МИНИСТЕРСТВО АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

«28» 05 2025 №082-ОД

О реализации мер по защите информации в информационных системах Министерства архитектуры и строительства Смоленской области

В целях обеспечения безопасности персональных данных при их обработке в информационных системах Министерства архитектуры и строительства Смоленской области, и выполнения требований приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

п р и к а з ы в а ю :

1. Утвердить нижеследующие внутренние документы Министерства архитектуры и строительства Смоленской области:

– Регламент идентификации и аутентификации в информационных системах Министерства архитектуры и строительства Смоленской области (Приложение № 1);

– Регламент управления доступом в информационных системах Министерства архитектуры и строительства Смоленской области (Приложение № 2);

– Регламент регистрации событий безопасности в информационных системах Министерства архитектуры и строительства Смоленской области (Приложение № 3);

– Регламент антивирусной защиты информационных систем Министерства архитектуры и строительства Смоленской области (Приложение № 4);

– Регламент контроля (анализа) защищенности информации в информационных системах Министерства архитектуры и строительства Смоленской области (Приложение № 5);

– Регламент защиты технических средств в информационных системах Министерства архитектуры и строительства Смоленской области (Приложение № 6);

– Регламент защиты информационных систем Министерства архитектуры и строительства Смоленской области, их средств, систем связи и передачи данных (Приложение № 7).

2. Контроль за исполнением настоящего приказа оставляю за собой.

Министр **К.Н. Ростовцев**

Приложение № 1
к приказу Министерства
архитектуры и строительства
Смоленской области
от «28» 05 2025 г. № 082-ОД

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. Цель 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;

– устройств (технических средств), участвующих в информационном взаимодействии.

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. Идентификация устройств должна обеспечиваться одним или комбинацией следующих способов:

– по логическому имени (имя устройства и (или) ID);

– по логическому адресу (например, IP-адресу);

– по физическому адресу (например, MAC-адресам) устройства.

5.6. Уничтожение идентификатора пользователя производится при прекращении полномочий (увольнении) сотрудника.

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

№ п/п	Характеристика	Значение	Примечание
			категорий: - латинские заглавные буквы (от A до Z); - латинские строчные буквы (от a до z); - цифры (от 0 до 9) - 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.

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.

6.4. Защита обратной связи при вводе пароля

6.4.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать исключение отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля должны отображаться условными знаками: «*», «●»или иными знаками.

7. Действия при компрометации аутентификационной информации

7.1. Компрометация действующих паролей является внештатной ситуацией.

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

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

8. Ответственность

8.1. 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 «28» 05 2025 г. № 082-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 доступа к объектам доступа через внешние информационно-

Условное обозначение и номер меры	Меры защиты информации
	телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
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. Требования 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

7.2. 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.

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

7.4. контроля правомерности предоставления доступа при разборе инцидентов информационной безопасности и конфликтных ситуаций;

7.5. проверки корректности предоставления доступа к информационным ресурсам.

7.6. Согласование предоставления доступа

7.7. Все сформированные заявки на доступ подлежат согласованию.

7.8. Согласование производится с:

7.9. руководителем подразделения (если заявка сформирована сотрудником подразделения);

7.10. сотрудником Министерства, назначенным ответственным за обеспечение безопасности персональных данных;

7.11. лицами, согласование доступа с которыми предусмотрено в рамках внутренних локальных нормативных актов Министерства.

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

7.13. верификацию пользователя – проверку личности пользователя, его должностных (функциональных) обязанностей;

7.14. оценку обоснованности доступа к информационному ресурсу и запрашиваемого уровня доступа.

7.15. Ознакомление с документацией

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

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

7.18. Предоставление доступа

7.19. Процесс предоставления доступа включает:

7.20. 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;

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

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

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

7.24. Дополнительные сведения

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

7.26. 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. Ответственность

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

Приложение № 3
к приказу Министерства
архитектуры и строительства
Смоленской области
от «28» 05 2025 г. № 082-ОД

Регламент регистрации событий безопасности 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 регистрации событий безопасности 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
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности

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. Регистрация и мониторинг событий безопасности

2.1. Общие положения

2.1.1. Сбор, запись и хранение информации о событиях безопасности осуществляется с целью выявления инцидентов информационной безопасности и реагирования на них.

