МИНИСТЕРСТВО АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

«01» 07 2025 № 116-ОД

Об утверждении Регламента обновления программного обеспечения в Министерстве архитектуры и строительства Смоленской области

В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», с приказом ФСТЭК России 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 прилагаемый Регламент обновления программного обеспечения в Министерстве архитектуры и строительства Смоленской области.

2. Контроль за исполнением настоящего приказа возложить на заместителя министра Кардаш Елену Владимировну.

Министр К.Н. Ростовцев

УТВЕРЖДАЮ
Министр архитектуры и
строительства Смоленской области
_____К.Н. Ростовцев
«01» 07 2025 г.

Регламент обновления программного обеспечения в Министерстве архитектуры и строительства Смоленской области

1. Общие положения

1.1. Настоящий Регламент обновления программного обеспечения в Министерстве архитектуры и строительства Смоленской области (далее – Регламент) разработан с учетом:

1.1.1. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.1.2. Приказ ФСТЭК России 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».

1.1.3. Методический документ ФСТЭК России от 28 октября 2022 г. «Методика тестирования обновлений безопасности программных, программно-аппаратных средств».

1.2. Целью разработки данного Регламента является установление Министерством архитектуры и строительства Смоленской области (далее – Министерство) общих правил, требований и процедур обновления программного обеспечения (в том числе программного обеспечения с открытым исходным кодом), применяемого в объектах информатизации Министерства.

1.3. Настоящий Регламент подлежит применению в отношении всех объектов информатизации[1] Министерства.

1.4. Настоящий Регламент предназначен для сотрудников, на которых возложены обязанности по обновлению программного обеспечения в Министерстве.

1.5. Изменения в настоящий Регламент вносятся при принятии Министерством решения об улучшении процесса обновления программного обеспечения.

---

[1] Объект информатизации – информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть или иной объект информатизации организации.

1.6. В регламенте используются термины и определения, установленные национальными стандартами в области защиты информации и обеспечения информационной безопасности.

2. Цель и задачи обновления программного обеспечения

2.1. Целью обновления программного обеспечения является поддержание должного уровня информационной безопасности Министерства.

2.2. Обновление программного обеспечения объектов информатизации Министерства направлено на решение следующих задач:

– обеспечение штатного режима функционирования объектов информатизации Министерства за счет своевременного устранения ошибок в используемом в их составе программном обеспечении;

– устранение уязвимостей, выявленных в рамках процесса управления уязвимостями.

3. Описание процесса обновления программного обеспечения

3.1. Процесс обновления программного обеспечения включает 3 (три) основных этапа:

– подготовка к проведению обновления;

– тестирование обновления;

– установка обновления.

3.2. Обновления сертифицированных программных и программно-аппаратных средств защиты информации, направленные на устранение уязвимостей, осуществляются в приоритетном порядке. Такие обновления выполняются в соответствии с эксплуатационной документацией на такие средства, рекомендациями разработчика и с учетом положений настоящего Регламента.

3.3. Этап 1. Подготовка к проведению обновления

3.3.1. Подготовка к проведению обновления предусматривает получение обновления и подготовку среды для последующего размещения файлов обновления и тестирования обновления.

3.3.2. В Министерстве допускается использование следующих сред для тестирования обновлений:

– исследовательский стенд, специально созданный для тестирования обновлений безопасности или иных целей;

– тестовая зона объекта информатизации («песочница»);

– объект информатизации, функционирующий в штатном режиме.

3.3.3. Выбор среды тестирования обновлений осуществляет исследователь[2], исходя из технических возможностей Министерства и угроз нарушения

---

[2] Исследователь – сотрудники организации, на которых возложены обязанности по обновлению программного обеспечения

функционирования объекта информатизации.

3.3.4. Получение обновлений программных и программно-аппаратных средств допускается только из доверенных источников. В качестве доверенного источника информации об обновлениях в Министерстве рассматриваются:

– официальные сайты (порталы) производителей (разработчиков) программных, программно-аппаратных средств;

– дистрибутивы на съемных машинных носителях (CD-R/RW, DVD-R/RW, USB flash-накопители и т.п.), полученные от производителя программного, программно-аппаратного средства или его официальных партнеров-поставщиков.

3.3.5. Полученное обновления (файлы обновления) подлежат размещению в среде тестирования, определенном исследователем.

