МИНИСТЕРСТВО АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

«01» 07 2025 № 121-ОД

Об утверждении Регламента управления уязвимостями в Министерстве архитектуры и строительства Смоленской области

В соответствии с приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также с приказом 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 прилагаемый Регламент управления уязвимостями 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 2025г.

Регламент управления уязвимостями в Министерстве архитектуры и строительства Смоленской области

1. Общие сведения

1.1. Настоящий Регламент управления уязвимостями в Министерстве архитектуры и строительства Смоленской области (далее – Регламент) разработан с учетом положений следующих документов:

1.1.1. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

1.1.2. Приказ 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»;

1.1.3. Методический документ ФСТЭК России от 17 мая 2023 г. «Руководство по организации процесса управления уязвимостями в органе (организации)»;

1.1.4. Методический документ ФСТЭК России от 28 октября 2022 г. «Методика оценки уровня критичности уязвимостей 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 анализа и устранения уязвимостей, выявленных в программных, программно-аппаратных средствах Министерства.

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

1.4. Настоящий Регламент предназначен для сотрудников Министерства, включенных в состав участников процесса управления уязвимостями, в соответствии с разделом 4 настоящего Регламента.

1.5. Изменения в настоящий Регламент вносятся при принятии Министерством

---

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

решения об улучшении процесса управления уязвимостями.

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

2. Цель, задачи процесса управления уязвимостями

2.1. Целью реализации процесса управления уязвимостями является снижение вероятности реализации нарушителями угроз безопасности информации, связанных с использованием (эксплуатацией) уязвимостей, опубликованных в общедоступных источниках.

2.2. Реализация процесса управления уязвимостями достигается решением следующих задач:

– определение участников процесса управления уязвимостями;

– определение операций, выполняемых в процессе управления уязвимостями;

– закрепление ответственности по операциям между участниками процесса.

3. Описание процесса управления уязвимостями

3.1. Процесс управления уязвимостями включает 5 (пять) основных этапов:

– мониторинг уязвимостей и оценка их применимости;

– оценка уязвимостей;

– определение методов и приоритетов устранения уязвимостей;

– устранение уязвимостей;

– контроль устранения уязвимостей.

3.2. Процесс управления уязвимостями связан со следующими процессами и процедурами Министерства:

– мониторинг информационной безопасности – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей;

– оценка защищенности от угроз безопасности информации – анализ возможности использования обнаруженных уязвимостей для реализации компьютерных атак на объекты информатизации Министерства;

– оценка угроз безопасности информации – выявление и оценка актуальности угроз, реализация (возникновение) которых возможна на объектах информатизации Министерства;

– управление конфигурацией – контроль изменений, состава и настроек программного и программно-аппаратного обеспечения объектов информатизации;

– управление обновлениями – приобретение, анализ и развертывание обновлений программного обеспечения в Министерства;

– применение компенсирующих мер защиты информации – разработка и применение мер защиты информации, которые применяются на объектах информатизации взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их применения.

3.3. Процесс управления уязвимостями должен носить системный характер. Актуализация сведений об уязвимостях, составе технических и программных средств объектов информатизации Министерства должна проводиться на периодической основе (не реже чем каждые 2 месяца) и должны быть включены в ежегодный план мероприятий по защите информации. Внеплановый поиск уязвимостей может быть произведен при появлении в общедоступных источниках информации (сведений) о новых уязвимостях, которые потенциально могут быть на объектах информатизации.

3.4. Этап 1. Мониторинг уязвимостей и оценка их применимости

3.4.1. На данном этапе мониторинга уязвимостей и оценки их применимости осуществляется выявление уязвимостей на основании данных, получаемых из внешних и внутренних источников, и принятие решений по их последующей обработке.

3.4.2. Осуществляется выявление уязвимостей на основании данных из следующих источников:

3.4.2.1. Внутренние источники:

– системы управления информационной инфраструктурой (далее – ИТ-инфраструктура);

– базы данных управления конфигурациями;

– документация на объекты информатизации;

– электронные базы знаний Министерства.

3.4.2.2. База данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК России, https://bdu.fstec.ru/vul).