2.1.2. Сбор, запись и хранение событий безопасности должны осуществляться на всех компонентах ИС (рабочие места пользователей, серверы, телекоммуникационное оборудование). Требования к составу и содержанию информации о событиях безопасности представлены в пункте 2.2.

2.1.3. Доступ к функциям управления механизмами регистрации (аудита) должен быть доступен только сотрудникам Министерства, назначенным ответственными за обеспечение безопасности персональных данных.

2.1.4. Доступ к записям аудита должен быть доступен только сотрудникам Министерства:

– Назначенным ответственными за обеспечение безопасности персональных данных.

2.1.5. Защита информации о событиях безопасности (записях регистрации (аудита)) должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования. В том числе должна обеспечиваться защита средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

2.1.6. Зарегистрированные события безопасности должны храниться не менее чем 1 год.

2.2. Требования к составу регистрируемых событий безопасности

2.2.1. Регистрации подлежат события, представленные в таблице 2.

Таблица 2 – Состав и содержание информации о событиях безопасности

№ п/п	Событие	Минимальный состав информации о событии
1.	Вход (выход), а также попытки входа субъектов доступа (пользователей) в операционную систему	Дата и время входа (выхода) в операционную систему (из операционной системы); Результат попытки входа (успешный или неуспешный); Идентификатор (логин), предъявленный при попытке доступа
2.	Изменение полномочий субъектов доступа и статуса объектов доступа, в том числе создание, модификация, удаление учетных записей	Дата и время создания или модификации или удаления учетной записи или статуса объекта доступа; Результат операции (успешный или неуспешный); Идентификатор (логин) субъекта доступа (пользователя), выполнившего операцию (создание или

№ п/п	Событие	Минимальный состав информации о событии
		модификация или удаление учетной записи / изменении статуса объекта доступа)
3.	Подключение съемных машинных носителей информации и вывод информации на носители информации	Дата и время подключения съемного машинного носителя информации и вывода информации на носители информации; Логическое имя (имя устройства и (или) ID) съемного машинного носителя информации; Идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
4.	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска; Имя (идентификатор) программы (процесса, задания); Идентификатор субъекта доступа (пользователя, устройства), запросившего программу (процесс, задание); Результат запуска (успешный, неуспешный)
5.	Попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам	Дата и время попытки доступа к защищаемому файлу; Результат попытки доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Спецификация защищаемого файла (логическое имя, тип)
6.	Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей)	Дата и время попытки доступа к защищаемому объекту; Результата попытки доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Спецификацию защищаемого объекта доступа (логическое имя (номер))
7.	Попытка удаленного доступа	Дата и время попытки удаленного доступа; Результат попытки удаленного доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Используемый протокол доступа; Используемый интерфейс доступа

3. Ответственность

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

Приложение № 4
к приказу Министерства
архитектуры и строительства
Смоленской области
от «28» 05 2025 г. №082-ОД

Регламент антивирусной защиты 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) порядка организации защиты от угроз, связанных с внедрением вредоносных компьютерных программ (вирусов) из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования), и съемных машинных носителей информации 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**
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

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

1.4. Регламент предназначен для сотрудников Министерства:

1.5. Назначенных ответственными за обеспечение безопасности персональных данных.

2. Термины и определения

2.1. Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

2.2. Безопасность информации – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

2.3. Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

2.4. Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

2.5. Сигнатура – характерные признаки компьютерной вредоносной программы (вируса), используемые для ее обнаружения.

2.6. Угроза безопасности информации – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.

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

3. Требования к антивирусной защите

3.1. Для реализации антивирусной защиты на всех компонентах ИС Министерства должны применяться средства антивирусной защиты.

3.2. Антивирусная защита должна быть реализована:

3.3. на автоматизированных рабочих местах пользователей (в том числе привилегированных пользователей);

3.4. на серверах.