3.4. Этап 2. Тестирование обновления

3.4.1. Тестирование обновления направлено на своевременное выявление в обновлениях потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств (в том числе политических баннеров, лозунгов, призывов и иной противоправной информации).

3.4.2. Тестирование обновлений безопасности проводится исследователем.

3.4.3. Тестирование обновлений осуществляется в обязательном порядке в отношении обновлений безопасности[3]. Проведение тестирования в отношении иных обновлений осуществляется по решению исследователя.

3.4.4. Объем тестирования (состав проводимых тестов) обновлений безопасности определяется исходя из типа лицензирования программного обеспечения.

3.4.5. При проведении тестирования обновлений допускается применять инструментальные средства анализа и контроля, функциональные возможности которых обеспечивают реализацию положений настоящего Регламента, имеющие техническую поддержку и возможность адаптации (доработки) под особенности проводимых тестирований, свободно распространяемые в исходных кодах, или средства тестирования собственной разработки. Рекомендуется применять инструментальные средства анализа и контроля, не имеющие каких-либо ограничений по их применению, адаптации (доработке) на территории Российской Федерации.

3.4.6. Состав и содержание работ по тестированию обновлений безопасности представлен в разделе 4 настоящего Регламента.

3.4.7. Результаты тестирования обновлений безопасности оформляются в виде отчета. Форма отчета представлена в Приложении № 1 к настоящему Регламенту.

---

[3] Обновления безопасности – обновления, предназначенные для устранения уязвимостей программных, программно-аппаратных средств объектов информатизации организации.

3.4.8. В случае если по результатам тестирования в обновлении безопасности выявлены признаки недекларированных возможностей, в отчет должна быть включена вся техническая информация, необходимая для пояснения выполненных в ходе исследования операций и результатов, полученных в ходе исследований (в том числе все отчеты инструментальных средств анализа и контроля). В отношении выявленных признаков недекларированных возможностей исследователем определяются ограничения и условия, при которых установка обновления безопасности возможна. Указанные сведения включаются в отчет тестирования обновлений безопасности.

3.4.9. По решению исследователя в отчет может быть включена иная информация (в том числе информация о иных проведенных тестах).

3.4.10. В случае если по результатам тестирования (выполнения ручного анализа) в обновлении безопасности выявлены вредоносное программное обеспечение и (или) недекларированные возможности, указанная информация направляется в ФСТЭК России и Национальный координационный центр по компьютерным инцидентам (НКЦКИ) в соответствии с порядком, представленным на сайте https://bdu.fstec.ru/.

3.4.11. Для целей настоящего Регламента к признакам недекларированных возможностей обновлений безопасности относятся:

– попытки обращений к файловой системе, базам данных, электронной почте и другой информации, не имеющие отношения к функционалу обновляемых программных, программно-аппаратных средств;

– недокументированные обращения к сторонним (неизвестным Министерству) сетевым адресам и доменным именам, не относящимся к Министерству;

– системные вызовы, характерные для вредоносного программного обеспечения (например, попытки загрузки из сети «Интернет» библиотек и программных пакетов, не имеющих отношения к функционалу программного обеспечения, попытки перехвата сетевого трафика другого программного обеспечения, попытки мониторинга действий пользователей с другим программным обеспечением);

– потенциально опасные изменения в файловой системе в результате установки обновления, в том числе загрузка и установка недокументированных программного обеспечения, драйверов и библиотек, не имеющих отношения к функционалу обновляемого программного, программно-аппаратного средства;

– изменения конфигурации среды функционирования, не имеющие отношения к обновляемому программному, программно-аппаратному средству (например, появление новых автоматически загружаемых программ);

– отключение средств защиты информации и функций безопасности информации.

3.5. Этап 3. Установка обновления

3.5.1. Решение об установке обновления принимается Министерством с учетом результатов тестирования и оценки рисков нарушения функционирования объектов информатизации от установки таких обновлений.

3.5.2. Решение об установке обновлений безопасности принимается на основании сформированных по результатам тестов выводов и оценки результатов.

3.5.3. В отношении обновлений безопасности итоговый вывод о возможности установки программного обеспечения формируется в соответствии с таблицей 1.

