DOI 10.37882/2223-2966.2026.03.26

ПРИМЕНЕНИЕ МЕТОДИКИ ОЦЕНКИ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ФСТЭК РОССИИ ДЛЯ АНАЛИЗА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

APPLICATION OF THE RUSSIAN FEDERATION'S FSTEC VULNERABILITY CRITICALITY ASSESSMENT METHOD TO ANALYZE THE EFFECTIVENESS OF INFORMATION SECURITY SYSTEMS IN GOVERNMENT INFORMATION SYSTEMS

E. Novikov
V. Afanasyev
N. Kunin

Summary. This article examines approaches to applying the new methodology of the Federal Service for Technical and Export Control of Russia (FSTEC) dated June 30, 2025 [1]. An analysis of the transition from a formal vulnerability assessment to a context-sensitive model is provided. An algorithm for using this methodology to quantitatively evaluate the effectiveness of implemented information security tools (ISS) is proposed, using government information systems (GIS) as an example, where information availability is a key parameter [10].

Keywords: analysis, evaluation methodology, effectiveness, information security systems, government information systems.

Новиков Евгений Иванович
кандидат технических наук, доцент,
МИРЭА — Российский технологический университет
novikov_ei@mirea.ru
Афанасьев Вадим Владимирович
кандидат технических наук, доцент,
МИРЭА — Российский технологический университет
afanasev_v@mirea.ru
Кунин Никита Тимофеевич
старший преподаватель,
МИРЭА — Российский технологический университет
kunin@mirea.ru

Аннотация. В статье рассматриваются подходы к применению новой методики ФСТЭК России от 30 июня 2025 года [1]. Проведен анализ перехода от формальной оценки уязвимости к контекстно-зависимой модели. Предложен алгоритм использования данной методики для количественной оценки эффективности внедренных средств защиты информации (СЗИ) на примере государственных информационных систем (ГИС), где ключевым параметром является доступность информации [10].

Ключевые слова: анализ, методика оценки, эффективность, системы защиты информации, государственные информационные системы.

Методика ФСТЭК России от 30 июня 2025 года представляет собой существенный шаг вперед по сравнению с чисто формальным подходом к управлению уязвимостями (например, основанным только на CVSS) [6, 7, 8, 12]. Она вводит контекстно-зависимую оценку, что критически важно для реальной безопасности.

Методика предлагает формулу расчета уровня критичности уязвимости (V), которая учитывает не только техническую сложность уязвимости, но и контекст инфраструктуры и актуальность угрозы:

$$V = I_{cvss} \times I_{infr} \times \left(I_{at} + I_{imp}\right),$$

где:

— I_{cvss} — базовая оценка по CVSS 3.1 (техническая опасность) [6];
— I_{infr} — влияние инфраструктуры (тип компонента, количество, доступность из Интернета);
— I_{at} — актуальность угрозы (наличие эксплойта);
— I_{imp} — тяжесть последствий (потеря целостности, выполнение произвольного кода и т.д.).

На выходе получается балл, определяющий жесткие сроки устранения: от 24 часов (Критический) до 4 месяцев (Низкий).

К положительным сторонам данной методики можно отнести:

1. Методика уходит от простой установки патчей «на всё подряд» к риск–ориентированному подходу. Это заставляет учитывать бизнес–значимость компонентов информационной системы.
2. Учет реальности угрозы (I_{at}) — пожалуй, самый сильный аспект. Если эксплойта нет, множитель I_{at}

равен 0,1, что резко снижает итоговый балл. Если есть эксплойт — 0,3, если зафиксирован факт его применения в реальной атаке — 0,6. Это позволяет не паниковать из-за теоретических уязвимостей с высоким CVSS.

3. Методика разделяет типы воздействий и их последствий (I_{imp}). Выполнение произвольного кода ($H = 0,5$) оценивается опаснее, чем XSS ($H = 0,1$), что технически обосновано.
4. Документ устанавливает конкретные сроки для устранения уязвимостей в зависимости от уровня, что дает ИБ–специалистам аргументы для бизнеса и ИТ–департамента.