3.5. Установка (инсталляция), настройка (конфигурирование), обновление модулей средств антивирусной защиты, удаление должны осуществляться только сотрудниками Министерства, назначенными ответственными за обеспечение безопасности персональных данных.

3.6. Управление параметрами настройки функций безопасности средств антивирусной защиты должно быть доступно только сотрудникам Министерства, назначенным ответственными за обеспечение безопасности персональных данных.

3.7. Средства антивирусной защиты должны постоянно находиться в активном состоянии и обеспечивать антивирусную защиту в режиме реального времени.

3.8. Автоматическое обновление модулей средств антивирусной защиты должно быть запрещено.

3.9. Обновление модулей средств антивирусной защиты должно производиться сотрудниками Министерства, назначенными ответственными за обеспечение безопасности персональных данных, в «ручном» режиме.

4. Требования к параметрам настроек средств антивирусной защиты

4.1. Периодичность поиска вредоносных компьютерных программ (вирусов) средствами антивирусной защиты должно обеспечиваться в соответствии с таблицей 2.

Таблица 2 – Периодичность поиска вирусов

№ п/п	Объект проверки	Частота проверки
1.	Системная память	Не реже одного раза в сутки
2.	Объекты (файлы), загружаемые при старте операционной системы	Не реже одного раза в сутки
3.	Объекты (файлы), поступающие по каналам передачи данных	Каждый раз перед открытием (запуском) объекта (файла)
4.	Файлы инсталляции программного обеспечения	Каждый раз перед установкой (инсталляцией)
5.	Файлы обновлений программного обеспечения	Каждый раз перед обновлением программного обеспечения
6.	Машинные носители информации, встроенные в портативные или стационарные технические средства	Не реже одного раза в неделю
7.	Съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители)	Каждый раз при подключении

4.2. Антивирусная проверка должна осуществляться современными методами обнаружения вредоносных компьютерных программ (вирусов), в том числе включать:

– сигнатурный метод. Метод, основанный на поиске в объектах (файлах) сигнатур известных компьютерных вирусов;

– метод обнаружения изменений. Метод, основанный на предварительном запоминании характеристик всех областей диска, которые могут подвергаться нападению компьютерными вирусами, и их периодической проверке на изменения;

– методы резидентных сторожей. Метод, основанный на отслеживании всех подозрительных действий, выполняемых другими программами;

– методы эвристического анализа (эвристического сканирования).

4.3. Средства антивирусной защиты при обнаружении вредоносной компьютерной программы (вируса) должны выполнять следующие действия:

– зафиксировать в журнале регистрации событий факт обнаружения вредоносной компьютерной программы (вируса);

– удалить зараженный объект (файла) либо переместить его в карантин;

– уведомить в масштабе времени, близком к реальному, об обнаружении вредоносной компьютерной программы (вируса).

4.4. Средства антивирусной защиты должны обеспечивать регистрацию событий, связанных с функционированием, включая:

4.5. проведение проверок объектов на наличие вредоносных компьютерных программ (вирусов);

4.6. отказ работоспособности средства антивирусной защиты и его компонентов;

4.7. обнаружение вредоносной компьютерной программы (вируса);

4.8. изменение конфигурации средства антивирусной защиты;

4.9. обновление модулей средства антивирусной защиты и базы данных признаков вредоносных компьютерных программ (вирусов).

4.10. Журналы регистрации событий средств антивирусной защиты должны храниться не менее 1 год и должны быть доступны для оперативного анализа в течение 1 месяца после регистрации событий.

5. Требования к обновлению базы данных признаков вредоносных компьютерных программ (вирусов)

5.1. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, должны обеспечить обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты по факту их выпуска производителем средства антивирусной защиты.

5.2. Базы данных признаков вредоносных компьютерных программ (вирусов) должны быть получены из доверенных источников. В качестве доверенных источников следует рассматривать официальные сайты производителей используемых средств защиты информации.

5.3. Сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, должны периодически проводить мероприятие по контролю обновления баз данных признаков вредоносных компьютерных программ (вирусов). Мероприятие должно быть включено в ежегодный план мероприятий по защите информации.

