



**МИНИСТЕРСТВО
АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА
СМОЛЕНСКОЙ ОБЛАСТИ**

П Р И К А З

«24» 02 2026

№ 027-00

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», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также протоколом заседания Комиссии по информационной безопасности при Правительстве Смоленской области от 18.12.2025 п. 1.3.2.

п р и к а з ы в а ю:

1. Утвердить прилагаемый Регламент управления уязвимостями в Министерстве архитектуры и строительства Смоленской области.
2. Возложить ответственность за публикацию Регламента управления уязвимостями в Министерстве архитектуры и строительства Смоленской области на официальном сайте Министерства (<https://minstroy67.admin-smolensk.ru>) в срок до 28.02.2026 на Сенилову Ольгу Анатольевну, консультанта отдела цифровизации и информационных систем.
3. Признать утратившим силу Регламент управления уязвимостями в Министерстве архитектуры и строительства Смоленской области утвержденный от

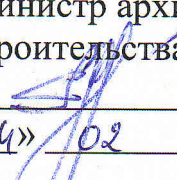
01.07.2025 приказом № 121-ОД, с изменением, внесенным приказом от 10.10.2025 № 186-ОД.

4. Контроль за исполнением настоящего приказа возложить на заместителя министра Жилкину Ингу Олеговну.

Министр

A handwritten signature in blue ink, consisting of several fluid, overlapping strokes, positioned between the words 'Министр' and 'К.Н. Ростовцев'.

К.Н. Ростовцев

Утверждаю
Министр архитектуры и
строительства Смоленской области

К.Н. Ростовцев
«24» 02 2026 г. 02700

Регламент управления уязвимостями в Министерстве архитектуры и строительства Смоленской области

1. Общие положения

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

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

1.1.2. Методический документ ФСТЭК России от 28 октября 2022 г. «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

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

1.3. Настоящий Регламент предназначен для сотрудников Министерства, включенных в состав участников процесса управления уязвимостями, в соответствии с разделом 9 настоящего Регламента и подлежит применению в отношении всех объектов информатизации¹, входящих в распределенную мультисервисную сеть Смоленской области (далее – Абоненты РМС СО) при принятии мер управления уязвимостями программных, программно-аппаратных средств информационных систем в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, а также иными нормативными правовыми актами и методическими документами ФСТЭК России.

1.4. Выявление, анализ и устранение уязвимостей 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.

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

Классификация уязвимостей информационных систем» и иными национальными стандартами в области защиты информации и обеспечения информационной безопасности.

Целями регламента являются:

- снижение вероятности реализации нарушителями угроз безопасности информации, связанных с использованием (эксплуатацией) уязвимостей, опубликованных в общедоступных источниках;
- создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования абонентов РМС СО;
- организация взаимодействия между Абонентами РМС СО по вопросам устранения уязвимостей.

2. Распределение ответственности за реализацию операций

2.1. Распределение ответственности за операции между участниками процесса управления уязвимостями представлена в таблице 1.

Таблица 1

Операции	Структурное подразделение, обеспечивающее информационную безопасность	
	Руководитель	Сотрудник
Мониторинг уязвимостей и оценка их применимости		
Анализ информации об уязвимостях	О	И
Оценка применимости уязвимости	О	И
Принятие решений на получение дополнительной информации		ОИ
Постановка задачи на сканирование объектов	ОИ	
Сканирование объектов	О	
Оценка защищенности	О	
Оценка уязвимостей		
Получение информации об объектах, подверженных уязвимости		ОИ
Определение уровня опасности		ОИ
Определение влияния на ИС		ОИ
Расчет критичности уязвимости	О	И
Определение методов и приоритетов устранения уязвимостей		
Определение приоритетности устранения уязвимостей	О	И
Определение методов устранения уязвимостей	О	И
Принятие решения о срочной установке обновлений	ОИ	
Создание заявки на срочную установку обновления	ОИ	

