АДМИНИСТРАЦИЯ ГОРОДА СМОЛЕНСКА

П О С Т А Н О В Л Е Н И Е

от 27.02.2026 № 309-адм

Об утверждении Регламента по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в Администрации города Смоленска

В соответствии с Руководством по организации процесса управления уязвимостями в органе (организации), утвержденным ФСТЭК России 17.05.2023, Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025, руководствуясь Уставом города Смоленска,

Администрация города Смоленска п о с т а н о в л я е т:

1. Утвердить прилагаемый Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в Администрации города Смоленска.

2. Управлению информационных технологий Администрации города Смоленска разместить настоящее постановление на официальном сайте Администрации города Смоленска.

Глава города Смоленска А.А. Новиков

УТВЕРЖДЕН
постановлением Администрации
города Смоленска
от 27.02.2026 № 309-адм

РЕГЛАМЕНТ
по выявлению, анализу и устранению критичных уязвимостей в информационных системах, эксплуатируемых в Администрации города Смоленска

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент по выявлению, анализу и устранению критичных уязвимостей в информационных системах (далее - ИС), эксплуатируемых в Администрации города Смоленска (далее - Регламент), разработан в соответствии с Руководством по организации процесса управления уязвимостями в органе (организации), утвержденным ФСТЭК России 17.05.2023, Методикой оценки уровня критичности уязвимостей программных, программно-аппаратных средств, утвержденной ФСТЭК России 30.06.2025.

1.2. Регламент определяет состав и содержание работ по анализу и устранению критичных уязвимостей (далее - управление уязвимостями), выявленных в программных, программно-аппаратных средствах ИС, информационно-телекоммуникационных сетей, автоматизированных систем управления, в информационно-телекоммуникационных инфраструктурах центров обработки данных, на базе которых функционируют эти системы и сети.

1.3. Регламент подлежит применению операторами ИС при принятии ими мер по выявлению и управлению уязвимостями программных, программно-аппаратных средств ИС в соответствии с требованиями о защите информации, содержащейся в ИС, а также нормативными правовыми актами и методическими документами ФСТЭК России.

1.4. Выявление, управление уязвимостями в сертифицированных программных, программно-аппаратных средствах защиты информации обеспечивается в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией на них, а также с рекомендациями разработчика.

1.5. В Регламенте используются термины и определения, установленные национальными стандартами ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей», ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» и иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

Целями Регламента являются:

- координация деятельности структурных подразделений Администрации города Смоленска по выявлению, управлению уязвимостями в ИС;

- создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования структурных подразделений Администрации города Смоленска, а также конкретных ИС;

- организация взаимодействия между структурными подразделениями Администрации города Смоленска по вопросам устранения уязвимостей.

2. ПОРЯДОК ВЫЯВЛЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2.1. В ИС должно осуществляться выявление следующих типов уязвимостей:

- недостатки и (или) ошибки программного обеспечения (далее - ПО) ИС и их систем защиты информации (далее - СЗИ);

- недостатки аппаратных средств ИС, в том числе аппаратных СЗИ;

- организационно-технические недостатки.

2.2. Непосредственными исполнителями мероприятий по выявлению, управлению уязвимостями ИС являются администраторы безопасности и системные администраторы ИС.

На 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.

Процесс управления уязвимостями организуется для всех ИС Администрации города Смоленска и должен предусматривать постоянную и непрерывную актуализацию сведений об уязвимостях и объектах ИС. При изменении статуса уязвимостей (применимость к ИС, наличие исправлений, критичность) должны корректироваться способы их устранения.

Процесс управления уязвимостями связан с другими процессами и процедурами деятельности Администрации города Смоленска:

- 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 - анализ возможности использования обнаруженных уязвимостей для реализации компьютерных атак на ИС Администрации города Смоленска;

- оценка угроз безопасности информации - выявление и оценка актуальности угроз, реализация (возникновение) которых возможна в ИС Администрации города Смоленска;

- управление конфигурацией - контроль изменений, состава и настроек программного и программно-аппаратного обеспечения ИС;

- управление обновлениями - приобретение, анализ и развертывание обновлений ПО в Администрации города Смоленска;

- применение компенсирующих мер защиты информации - разработка и применение мер защиты информации, которые используются в ИС взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их применения.

Уровень критичности уязвимостей оценивается в целях принятия обоснованного решения администраторами безопасности о необходимости устранения уязвимостей, выявленных в программных, программно-аппаратных средствах по результатам анализа уязвимостей в ИС.

Исходными данными для определения критичности уязвимостей являются:

- база уязвимостей ПО, программно-аппаратных средств, содержащаяся в Банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), а также иные источники, содержащие сведения об известных уязвимостях;

- официальные информационные ресурсы разработчиков ПО, программно-аппаратных средств и исследователей в области информационной безопасности;

- сведения о составе и архитектуре ИС, полученные по результатам их инвентаризации и (или) приведенные в документации на ИС;

- результаты контроля защищенности ИС, проведенного оператором.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют ИС.

Оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится администраторами безопасности.

