строительства Смоленской области Министерства;

– доступ необходим для выполнения пользователем работ по письменному указанию Министра архитектуры и строительства Смоленской области Министерства;

– доступ необходим для выполнения пользователем работ в ходе реализации контрактов, договоров, заключенных с Министерством (для сотрудников «сторонних» организаций).

3.3. Физический доступ пользователей к техническим средствам ИС Министерства осуществляется в соответствии с установленным в Министерстве порядком доступа сотрудников Министерства в помещения, в которых осуществляется обработка персональных данных.

3.4. Пользователи допускаются к информационному ресурсу на основании заявок, в соответствии с установленным порядком, представленным в пункте 7.

3.5. Допуск к информационному ресурсу предоставляется исключительно после ознакомления с локальными актами Министерства и прохождения обучения (инструктажа) по вопросам обеспечения информационной безопасности.

3.6. Доступ пользователей к программным функциям технических средств ИС Министерства должен осуществляться в соответствии с правилами разграничения доступа и с использованием учетных записей при успешном прохождении процедуры идентификации и аутентификации.

3.7. Средства, реализующие управление доступом, должны обеспечивать:

3.7.1. Ограничение неуспешных попыток входа (доступа) в количестве 5 раз за период времени в 1 час, а также обеспечивать блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем установленного ограничения.

4. Методы управления доступом

4.1. В ИС Министерства должен быть реализован ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

4.2. Список ролей определяется в отношении каждой ИС Министерства ответственными за обеспечение безопасности персональных данных с учетом особенностей функционирования ИС и должностных обязанностей (функций) сотрудников Министерства при эксплуатации ИС и ее системы защиты информации.

4.3. При этом, в обязательном порядке должны быть выделены роли, осуществляющие функции по:

– управлению функциями безопасности и средствами защиты информации.

– управлению (администрированию) базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями и серверами;

– обработке персональных данных;

– обслуживанию помещений, в которых размещаются технические средства информационной системы – уборка, обслуживание и ремонт инженерных систем и т.п.;

– обслуживанию, ремонту, настройке и контролю работы обеспечивающих функционирование информационной системы – технических средств и систем.

4.4. Каждой роли должны быть определены минимально необходимые права и привилегии, необходимые для обеспечения функционирования информационной системы.

4.5. Каждому сотруднику при предоставлении доступа в информационную систему должна быть определена одна из определенных ролей.

4.6. Сведения о ролях и их полномочиях детализируется в рамках приказа о системе разграничения доступа.

4.7. Полномочия пользователей могут уточняться сотрудником Министерства, назначенным ответственным за обеспечение безопасности персональных данных, исходя из должностных обязанностей (функций), возложенных на пользователя.

5. Идентификация объектов доступа

5.1. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, исходя из должностных обязанностей (функций), возложенных на пользователей, должны идентифицировать (определить) объекты доступа, в отношении которых реализуется управление доступом.

5.2. В качестве объектов доступа следует рассматривать:

5.2.1. Из числа технических средств:

– автоматизированные рабочие места пользователей;

– серверное оборудование;

– оборудование, обеспечивающее функционирование информационной системы (сервер синхронизации времени, оборудование локальной вычислительной сети, источники бесперебойного питания и т.п.).

5.2.2. Из числа объектов файловой системы:

– файлы и каталоги системного программного обеспечения;

– пользовательский каталог;

– запускаемые и исполняемые модули прикладного программного обеспечения;

– конфигурационные файлы прикладного программного обеспечения;

– запускаемые и исполняемые модули программного обеспечения средств защиты информации;

– конфигурационные файлы программного обеспечения средств защиты информации;

– файлы журналов регистрации событий безопасности;

– контейнеры (файлы), в которых хранится аутентификационная информация (или ее образы) пользователей.

5.3. Подробный состав объектов доступа в отношении каждой ИС Министерства детализируется в рамках приказа о системе разграничения доступа.

6. Типы доступа

6.1. В рамках управления доступа должны рассматриваться следующие типы доступа:

– физический доступ к техническим средствам;

– доступ к объектам файловой системы.

6.2. В качестве разрешенных к выполнению пользователю или запускаемому от его имени процессу при доступе к объектам файловой системы должны рассматриваться следующие операции:

– чтение (r);
– запись (w);
– удаление (d);
– выполнение (e).