Создание задания на установку обновлений		ОИ
Принятие решения о срочной реализации компенсирующих мер защиты информации	ОИ	
Создание задания на реализацию компенсирующих мер защиты информации		ОИ
Устранение уязвимостей		
Согласование установки с руководством подразделения ИТ	ОИ	
Тестирование обновления	О	И
Установка обновления в тестовом сегменте	О	И
Принятие решения об установке обновления	ОИ	
Установка обновления	О	И
Формирование плана установки обновлений	ОИ	
Разработка и реализация компенсирующих мер защиты информации	О	И
Разработка и реализация компенсирующих мер защиты информации		
Определение мер защиты информации и ответственных за их реализацию	О	И
Согласование привлечения работников	ОИ	У
Реализация организационных мер защиты информации	ОИ	
Настройка средств защиты информации	О	
Организация анализа событий безопасности	О	
Внесение изменений в ИТ-инфраструктуру		У
Контроль устранения уязвимостей		
Принятие решения о способе контроля	ОИ	
Проверка объектов на наличие уязвимостей	О	
Оценка защищенности	О	
Выявление отклонений и неисполнений	О	
Разработка предложений по улучшению процесса управления уязвимостями	ОИ	И
Разработка предложений по улучшению процесса управления уязвимостями		
Определение причин и неисполнений	ОИ	
Корректировка механизмов мониторинга	О	И
Добавление источника сведений об уязвимостях	О	И
Корректировка механизмов оценки уязвимостей	О	И
Согласование сроков устранения уязвимости	ОИ	У
Создание заявки на срочную реализацию компенсирующих мер защиты информации	О	И
Обозначения:		
О – Ответственный – работник, ответственный за завершение выполнения задачи		
И – Исполнитель – работник, непосредственно выполняющий задачу		
У – Участник – работник, участие которого требуется для выполнения задачи		

3. Описание процесса управления уязвимостями

3.1. На объектах информатизации должно осуществляться выявление следующих типов уязвимостей:

- недостатки и (или) ошибки программного обеспечения (далее – ПО) и ее системы защиты информации (далее – СЗИ);
- недостатки аппаратных средств информационных систем, в том числе аппаратных СЗИ;
- организационно-технические недостатки.

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

- мониторинг уязвимостей и оценка их применимости;
- анализ уязвимостей;
- определение методов и приоритетов устранения уязвимостей;
- устранение уязвимостей;
- контроль устранения уязвимостей.

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 должна быть включена 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.

4. Этап мониторинга уязвимостей и оценки их применимости осуществляется

4.1. 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.

4.2. Процесс управления уязвимостями связан с другими процессами и процедурами деятельности 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 – 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 объекты информатизации Министерства;

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

Министерства;

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

- 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.

4.3. 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 на объектах информатизации.

4.4. Исходными данными для определения критичности уязвимостей являются:

- база уязвимостей программного обеспечения, 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 программного обеспечения, программно-аппаратных средств и исследователей в области информационной безопасности;

- сведения о составе и архитектуре информационных систем, полученные по результатам их инвентаризации и (или) приведенные в документации на информационные системы персональных данных;

- результаты контроля защищенности информационных систем, проведенные оператором.

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

4.6. Оценка уровня критичности уязвимостей программных, программно-аппаратных средств проводится лицами, назначенными ответственными за выполнение данной операции в разделе 9.

4.7. Оценка уровня критичности уязвимостей производится в соответствии с порядком, представленным в Приложении № 1 к настоящему Регламенту, в отношении конкретного объекта информатизации Министерства.

5. Этап анализа уязвимостей

5.1. На этапе анализа уязвимостей определяется уровень критичности уязвимостей применительно к объектам информатизации Абонента РМС СО 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 объект информатизации;
- электронные базы знаний Министерства;

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.

5.2. На этапе анализа уязвимостей и оценки их применимости выполняются операции, приведенные в таблице 2.

Таблица 2

№ п/п	Наименование операции	Описание операции
1	Анализ информации об уязвимости	Анализ информации из различных источников с целью поиска актуальных и потенциальных уязвимостей и оценки их применимости к объектам информатизации. Агрегирование и корреляция собираемых данных об уязвимостях
2	Оценка применимости уязвимости	На основе информации об объектах информатизации и их состоянии определяется применимость уязвимости к информационным системам Министерства 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
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 информатизации в случае недостаточности либо неактуальности имеющихся данных, а также в случае получения информации об уязвимости после последнего сканирования
5	Сканирование объектов	Поиск уязвимостей и недостатков с помощью автоматизированных систем анализа защищенности. Выбор объектов и времени сканирования, уведомление заинтересованных подразделений о проведении

		сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
6	Оценка защищенности	Экспертная оценка возможности применения уязвимости к объектам информатизации. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости на объектах информатизации с использованием средства эксплуатации уязвимости, в том числе, в ходе тестирования на проникновение (тестирования системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к объекту информатизации в обход ее системы защиты информации)

6. Этап определения методов и приоритетов устранения уязвимостей

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

6.2. На этапе определения методов и приоритетов устранения уязвимостей решаются задачи:

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

На этапе определения методов и приоритетов устранения уязвимостей выполняются операции, приведенные в таблице 3.

Таблица 3

№ п/п	Наименование операции	Описание операции
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 критической уязвимости может быть принято решение о срочной установке обновления программного обеспечения объектов информатизации, подверженных уязвимости
4	Создание заявки на срочную установку обновления	Заявка на срочную установку обновления направляется на согласование руководителю подразделения, обеспечивающего информационную

		безопасность
5	Принятие решения о срочной реализации компенсирующих мер защиты информации	При обнаружении критической 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

7. Этап устранения уязвимостей

7.1. На этапе устранения уязвимостей принимаются меры, направленные на устранение или исключение возможности использования (эксплуатации) уязвимостей, выявленные на этапе мониторинга. При этом выполняются операции, представленные в таблице 4.