3.4.2.3. Внешние источники:

– открытые базы данных, содержащие сведения об известных уязвимостях;

– открытые официальные информационные ресурсы разработчиков программных и программно-аппаратных средств, используемых на объектах информатизации, и исследователей в области информационной безопасности.

3.4.3. Выбор конкретных источников и средств анализа защищенности (поиска уязвимостей) осуществляется исполнителем данной операции.

3.4.4. При использовании специализированных средств анализа защищенности (поиска уязвимостей) должно обеспечиваться использование актуальной (последней официально опубликованной разработчиком такого средства) базы признаков уязвимостей.

3.4.5. Для проведения выявления (поиска) уязвимостей могут привлекаться организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации.

3.4.6. Выявление (поиск) уязвимостей должен быть осуществлен в отношении всех компонентов объектов информатизации: автоматизированные рабочие места пользователей, серверы, среда виртуализации (при наличии), телекоммуникационное оборудование.

3.5. Этап 2. Оценка уязвимостей

3.5.1. На данном этапе определяется уровень критичности уязвимостей применительно к каждому объекту информатизации Министерства.

3.5.2. Уровень критичности уязвимостей оценивается в целях принятия Министерства обоснованного решения о необходимости устранения выявленных по результатам анализа уязвимостей в программных, программно-аппаратных средствах объектов информатизации.

3.5.3. Оценка уровня критичности производится лицами, назначенными ответственным за выполнение данной операции в разделе 7.

3.5.4. Оценка уровня критичности уязвимостей производится в соответствии с порядком, представленным в Приложении № 2 к настоящему Регламенту, в отношение конкретного объекта информатизации Министерства.

3.6. Этап 3. Определение методов и приоритетов устранения уязвимостей

3.6.1. На данном этапе определяются методы и приоритеты устранения уязвимостей. Определяется приоритетность устранения уязвимостей и выбираются методы их устранения.

3.6.2. Допускаются следующие методы устранения уязвимостей:

– установка обновления программного обеспечения;

– применение компенсирующих мер защиты информации.

3.6.3. Устранение уязвимостей в сертифицированных программных, программно-аппаратных средствах защиты информации должно обеспечивается в приоритетном порядке.

3.7. Этап 4. Устранение уязвимостей

3.7.1. На данном этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

3.7.2. Решение о необходимости устранения уязвимости в отношении конкретного объекта информатизации принимается Министерства (лицом, назначенным ответственным за выполнение соответствующей операции) в зависимости от уровня критичности уязвимостей программных, программно-аппаратных средств в объекте информатизации.

3.7.3. Устранение уязвимостей в сертифицированных программных,

программно-аппаратных средствах защиты информации должно осуществляться в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

3.7.4. В случае если уязвимости содержатся в зарубежных программных, программно-аппаратных средствах или программном обеспечении с открытым исходным кодом, решение об установке обновления такого программного обеспечения, программно-аппаратного средства принимается Министерством (лицом, назначенным ответственным за выполнение соответствующей операции) с учетом результатов тестирования этого обновления. Тестирование обновления должно быть проведено в соответствии с утвержденным в Министерстве Регламентом обновления программного обеспечения.

3.7.5. В случае невозможности получения, установки и тестирования обновлений программных, программно-аппаратных средств принимаются компенсирующие меры защиты информации.

3.7.6. Компенсирующие меры, как правило, представленные в бюллетенях безопасности разработчиков программных, программно-аппаратных средств, а также в описаниях уязвимостей, опубликованных в БДУ ФСТЭК России.

3.7.7. Выбор компенсирующих мер по защите информации должен осуществляться с учетом архитектуры и особенностей функционирования объекта информатизации, а также способов эксплуатации уязвимостей программных, программно-аппаратных средств.

3.7.8. Компенсирующими организационными и техническими мерами, направленными на предотвращение возможности эксплуатации уязвимостей, могут являться:

– изменение конфигурации уязвимых компонентов объекта информатизации, в том числе в части предоставления доступа к их функциям, исполнение которых может способствовать эксплуатации выявленных уязвимостей;

– ограничение по использованию уязвимых программных, программно-аппаратных средств или их перевод в режим функционирования, ограничивающий исполнение функций, обращение к которым связано с использованием выявленных уязвимостей (например, отключение уязвимых служб и сетевых протоколов);

– резервирование компонентов объекта информатизации, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

– использование сигнатур, решающих правил средств защиты информации, обеспечивающих выявление на объекте информатизации признаков эксплуатации уязвимостей;

– мониторинг информационной безопасности и выявление событий безопасности информации на объекте информатизации, связанных с возможностью эксплуатации уязвимостей.