Таблица 1

№ п/п	Тип лицензирования программного обеспечения	Тесты, на основании которых формируется итоговый вывод
1.	Проприетарное программное, программно-аппаратное средство	– Сверка идентичности обновлений безопасности (Т001) и (или) проверка подлинности обновлений безопасности (Т002); – Антивирусный контроль обновлений безопасности (Т003) и (или) поиск опасных конструкций безопасности (Т004); – Мониторинг активности обновлений безопасности в среде функционирования (Т005)
2.	Свободно распространяемое программное обеспечение	– Сверка идентичности обновлений безопасности (Т001) и (или) проверка подлинности обновлений безопасности (Т002); – Антивирусный контроль обновлений безопасности (Т003) и (или) поиск опасных конструкций безопасности (Т004); – Мониторинг активности обновлений безопасности в среде функционирования (Т005)
3.	Программное обеспечение с открытым исходным кодом	– Проверка подлинности обновлений безопасности (Т002); – Антивирусный контроль обновлений безопасности (Т003); – Мониторинг активности обновлений безопасности в среде функционирования

№ п/п	Тип лицензирования программного обеспечения	Тесты, на основании которых формируется итоговый вывод
		(Т005); – Ручной анализ обновлений безопасности (Т006).

4. Состав и содержание работ по тестированию обновлений программных, программно-аппаратных средств

4.1. Общие требования к проведению тестирования

4.1.1. Работы по тестированию обновлений программных, программно-аппаратных средств включают:

– проведение тестов в выбранной исследователем среде тестирования;

– оформление результатов выполненных тестов (тестирования обновления).

4.1.2. При проведении тестирования обновлений рекомендуется проведение следующих тестов:

– сверка идентичности обновлений (Т001);

– проверка подлинности обновлений (Т002);

– антивирусный контроль обновлений (Т003);

– поиск опасных конструкций в обновлениях (Т004);

– мониторинг активности обновлений в среде функционирования (Т005);

– ручной анализ обновлений (Т006).

4.1.3. Выбор тестов для конкретного обновления осуществляется исполнителем исходя из:

– возможности получения обновлений разными способами;

– возможности получения обновлений из разных источников в распакованном (расшифрованном) виде;

– возможности распаковки (расшифрования) обновления;

– наличия инструментальных средств анализа (контроля);

– типа лицензии программного обеспечения;

– иных технических возможностей.

4.1.4. В случае выявления исследователем признаков недекларированных возможностей в ходе прохождения теста, обновление должно быть проанализировано в обязательном порядке ручным способом, в соответствии с разделом 4.7 настоящего Регламента.

4.2. Сверка идентичности обновлений (Т001)

4.2.1. Сверка идентичности проводится в случае возможности получения обновлений разными способами и (или) из различных источников.

4.2.2. Сверка идентичности предусматривает:

– получение обновления разными способами и (или) получение обновления из

различных источников (например, получение обновления с IP-адресов, расположенных на территории Российской Федерации, а также за ее пределами);

– расчет контрольных сумм файлов обновления, полученных различными способами и (или) из различных источников;

– сравнение обновлений, полученных разными способами и (или) из разных источников, путем сравнения их контрольных сумм.

4.2.3. По результатам выполнения теста делается промежуточный вывод по обновлению в соответствии с таблицей 2.

Таблица 2

Результат выполнения теста	**Промежуточный вывод по обновлению**
Обновления идентичны (контрольные суммы файлов обновления сходятся)	Является безопасным
Выявлены различия, объяснены исследователем и не вызывают опасности	
Выявлены различия, идентифицировать назначение которых не удалось	Являются потенциально опасным
Выявлены признаки недекларированных возможностей	Являются опасным

4.2.4. В случае выявления несоответствий в контрольных суммах файлов обновления, данное обновление должно быть проанализировано в обязательном порядке ручным способом, в соответствии с разделом 4.7 настоящего Регламента.

4.3. Проверка подлинности обновлений (T002)

4.3.1. Проверка подлинности обновления проводится в случае наличия у исследователя возможности получить файл(ы) обновления в распакованном (расшифрованном) виде до его установки в среде функционирования, а также при наличии предоставляемых разработчиком обновления штатных средств проверки подлинности файла(ов) обновления.

4.3.2. Проверка подлинности предусматривает:

– распаковку (расшифрование) файла(ов) обновления;

– сверку на соответствие критериям подлинности.

4.3.3. Критерии проверки подлинности предоставляются разработчиком программного обеспечения (обновления программного обеспечения). В качестве таких критериев могут выступать контрольные суммы файлов или электронная цифровая подпись файлов.