Таблица 4

№ п/п	Наименование операции	Описание операции
1	Согласование установки с руководством подразделения, обеспечивающего информационную безопасность	Срочная установка обновлений программного обеспечения предварительно согласовывается с руководством подразделения, обеспечивающего информационную безопасность
2	Тестирование обновления	Выявление потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, в том числе политических баннеров, лозунгов, призывов и иной противоправной информации (далее – недеklarированные возможности)
3	Установка обновления в тестовом сегменте	Установка обновлений на выбранном тестовом сегменте информационной системы в целях определения влияния их установки на ее функционирование
4	Принятие решения об установке обновления	В случае, если негативного влияния от установки обновления на выбранном сегменте системы не выявлено, принимается решение о его распространении в системе. В случае обнаружения негативного влияния от установки

		обновления на выбранном сегменте системы дальнейшее распространение обновления не осуществляется, при этом для нейтрализации уязвимости применяются компенсирующие меры защиты информации
5	Установка обновления	Распространение обновления на объекты информационных систем
6	Формирование плана установки обновлений	Уязвимости, для устранения которых не была определена необходимость срочной установки обновлений, устраняются в ходе плановой установки обновлений. Формирование плана обновлений осуществляется с учетом заявок на установку обновлений
7	Разработка и реализация компенсирующих мер защиты информации	Разработка и применение мер защиты информации, которые применяются в информационных системах 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

7.2. Тестирование обновлений программных и программно-аппаратных средств осуществляется в соответствии с утвержденным в Министерстве Регламентом обновления программного обеспечения.

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

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

7.5. 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.

7.6. 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.

7.7. В Министерстве установлены следующие сроки устранения уязвимостей:

– критический уровень опасности до 24 часов;

– высокий уровень опасности – до 7 дней;

– средний уровень опасности – до 4 недель;

– низкий уровень опасности – до 4 месяцев.

7.8. В рамках выполнения подпроцесса разработки и реализации компенсирующих мер защиты информации выполняются операции, приведенные в таблице 5.

Таблица 5

№ п/п	Наименование операции	Описание операции
1	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
2	Согласование привлечения работников	В случае необходимости привлечения работников других подразделений для реализации компенсирующих мер защиты информации руководитель подразделения, обеспечивающего информационную безопасность, согласует их привлечение с руководителями соответствующих подразделений
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 персонала Министерства
4	Настройка средств защиты информации	Оценка возможности реализации компенсирующих мер с использованием средств защиты информации, выбор средств защиты информации (при необходимости). Выполнение работ по настройке средств защиты

		информации
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))

8. Этап контроля устранения уязвимостей

8.1. На этапе контроля устранения уязвимостей осуществляется сбор и обработка данных о процессе управления уязвимостями и его результатах, принятие оперативных решений и их доведение до руководства Министерства для принятия решений по улучшению процесса управления уязвимостями.

8.2. На этапе контроля устранения уязвимостей выполняются операции, приведенные в таблице 6.

Таблица 6

№ 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 подразделений о проведении сканирования и дальнейшее сканирование выбранных объектов на наличие уязвимости
3.	Оценка защищенности	Экспертная оценка возможности применения уязвимости к объектам информатизации. В ходе оценки защищенности осуществляется проверка возможности эксплуатации уязвимости на объектах информатизации Министерства 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)
4.	Выявление отклонений и неисполнений	Анализ результатов контроля устранения уязвимостей (определение корректности устранения уязвимостей и соблюдения сроков)

5.	Разработка	Определение причин отклонений и неисполнений, предложений по разработке на их основе решений по улучшению процесса управления уязвимостями
----	------------	--

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

9. Участники процесса управления уязвимостями

9.1. Участниками управления уязвимостями являются:

- Начальник отдела бухгалтерского учета, отчетности и планирования;
- Начальник отдела правового и кадрового обеспечения;
- Начальник отдела цифровизации и информационных систем.

10. Ответственность

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

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 3.1².

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 устранения, степень доверия к информации об уязвимостях.

- 2.2.3. Контекстные метрики отражают характеристики уязвимости, зависящие

² <https://www.first.org/cvss/>

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 оборудование, система управления сетью передачи данных	0,8	0,32
			Уязвимости подвержены	0,5	0,2

³ <https://bdu.fstec.ru/calc3> или <https://bdu.fstec.ru/calc31>

№ п/п	Показатель	Вес	Значение	Оценка	Итог
			автоматизированные рабочие места		
			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) (<i>L</i>)	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 (<i>P</i>)	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

3.2. 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