7. Порядок предоставления доступа

7.1. Формирование запроса

7.1.1. Предоставление доступа к ИС Министерства осуществляется на основании заявок. Формирование заявки осуществляет либо сам сотрудник, которому необходимо предоставить доступ, либо руководитель сотрудника. Работа с заявками осуществляется в соответствии с установленным Министерством порядком. При этом, в заявке в обязательном порядке должен быть указан информационный ресурс, к которому необходим доступ, уровень доступа к нему, период, на который требуется предоставление доступа, и обоснование необходимости предоставления доступа.

7.1.2. Все заявки на предоставление доступа должны храниться сотрудниками Министерства, назначенными ответственными за обеспечение безопасности персональных данных, и могут впоследствии использоваться для:

– контроля правомерности предоставления доступа при разборе инцидентов информационной безопасности и конфликтных ситуаций;
– проверки корректности предоставления доступа к информационным ресурсам.

7.2. Согласование предоставления доступа

7.2.1. Все сформированные заявки на доступ подлежат согласованию.

7.2.2. Согласование производится с:

– руководителем подразделения (если заявка сформирована сотрудником подразделения);
– сотрудником Министерства, назначенным ответственным за обеспечение безопасности персональных данных;
– лицами, согласование доступа с которыми предусмотрено в рамках внутренних локальных нормативных актов Министерства.

7.2.3. Сотрудник Министерства, назначенный ответственным за обеспечение безопасности персональных данных, в процессе согласования должен выполнить:

– верификацию пользователя – проверку личности пользователя, его должностных (функциональных) обязанностей;
– оценку обоснованности доступа к информационному ресурсу и

запрашиваемого уровня доступа.

7.3. Ознакомление с документацией

7.3.1. Перед предоставлением доступа в обязательном порядке следует лиц, которым предоставляется доступ, ознакомить с локальными нормативными актами в области обеспечения безопасности персональных данных.

7.3.2. Ознакомление должно производиться ответственным за обеспечение безопасности персональных данных. Факты ознакомления должны фиксироваться в листах ознакомления и/или соответствующих журналах.

7.4. Предоставление доступа

7.4.1. Процесс предоставления доступа включает:

– создание сотрудником Министерства, назначенным ответственным за обеспечение безопасности персональных данных, учетной записи пользователя. Формирование реквизитов учетной записи (идентификатора и начальной аутентификационной информации (пароля)) осуществляется в соответствии с Регламентом идентификации и аутентификации;

– настройка средств защиты информации сотрудником Министерства, назначенным ответственным за обеспечение безопасности персональных данных;

– настройка программного обеспечения автоматизированного рабочего места и/или сервера сотрудником Министерства, назначенным ответственным за обеспечение безопасности персональных данных;

7.4.2. Предоставление доступа пользователю должно осуществляться в течение 2-х рабочих дней со дня согласования заявки.

7.5. Дополнительные сведения

7.5.1. Доступ пользователям к информационным ресурсам может быть предоставлен без оформления заявки в случае письменного указания руководства Министерства.

7.5.2. Доступ сотрудниками федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, иных государственных органов, органов прокуратуры и других правоохранительных органов, осуществляющих контрольные мероприятия и обладающих соответствующими полномочиями, осуществляется в соответствии с порядком, установленным законодательством Российской Федерации.

8. Порядок прекращения доступа

8.1. Доступ к ИС Министерства должен быть незамедлительно прекращен:

– при истечении срока предоставления доступа;

– при прекращении полномочий пользователя;

– по указанию руководства Министерства;

– по указанию сотрудника, назначенного ответственным за обеспечение

безопасности персональных данных;

– в случаях обнаружения факта компрометации учетной записи пользователя.

9. Защита удаленного доступа

9.1. Процесс предоставления защищенного удаленного доступа включает:

– установление видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы в соответствии с установленными методами, типами и правилами разграничения доступа;

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа.

– предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации.

10. Управление информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

10.1. В информационных системах должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

– фильтрацию информационных потоков в соответствии с правилами управления потоками;

– разрешение передачи информации в информационной системе только по маршруту, установленному оператором;

– изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;

– запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.

Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между

пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

11. Управление взаимодействием с внешними информационными системами

11.1. Процесс обеспечения управления взаимодействием с внешними информационными системами включает:

– предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с установленными методами, типами и правилами разграничения доступа

– определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

– определение системных учетных записей, используемых в рамках данного взаимодействия;

– определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;

– определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

12. Ответственность

12.1. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 5
к приказу Министерства
архитектуры и строительства
Смоленской области
от «02»04 2026 г. №055-01

Регламент контроля (анализа) защищенности в информационных системах Министерства архитектуры и строительства Смоленской области

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления Министерством архитектуры и строительства Смоленской области (далее – Министерство) общих правил, требований и процедур контроля (анализа) защищенности в информационных системах (далее – ИС) Министерства.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

1.3. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИС Министерства.

1.4. Регламент предназначен для сотрудников Министерства:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

2. Контроль установки обновлений программного обеспечения

2.1. Мероприятия по контролю установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. В ходе проведения данного мероприятия должно осуществляться:

2.1.1. Проверка использования последних версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения,

включая программное обеспечение средств защиты информации (проверка соответствия версий – используемой и представленной на официальном сайте (портале) производителя (разработчика));

2.1.2. Проверка наличия отметок об установке (применении) обновлений в эксплуатационной документации (техническом паспорте).

2.1.3. Документирование результатов контроля.

2.1.4. При обнаружении фактов пропуска обновлений – уведомление сотрудника Министерства, выполняющего функции по управлению (администрированию) системой защиты информации.

3. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

3.1. Мероприятия по контролю правил генерации и смены паролей, заведения и удаления учетных записей пользователя, реализации правил разграничения доступом, полномочий пользователя в информационной системе должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите информации. В ходе проведения данного мероприятия должно осуществляться:

3.1.1. Проверка соблюдения правил генерации и смены паролей пользователями.

3.1.2. Проверка соблюдения правил заведения и удаления учетных записей пользователей, предусмотренных регламентом управления доступом.

3.1.3. Проверка реализации правил разграничения доступом в соответствии с регламентом управления доступом и организационно-распорядительным документом об утверждении системы разграничения доступом в информационной системе.

3.1.4. Принятие мер, направленных на устранение выявленных недостатков.

4. Ответственность

4.1. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

Приложение № 7
к приказу Министерства архитектуры и строительства Смоленской области
от «02» 04 2026г. № 055-04

Регламент защиты информационных систем Министерства архитектуры и строительства Смоленской области, их средств, систем связи и передачи данных

1. Общие положения

1.1. Настоящий Регламент разработан с целью установления Министерством архитектуры и строительства Смоленской области (далее – Министерство) общих правил, требований и процедур защиты информационных систем (далее – ИС) Министерства, ее средств, систем связи и передачи данных.

1.2. Меры защиты информации, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты информации, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты информации
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

1.3. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИС Министерства.

1.4. Регламент предназначен для сотрудников Министерства:

1.4.1. Назначенных ответственными за обеспечение безопасности персональных данных.

2. Защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны

2.1. При передаче информации по каналам связи, выходящим за пределы контролируемой зоны, должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации).

2.2. Защита информации при ее передаче по каналам связи должна обеспечиваться одним или комбинацией из следующих способов:

– защита каналов связи от несанкционированного физического доступа (подключения) к ним;

– применение средств криптографической защиты информации.

2.3. Для защиты информации криптографическими методами должны использоваться программные или программно-аппаратные средства, прошедшие оценку соответствия в форме обязательной сертификации.

3. Управление сетевыми потоками

3.1. В информационной системе должно осуществляться управление сетевыми потоками при передаче информации между устройствами, сегментами, включающее:

– фильтрацию сетевых потоков в соответствии с правилами управления потоками;

– разрешение передачи информации только по разрешенному маршруту;

– изменение (перенаправление) маршрута передачи информации (в установленных Министерством случаях);

– запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи (в установленных Министерством случаях).

3.2. Управление сетевыми потоками должно обеспечивать разрешенный маршрут прохождения информации между устройствами, сегментами информационной системы, а также между информационными системам или при взаимодействии с информационно-телекоммуникационными сетями провайдеров, предоставляющих услуги связи или сетями связи общего пользования на основе правил управления сетевыми потоками.

4. Ответственность

4.1. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, несут персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.