6. Действия при обнаружении вредоносных компьютерных программ (вирусов)

6.1. При обнаружении вредоносных компьютерных программ (вирусов) сотрудники Министерства, назначенные ответственными за обеспечение безопасности персональных данных, должны сообщить об этом сотруднику Министерства, выполняющему функции по выявлению инцидентов информационной безопасности и реагированию на них. Данные лица совместно принимают меры по предотвращению наступления негативных последствий заражения. Меры могут включать:

– остановку эксплуатации зараженного компонента информационной системы и (или) изоляцию его от остальных компонентов;

– удаление вредоносной программы;

– установление причин и источника заражения;

– инициацию и проведение служебной проверки по факту заражения вредоносной компьютерной программой (вирусом).

– принятие мер по минимизации возможности подобных заражений в дальнейшем;

– проведение полной антивирусной проверки всех компонентов информационной системы.

6.2. Возобновление работы с компонентом информационной системы, подвергшимся заражению, осуществляется только после окончания работ по удалению вредоносных программ и проведения антивирусной проверки прочих объектов (файлов).

7. Ответственность

7.1. 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 «28» 05 2025 г. №082-ОД

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**
АНЗ.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:

1.5. 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. Ответственность

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

Приложение № 6
к приказу Министерства
архитектуры и строительства
Смоленской области
от «28» 05 2025 г. №087-ОД

Регламент защиты технических средств 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 защиты технических средств информационных систем (далее – ИС) Министерства и персональных 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**
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

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. Управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены

2.1. Управление физическим доступом предусматривает:

– определение перечня помещений, в которых размещены информационные системы Министерства. Перечень утверждается Министром архитектуры и строительства Смоленской области Министерства;

– определение порядка доступа сотрудников Министерства в помещения, в которых осуществляется обработка защищаемой информации и размещены информационные системы. Порядок утверждается Министром архитектуры и строительства Смоленской области Министерства;

– санкционирование физического доступа;

– учет доступа.

2.2. Управление физическим доступом может достигаться за счет:

– оснащения входных дверей помещений, в которых расположены технические средства и устройства информационной системы, замками;

– постоянным закрытием входных дверей помещений, в которых расположены технические средства и устройства информационной системы, на замок и их открытием только для санкционированного прохода;

– внедрением контрольно-пропускного и внутриобъектового режима (доступ посетителей на территорию Министерства осуществляется только при наличии пропуска и документа, удостоверяющего личность);

– организацией доступа к информационным ресурсам по заявке, согласованной в соответствии с пропускным внутриобъектовым режимом;

– предоставления доступа в помещения, в которых размещены серверные компоненты информационной системы и обеспечивающие их функционирование устройства, строго определенному кругу лиц, осуществляющему их техническое обслуживание и сопровождение;

– ограничения нахождения посетителей и других лиц имеющих право разового доступа на территории Министерства. Нахождение таких лиц допускается только в присутствии лиц, имеющих право постоянного доступа на территорию Министерства;

– ознакомления лиц, имеющих право постоянного доступа в помещения, в которых размещены информационные системы Министерства, с локальными нормативными актами Министерства в области обеспечения безопасности информации;

– предоставление доступа в помещения, в которых размещены информационные системы, только тем лицам, которым указанный доступ необходим в рамках исполнения должностных обязанностей или обязанностей,

предусмотренных договорами (соглашениями);

– фиксированием факта разового доступа лиц в помещения, в которых размещены информационные системы.

3. Размещение устройств вывода (отображения) информации

3.1. В качестве устройств вывода (отображения) информации рассматриваются:

– мониторы автоматизированных рабочих мест пользователей;

– мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств);

– печатающие устройства.

3.2. При размещении данных устройств вывода (отображения) информации следует исключать возможность несанкционированного просмотра выводимой на них информации как из-за пределов помещения, в которых размещено устройство, так и в пределах этих помещений. С этой целью не следует размещать устройства вывода (отображения, печати) информации напротив:

– оконных проемов;

– входных дверей;

– технологических отверстий;

– в коридорах, холлах;

– в иных местах, доступных для несанкционированного просмотра.

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 «28» 05 2025 г. №082-ОД

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

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.