3.7.9. В Министерстве установлены следующие сроки устранения уязвимостей, представленные в таблице 1.

Таблица 1

Уровень опасности уязвимости	Предельный срок устранения уязвимости	Единица измерения срока
Критический	1	час
Высокий	1	день
Средний	1	неделя
Низкий	1	месяц

3.8. Этап 5. Контроль устранения уязвимостей

3.8.1. На данном этапе осуществляются сбор и обработка данных о процессе управления уязвимостями и его результатах, а также принятие решений по улучшению данного процесса.

3.8.2. В случае выявления в ходе оценки защищенности неизвестных ранее уязвимостей (уязвимостей «нулевого дня») сведения о них, по решению Министерства, могут быть направлены в БДУ ФСТЭК России.

4. Участники процесса управления уязвимостями

4.1. Участниками процесса управления уязвимостями являются:

– Начальник отдела бухгалтерского учета, отчетности и планирования;

– Начальник отдела правового и кадрового обеспечения;

– Начальник отдела цифровизации и информационных систем.

5. Операции процесса управления уязвимостями

5.1. В рамках процесса управления уязвимостями в Министерстве реализуются следующие операции, представленные в таблице 2.

Таблица 2

№ п/п	Операция	Описание операции
Мониторинг уязвимостей и оценка их применимости		
1.	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к информационным системам органа (организации). Агрегирование и корреляция собираемых данных об уязвимостях
2.	Оценка применимости уязвимости	На основе информации об объектах информационных систем и их состоянии

№ п/п	Операция	Описание операции
		определяется применимость уязвимости к информационным системам органа (организации) с целью определения уязвимостей, не требующих дальнейшей обработки (не релевантных уязвимостей). Оценка применимости уязвимостей производится: - на основе анализа данных об ИТ-инфраструктуре, полученных из баз данных управления конфигурациями в рамках процесса «Управление конфигурацией»; - на основе анализа данных о возможных объектах воздействия, полученных в результате моделирования угроз в рамках процесса «Оценка угроз»; - по результатам оценки защищенности (п. 6)
3.	Принятие решений на получение дополнительной информации	Запрос дополнительной информации об уязвимости (сканирование объектов, оценка защищенности), если имеющихся данных недостаточно для принятия решений по управлению уязвимостями
4.	Сканирование объектов	Поиск уязвимостей и недостатков с помощью автоматизированных систем анализа защищенности. Выбор объектов и времени сканирования, уведомление заинтересованных подразделений (например, ситуационного центра, подразделения ИТ) о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
5.	Оценка защищенности	Экспертная оценка возможности применения уязвимости в информационных системах. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах органа (организации) с использованием PoC или средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение

№ п/п	Операция	Описание операции
		(тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации)
Оценка уязвимостей		
6.	Определение уровня опасности уязвимости	Расчет базовой, контекстной и временной метрик по методике CVSS с использованием калькулятора CVSS V3 или V3.1, размещенного в БДУ ФСТЭК России
7.	Определение влияния на информационные системы	Определение влияния уязвимого компонента на защищенность информационных систем выполняется с использованием результатов процесса «Оценка угроз» (в части сведений о недопустимых негативных последствиях и возможных объектах воздействий), при этом могут быть использованы данные об ИТ-инфраструктуре, полученные из баз данных управления конфигурациями (отдельные результаты из процесса «Управление конфигурацией»)
Определение методов и приоритетов устранения уязвимостей		
8.	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации
9.	Принятие решения о срочной установке обновлений	При обнаружении критической уязвимости может быть принято решение о срочной установке обновления программного обеспечения объектов информационных систем, подверженных уязвимости
Устранение уязвимостей		
10.	Тестирование обновления	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной

№ п/п	Операция	Описание операции
		информации (далее – недекларированные возможности)
Разработка и реализация компенсирующих мер защиты информации		
11.	Определение мер защиты информации и ответственных за их реализацию	Определение компенсирующих мер защиты информации, необходимых для нейтрализации уязвимости либо снижения возможных негативных последствий от ее эксплуатации. В ходе выполнения данной операции должны быть определены работники, участие которых необходимо для реализации выбранных компенсирующих мер защиты информации
12.	Согласование привлечения работников	В случае необходимости привлечения работников других подразделений для реализации компенсирующих мер защиты информации руководитель подразделения защиты согласует их привлечение с руководителями соответствующих подразделений
Контроль устранения уязвимостей		
13.	Принятие решения о способе контроля	Определение способа контроля устранения уязвимости: проверка объектов на наличие уязвимости (сканирование средствами анализа защищенности) либо оценка защищенности
14.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационным системам. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в информационных системах органа (организации) с использованием PoC или средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационным системам в обход ее системы защиты информации)
Разработка предложений по улучшению процесса управления уязвимостями		

№ п/п	Операция	Описание операции
15.	Согласование сроков устранения уязвимости	В случае нарушения сроков устранения уязвимостей новые сроки установки обновления согласуются с подразделением ИТ, сроки реализации компенсирующих мер защиты информации – с ответственными лицами, определенными на этапе 4.
16.	Создание заявки на срочную реализацию компенсирующих мер защиты информации	Заявка на реализацию компенсирующих мер формируется при отсутствии возможности установки обновления либо в случае недостаточности уже принятых компенсирующих мер защиты информации

6. Распределение ответственности за реализацию операций

6.1. Распределение ответственности за операции между участниками процесса управления уязвимостями представлена в Приложении № 1 к настоящему регламенту.

7. Ответственность

7.1. Участники процесса управления уязвимостями несут персональную ответственность за ненадлежащее исполнение или неисполнение требований, предусмотренных настоящим Регламентом.

Приложение № 1
к Регламенту управления уязвимостями
в Министерстве архитектуры и
строительства Смоленской области

Распределение ответственности за операции между участниками процесса управления уязвимостями

№ п/п	Операция	Участник и и роли
Мониторинг уязвимостей и оценка их применимости		
1.	Анализ информации об уязвимости	О, И
2.	Оценка применимости уязвимости	О, И
3.	Принятие решений на получение дополнительной информации	О, И
4.	Сканирование объектов	О, И
5.	Оценка защищенности	О, И
Оценка уязвимостей		
6.	Определение уровня опасности уязвимости	О, И
7.	Определение влияния на информационные системы	О, И
Определение методов и приоритетов устранения уязвимостей		
8.	Определение методов устранения уязвимостей	О, И
9.	Принятие решения о срочной установке обновлений	О, И
Устранение уязвимостей		
10.	Тестирование обновления	О, И
Разработка и реализация компенсирующих мер защиты информации		
11.	Определение мер защиты информации и ответственных за их реализацию	О, И

№ п/п	Операция	Участник и и роли
12.	Согласование привлечения работников	О, И, У
Контроль устранения уязвимостей		
13.	Принятие решения о способе контроля	О, И
14.	Оценка защищенности	О, И
Разработка предложений по улучшению процесса управления уязвимостями		
15.	Согласование сроков устранения уязвимости	О, И, У
16.	Создание заявки на срочную реализацию компенсирующих мер защиты информации	О, И

Ответственный – работник, ответственный за завершение выполнения операции
Исполнитель – работник, непосредственно выполняющий операцию
Участник – работник, участие которого требуется для выполнения операции

ПРИЛОЖЕНИЕ № 2
к Регламенту управления
уязвимостями в Министерстве
архитектуры и строительства
Смоленской области

Порядок оценки уровня критичности уязвимостей в Министерстве архитектуры и строительства Смоленской области

1. Порядок оценки уровня критичности уязвимостей

1.1. Определить перечень программных и программно-аппаратных средств, подверженных уязвимостям.

1.2. Определить места установки программных, программно-аппаратных средств, подверженных уязвимостям.

1.3. Произвести расчет уровня критичности уязвимости (V).