Оценка уровня критичности уязвимостей программных, программно-аппаратных средств применительно к конкретной ИС включает:

- определение программных, программно-аппаратных средств, подверженных уязвимостям;

- определение в ИС места установки программных, программно-аппаратных средств, подверженных уязвимостям (например на периметре системы, во внутреннем сегменте системы, при реализации критичных процессов (бизнес-процессов), и других сегментах ИС);

- расчет уровня критичности уязвимости программных, программно-аппаратных средств в ИС.

3. ПОРЯДОК АНАЛИЗА КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

На этапе анализа уязвимостей определяется уровень критичности уязвимостей применительно к ИС Администрации города Смоленска и осуществляется выявление уязвимостей на основании данных из следующих источников:

а) внутренние источники:

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

- базы данных управления конфигурациями;

- документация на ИС;

- электронные базы знаний Администрации города Смоленска;

б) база данных уязвимостей, содержащаяся в Банке данных угроз безопасности информации (далее - БДУ) ФСТЭК России;

в) внешние источники:

- базы данных, содержащие сведения об известных уязвимостях;

- официальные информационные ресурсы разработчиков программных и программно-аппаратных средств и исследователей в области информационной безопасности.

Источники данных могут уточняться или дополняться с учетом особенностей функционирования структурных подразделений Администрации города Смоленска, а также конкретных ИС.

На этапе анализа уязвимостей и оценки их применимости выполняются следующие операции:

№ п/п	Наименование операции	Описание операции
1	2	3
1.	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к ИС Администрации города Смоленска. Агрегирование и корреляция собираемых данных об уязвимостях
2.	Оценка применимости уязвимости	На основе информации об объектах ИС и их состоянии определяется применимость уязвимости к ИС Администрации города Смоленска 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»; - данных о возможных объектах воздействия, полученных в результате моделирования угроз в рамках процесса «Оценка угроз»; - результатов оценки защищенности
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.	Постановка задачи на сканирование объектов	Запрос на внеплановое сканирование объектов ИС в случае недостаточности либо неактуальности имеющихся данных, а также в случае получения информации об уязвимости после последнего сканирования

1	2	3
5.	Сканирование объектов	Поиск уязвимостей и недостатков с помощью автоматизированных систем анализа защищенности. Выбор объектов и времени сканирования, уведомление заинтересованных структурных подразделений Администрации города Смоленска о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
6.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к информационным системам. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в ИС Администрации города Смоленска с использованием средства эксплуатации уязвимости, в том числе в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации)

4. ПОРЯДОК УСТРАНЕНИЯ КРИТИЧНЫХ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

4.1. На этапе определения методов и приоритетов устранения уязвимостей определяется приоритетность устранения уязвимостей и выбираются методы их устранения: обновление ПО и (или) применение компенсирующих мер защиты информации, также принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) выявленных уязвимостей.

На этапе определения методов и приоритетов устранения уязвимостей решаются задачи:

- определения приоритетности устранения уязвимостей;
- выбора методов устранения уязвимостей: обновление ПО и (или) применение компенсирующих мер защиты информации.

На этапе определения методов и приоритетов устранения уязвимостей выполняются следующие операции:

№ п/п	Наименование операции	Описание операции
1	2	3
1.	Определение приоритетности устранения уязвимостей	Определение приоритетности устранения уязвимостей в соответствии с результатами расчета критичности уязвимостей на этапе оценки уязвимостей
2.	Определение методов устранения уязвимостей	Выбор метода устранения уязвимости: установка обновления или применение компенсирующих мер защиты информации
3.	Принятие решения о срочной установке обновлений	При обнаружении критичной уязвимости может быть принято решение о срочной установке обновления ПО объектов ИС, подверженных уязвимости
4.	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется в Управление информационных технологий Администрации города Смоленска (далее - Управление)

1	2	3
5.	Принятие решения о срочной реализации компенсирующих мер защиты информации	При обнаружении критичной уязвимости может быть принято решение о срочной реализации компенсирующих мер защиты информации в качестве временного решения до установки обновления
6.	Создание заявки на установку обновления	Заявка создается в случае, если определено, что установка обновления для устранения данной уязвимости не запланирована
7.	Создание заявки на реализацию компенсирующих мер защиты информации	Заявка на реализацию компенсирующих мер защиты информации формируется при отсутствии возможности установки обновления, а также в случае необходимости принятия мер до устранения уязвимости

4.2. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга. При этом выполняются следующие операции:

№ п/п	Наименование операции	Описание операции
1	2	3
1.	Согласование установки обновлений ПО с руководством Управления	Срочная установка обновлений ПО предварительно согласовывается с руководством Управления
2.	Тестирование обновления ПО	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации
3.	Установка обновлений ПО в тестовом сегменте	Установка обновлений ПО на выбранном тестовом сегменте ИС в целях определения влияния их установки на ее функционирование
4.	Принятие решения об установке обновления ПО	В случае, если негативного влияния от установки обновления ПО на выбранном сегменте ИС не выявлено, принимается решение о его распространении в ИС. В случае обнаружения негативного влияния от установки обновления ПО на выбранном сегменте ИС дальнейшее распространение обновления ПО не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации
5.	Установка обновления ПО	Распространение обновления ПО на объекты ИС
6.	Формирование плана установки обновлений ПО	Уязвимости, для устранения которых не была определена необходимость срочной установки обновлений ПО, устраняются в ходе плановой установки обновлений ПО. Формирование плана обновлений ПО осуществляется с учетом заявок на установку обновлений ПО