4.3.4. По результатам выполнения теста делается промежуточный вывод по обновлению в соответствии с таблицей 3.

Таблица 3

Результат выполнения теста	Промежуточный вывод по обновлению
Установлена подлинность обновлений (значения критериев по результатам сверки идентичны)	Является безопасным
Обновления не прошли проверку подлинности	Являются опасным

4.3.5. В случае неуспешного прохождения теста или отсутствия возможности проведения теста, данное обновление должно быть проанализировано в обязательном порядке ручным способом, в соответствии с разделом 4.7 настоящего Регламента.

4.4. Антивирусный контроль обновлений (Т003)

4.4.1. Антивирусный контроль обновлений заключается в выявлении вредоносных компьютерных программ (вирусов) в исследуемом обновлении с использованием средств антивирусной защиты.

4.4.2. Для проведения теста обновлений безопасности обязательно использовать не менее двух средств антивирусной защиты разных разработчиков. Иные обновления допускается проверять с использованием одного средства антивирусной защиты.

4.4.3. Антивирусный контроль предусматривает:

– проверку обновлений средствами антивирусной защиты до их установки;

– проведение сигнатурного и эвристического анализа содержимого оперативной памяти, файловой системы и загрузочных секторов всех используемых носителей информации по завершению установки обновления.

4.4.4. По результатам выполнения теста делается промежуточный вывод по обновлению в соответствии с таблицей 4.

Таблица 4

Результат выполнения теста	Промежуточный вывод по обновлению
Не выявлены признаки вредоносной активности (в файлах обновления и в самом программном обеспечении после установки обновления)	Является безопасным
Признаки вредоносной активности выявлены (в файлах обновления или в самом программном обеспечении после установки обновления), сигнатура вредоносного программного обеспечения не определена	Являются потенциально опасным
Признаки вредоносной активности выявлены (в файлах обновления или в самом программном обеспечении после установки обновления), сигнатура вредоносного	Являются опасным

Результат выполнения теста	Промежуточный вывод по обновлению
программного обеспечения определена	

4.4.5. В случае неуспешного прохождения теста, файл(ы) обновлений, в которых выявлены признаки вредоносной активности, должны быть проанализированы в обязательном порядке ручным способом, в соответствии с разделом 4.7 настоящего Регламента.

4.5. Поиск опасных конструкций в обновлениях (T004)

4.5.1. Поиск опасных конструкций в обновлениях проводится в случае наличия у исследователя возможности получить файл(ы) обновления в распакованном (расшифрованном) виде до или после установки обновления в среде функционирования.

4.5.2. Поиск опасных конструкций предусматривает:

– поиск опасных конструкций в обновлениях с применением индикаторов компрометации, YARA-правил и других способов. Выбор конкретного способа определяется исследователем;

– контекстный поиск политических баннеров, лозунгов и другой противоправной информации в обновлениях.

4.5.3. По результатам выполнения теста делается промежуточный вывод по обновлению в соответствии с таблицей 5.

Таблица 5

Результат выполнения теста	Промежуточный вывод по обновлению
Опасные конструкции не найдены	Является безопасным
Найдены потенциально опасные конструкции, идентифицировать назначение которых не удалось	Являются потенциально опасным
Опасные конструкции найдены	Являются опасным

4.5.4. В случае неуспешного прохождения теста, файл(ы) обновлений, в которых выявлены опасные конструкции, должны быть проанализированы в обязательном порядке ручным способом, в соответствии с разделом 4.7 настоящего Регламента.

4.5.5. При проведении ручного анализа исследователем должно быть исследовано назначение выявленных опасных конструкций, подтверждена или опровергнута их опасность.

4.6. Мониторинг активности обновлений в среде тестирования (T005)

4.6.1. Мониторинг активности обновлений в среде тестирования заключается в получении и анализе сведений о поведении обновляемого программного, программно-аппаратного средства в результате его взаимодействия со средой функционирования или другими программами, а также анализе сведений о взаимодействии компонентов обновленного программного, программно-аппаратного средства.

4.6.2. Мониторинг активности обновлений в среде функционирования проводится при наличии возможности установки необходимых инструментов в среде тестирования обновляемого программного, программно-аппаратного средства.

4.6.3. Мониторинг активности обновлений предусматривает проведение:

– анализа результатов выполнения системных вызовов обновленного программного обеспечения;

– анализа получаемых и отправляемых обновленным программным, программно-аппаратным средством сетевых пакетов;

– анализа состава файловой системы до и после установки обновления программного, программно-аппаратного средства;

– сигнатурного поиска известных уязвимостей.