2. Расчет уровня критичности уязвимости

2.1. Расчет уровня критичности осуществляется по следующей формуле:

$$V = I_{cvss} * I_{infr}$$

2.1.1. I_{cvss} – показатель, характеризующий уровень опасности уязвимости;

2.1.2. I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование объекта информатизации.

2.2. Показатель I_{cvss} определяется путем расчета базовых, временных и контекстных метрик по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1[2].

2.2.1. Базовые метрики отражают основные характеристики уязвимостей, влияющие на доступность, целостность и конфиденциальность информации, которые не изменяются с течением времени и не зависят от среды функционирования программных, программно-аппаратных средств. Базовые метрики включают показатели, характеризующие вектор атаки, сложность атаки, уровень привилегий, взаимодействие с пользователем, влияние на конфиденциальность, целостность и доступность.

2.2.2. Временные метрики отражают характеристики уязвимости, которые изменяются со временем, но не зависят от среды функционирования программных, программно-аппаратных средств. Временные метрики включают показатели, характеризующие доступность средств эксплуатации, доступность средств

[2] https://www.first.org/cvss/

устранения, степень доверия к информации об уязвимостях.

2.2.3. Контекстные метрики отражают характеристики уязвимости, зависящие от среды функционирования программных, программно-аппаратных средств.

2.3. Показатель I_{cvss} может быть рассчитан с использованием калькулятора, содержащегося в Банке данных угроз безопасности информации ФСТЭК России в разделе «Уязвимости»[3]. Пошаговое руководство по расчету с использованием калькулятора Банка данных угроз ФСТЭК России отражено в Методическом документе ФСТЭК России от 28 октября 2022 г. «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

2.4. Показатель I_{infr} определяется по следующей формуле:

$$I_{infr} = k * K + l * L + p * P$$

2.4.1. K – показатель, характеризующий тип компонента объекта информатизации, подверженного уязвимости.

2.4.2. L – показатель, характеризующий количество уязвимых компонентов объекта информатизации (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов).

2.4.3. P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра объекта информатизации.

2.4.4. k, l, p – весовые коэффициенты показателей. Расчет весовых коэффициентов и оценок показателей, определяющих влияние уязвимости программных, программно-аппаратных средств на объект информатизации, проводится в соответствии с таблицей 1.

Таблица 1

№ п/п	Показатель	Вес	Значение	Оценка	Итог
1	Тип компонента информационной системы, подверженного уязвимости (K)	0,4	Уязвимости подвержены компоненты объекта информатизации, обеспечивающие реализацию критических процессов (бизнес-процессов), функций, полномочий	1	0,4
			Уязвимости подвержены серверы	0,8	0,32
			Уязвимости подвержено телекоммуникационное	0,8	0,32

[3] https://bdu.fstec.ru/calc3 или https://bdu.fstec.ru/calc31

№ п/п	Показатель	Вес	Значение	Оценка	Итог
			оборудование, система управления сетью передачи данных		
			Уязвимости подвержены автоматизированные рабочие места	0,5	0,2
			Уязвимости подвержены другие компоненты	0,5	0,2
2	Количество уязвимых компонентов объекта информатизации (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов) (L)	0,2	Более 70% компонентов от общего числа компонентов объекта информатизации	1	0,2
			50-70% компонентов от общего числа компонентов объекта информатизации	0,8	0,16
			10-50% компонентов от общего числа компонентов объекта информатизации	0,6	0,12
			Менее 10% компонентов от общего числа компонентов объекта информатизации	0,5	0,1
3	Влияние на эффективность защиты периметра системы, сети (P)	0,4	Уязвимое программное, программно-аппаратное средство доступно из сети «Интернет»	1	0,4
			Уязвимое программное, программно-аппаратное средство недоступно из сети «Интернет»	0,5	0,2

1.4. По результатам расчета определяется уровень критичности уязвимости в соответствии с таблицей 2.

Таблица 2

№ п/п	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
1	$7,0 \leq V \leq 10,0$	Критичный
2	$4,5 \leq V < 7,0$	Высокий
3	$1,5 \leq V < 4,5$	Средний
4	$V < 1,5$	Низкий