1	2	3
7.	Разработка и реализация компенсирующих мер защиты информации	Разработка и применение мер защиты информации, которые применяются в ИС взамен отдельных мер защиты информации, подлежащих реализации в соответствии с требованиями по защите информации, в связи с невозможностью их установки, обнаружением негативного влияния от установки обновления, а также в случае необходимости принятия мер до устранения уязвимости. К компенсирующим мерам защиты информации могут относиться: организационные меры защиты информации, настройка средств защиты информации, анализ событий безопасности, внесение изменений в ИТ-инфраструктуру

В случае отсутствия соответствующих результатов тестирования в БДУ ФСТЭК России тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с Регламентом.

При наличии соответствующих сведений могут быть использованы компенсирующие меры защиты информации, представленные в бюллетенях безопасности разработчиков программных, программно-аппаратных средств, а также в описаниях уязвимостей, опубликованных в БДУ ФСТЭК России.

Рекомендуемые сроки устранения уязвимостей:

- критичный уровень опасности - до 24 часов;
- высокий уровень опасности - до 7 дней;
- средний уровень опасности - до 4 недель;
- низкий уровень опасности - до 4 месяцев.

В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации выполняются следующие операции:

№ п/п	Наименование операции	Описание операции
1	2	3
1.	Определение компенсирующих 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 сотрудники Администрации города Смоленска, участие которых необходимо для реализации выбранных компенсирующих мер защиты информации
2.	Согласование привлечения сотрудников Администрации города Смоленска	В случае необходимости привлечения сотрудников Администрации города Смоленска, не входящих в состав Управления, для реализации компенсирующих мер защиты информации начальник Управления согласует их привлечение с руководителями соответствующих структурных подразделений Администрации города Смоленска
3.	Реализация организационных мер защиты информации	Реализация организационных мер защиты информации предусматривает: ограничение использования ИТ-инфраструктуры; организация режима охраны (в частности, ограничение доступа к техническим средствам); информирование и обучение сотрудников Администрации города Смоленска

1	2	3
4.	Настройка средств защиты информации	Оценка возможности реализации компенсирующих мер с использованием СЗИ, выбор СЗИ (при необходимости). Выполнение работ по настройке СЗИ
5.	Организация анализа событий безопасности	Организация постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления и блокирования попыток эксплуатации уязвимости
6.	Внесение изменений в ИТ-инфраструктуру	Внесение изменений в ИТ-инфраструктуру включает действия по внесению изменений в конфигурации программных и программно-аппаратных средств (в том числе удаление (выведение из эксплуатации)

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

Выбор компенсирующих мер защиты информации осуществляется оператором с учетом архитектуры и особенностей функционирования ИС, а также способов эксплуатации уязвимостей программных, программно-аппаратных средств.

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

- изменение конфигурации уязвимых компонентов ИС, 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 ИС, включая резервирование серверов, телекоммуникационного оборудования и каналов связи;

- использование сигнатур, решающих правил СЗИ, обеспечивающих выявление в ИС признаков эксплуатации уязвимостей;

- мониторинг информационной безопасности и выявление событий безопасности информации в ИС, связанных с возможностью эксплуатации уязвимостей.

5. КОНТРОЛЬ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

5.1. На этапе контроля устранения уязвимостей осуществляются:

- сбор и обработка данных о процессе управления уязвимостями и его результатах;

- принятие оперативных решений;

- доведение вышеуказанного до руководства Администрации города Смоленска для принятия решений по улучшению процесса управления уязвимостями.

На этапе контроля устранения уязвимостей выполняются следующие операции:

№ п/п	Наименование операции	Описание операции
1.	Принятие решения о способе контроля	Определение способа контроля устранения уязвимости: проверка объектов на наличие уязвимости (сканирование средствами анализа защищенности) либо оценка защищенности
2.	Проверка объектов на наличие уязвимостей	Выбор объектов и времени сканирования, уведомление заинтересованных структурных подразделений Администрации города Смоленска о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
3.	Оценка защищенности	Оценка возможности применения уязвимости к ИС. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости в ИС с использованием соответствующих инструкций или фрагмента кода, или средства эксплуатации уязвимости, в том числе в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к ИС в обход ее системы защиты информации)
4.	Выявление отклонений и неисполнений	Анализ результатов контроля устранения уязвимостей (определение корректности устранения уязвимостей и соблюдения сроков)
5.	Формирование предложений по разработке решений по улучшению процесса управления уязвимостями	Определение причин отклонений и неисполнений. Формирование предложений по разработке решений по улучшению процесса управления уязвимостями

5.2. В случае выявления в ходе оценки защищенности неизвестных ранее уязвимостей (уязвимостей «нулевого дня») сведения о них рекомендуется направлять в БДУ ФСТЭК России.