4.6.4. По результатам выполнения теста делается промежуточный вывод по обновлению в соответствии с таблицей 6.

Таблица 6

Результат выполнения теста	**Промежуточный вывод по обновлению**
Не выявлено признаков недекларированных возможностей	Является безопасным
Найдены признаки недекларированных возможностей, идентифицировать назначение которых не удалось	Являются потенциально опасным
Найдены признаки недекларированных возможностей	Являются опасным

4.6.5. В случае неуспешного прохождения теста, файл(ы) обновлений безопасности, в которых выявлены признаки недекларированных возможностей, должны быть проанализированы в обязательном порядке ручным способом, в соответствии с разделом 4.7 настоящего Регламента.

4.7. Ручной анализ обновлений (T006)

4.7.1. Ручной анализ обновлений проводится в случае, если по результатам выполнения тестов:

– выявлены различия в обновлениях безопасности, полученных разными

способами и (или) из разных источников;

– неуспешно пройден тест подлинности файла(ов) обновления безопасности;

– выявлены признаки вредоносной активности в файлах обновления в результате антивирусного контроля или мониторинга активности обновления в среде функционирования;

– обнаружены опасные конструкции.

4.7.2. Ручной анализ обновлений проводится в отношении компонентов обновлений, в которых по результатам прохождения перечисленных выше тестов выявлены указанные в пункте 4.7.1 настоящего Регламента условия. В случае если ручной анализ провести невозможно, исследователем делается вывод о наличии в обновлении признаков недекларированных возможностей.

4.7.3. Ручной анализ обновления предусматривает:

– анализ логики работы (в том числе дизассемблирование или декомпиляцию бинарного кода при наличии соответствующих возможностей);

– исследование компонентов обновления с помощью отладчиков и трассировщиков;

– проверку наличия в обновлении ключевой информации (паролей, секретных ключей и другой чувствительной информации);

– статический и динамический анализ (при наличии исходных кодов обновлений).

4.7.4. По результатам выполнения теста делается промежуточный вывод по обновлению в соответствии с таблицей 7.

Таблица 7

Результат выполнения теста	**Промежуточный вывод по обновлению**
Наличие недекларированных возможностей опровергнуто	Является безопасным
Выявлены недекларированные возможности без деструктивного функционала	
Выявлены недекларированные возможности с неустановленным функционалом	Являются потенциально опасным
Выявлены недекларированные возможности	Являются опасным

5. Ответственность

5.1. Сотрудники Министерства, на которых возложены обязанности по обновлению программного обеспечения, несут персональную ответственность за ненадлежащее исполнение или неисполнение требований, предусмотренных настоящим Регламентом.

Приложение № 1
к Регламенту обновления
программного обеспечения в
Министерстве архитектуры и
строительства Смоленской области

Форма отчета о тестировании обновления программного, программно-аппаратного средства в Министерстве архитектуры и строительства Смоленской области

1. Сведения об обновлении безопасности:

1.1	Наименование обновления безопасности	
1.2	Описание обновления безопасности	
1.3	Адрес информационного ресурса, на котором размещено обновление (URL-адрес)	
1.4	Контрольная сумма программного, программно-аппаратного средства, рассчитанная по ГОСТ 34.11 и иным алгоритмам	
1.5	Дата выпуска обновления безопасности	
1.6	Разработчик обновления безопасности	
1.7	Версия программного, программно-аппаратного средства	
1.8	Идентификаторы уязвимостей, на устранение которых направлено обновление безопасности	
1.9	Дата начала тестирования обновления безопасности	
1.10	Дата завершения тестирования обновления безопасности	

2. Результаты тестирования обновления безопасности:

Идентификатор теста	**Результат[4]**	**Среда тестирования[5]**	**Описание результатов тестирования[6]**
T001			
T002			

[4]В результате указывается выполнен или не выполнен тест. В случае, если выполнен, указывается промежуточный вывод по обновлению

[5] Указывается среда тестирования, согласно пункту 3.3.2 Регламента обновления программного обеспечения

[6] Описание результатов тестирования представляется в произвольной форме и должно включать описание теста, средств проведения тестирования, среды тестирования, выявленных признаков недекларированных возможностей и т.д.