К недостаткам методики можно отнести:

1. Чувствительность к качеству анализа киберугроз. Показатель I_{at} (наличие атак/эксплойтов) требует постоянного мониторинга БДУ ФСТЭК или иных баз [4]. Если данные об атаках поступят с задержкой, организация может ошибочно классифицировать критическую уязвимость как «среднюю».
2. Статичность весовых коэффициентов. Например, утечка конфиденциальной информации имеет вес 0,3, а нарушение целостности — 0,3. Для некоторых организаций (например, банков) утечка может быть критичнее нарушения целостности вспомогательной системы, но методика уравнивает эти риски.
3. Для каждой уязвимости нужно определить тип компонента, его количество и доступность [13]. Без автоматизации процесс для крупной инфраструктуры станет неподъемным.

Хотя методика предназначена для оценки уязвимостей, ее логику можно применить для оценки эффективности внедренных средств защиты информации (далее СЗИ).

Показатель эффективности защиты коррелирует с уровнем критичности уязвимостей [9, 11]. Высокая критичность неизбежно требует мобилизации больших ресурсов (как денежных, так и временных) для нейтрализации угрозы или минимизации ущерба. Важно также помнить, что массовое наличие критических уязвимостей кумулятивно снижает защищенность всей информационной системы.

Будем считать, что повышение эффективности СЗИ можно оценить через их способность снижать численные показатели формулы критичности уязвимости, переводя ее из статуса «Критический» в «Средний» или «Низкий».

Исходя из вышеописанного, попытаемся адаптировать методику ФСТЭК под такой класс информационных систем, как государственные информационные системы (далее ГИС). Предназначение ГИС заключается в инфраструктурной поддержке деятельности органов власти, организации межведомственного обмена данными и обеспечении прозрачности социально значимых процессов (например, выборов или реализации национальных проектов) для граждан [2]. Ключевым требованием к функционированию ГИС является предоставление пользователям данных, гарантирующее их полноту, оперативность и достоверность [3].

Для подобного класса систем подберём соответствующие общие значения показателей формулы расчета критичности уязвимостей. Основной упор сделаем на уязвимости, эксплуатируемые для реализации угроз доступности информации, что обусловлено функциональным назначением ГИС [10].

I_{at} — показатель, характеризующий возможность эксплуатации уязвимости. Примем его равным 0,6. Это указывает на то, что оцениваемая потенциальная уязвимость применяется в реальных атаках.

I_{imp} — показатель, характеризующий последствия эксплуатации уязвимости. Когда злоумышленник (или программный сбой) эксплуатирует уязвимость, направленную на доступность, ГИС перестает выполнять свою главную функцию — предоставлять сервис вовремя и в полном объеме.

Приведем список преднамеренных киберугрозы (по отношению к доступности) [4, 5]:

— DoS/DDoS–атаки. Перегрузка каналов связи или ресурсов серверов огромным количеством ложных запросов.
— Вредоносное ПО (шифровальщики/вайперы). Блокировка доступа к данным путем их шифрования или полное удаление информации.
— Взлом системы с целью остановки критических процессов.

Возможные последствия (по отношению к доступности):

— Полный отказ в обслуживании. Система перестает отвечать на любые запросы. Это может быть следствием «падения» службы, критической ошибки ядра или переполнения очереди запросов.
— Деградация производительности. Система работает, но крайне медленно. Время ответа увеличивается с миллисекунд до десятков секунд или минут, что делает использование ИС фактически невозможным.
— Исчерпание ресурсов. Эксплуатация уязвимости (например, утечки памяти или бесконечные циклы) приводит к тому, что процессор загружен на 100 %, оперативная память заполнена, а дисковое пространство забито временными файлами или логами.

— Каскадный сбой. Отказ одного компонента (например, базы данных) вызывает «эффект домино». Другие связанные системы (веб-интерфейс, мобильные приложения, системы межведомственного взаимодействия) также выходят из строя, пытаясь достучаться до упавшего узла.

В отношении показателей I_{infr}, I_{at} и I_{imp} действует принцип максимизации оценки. В случаях, когда контекст анализа допускает использование нескольких значений для одного показателя, в качестве итогового результата необходимо выбирать наибольшее из них. Поэтому, I_{imp} принимаем равным 0,3. Данное значение учитывает такие числовые показатели последствий воздействий, как: отказ в обслуживании (0,26, киберугроза — DoS/DDoS–атаки) и нарушение целостности данных (0,3, киберугроза — Вредоносное ПО (шифровальщики/вайперы)).

Таким образом:

$$V = I_{cvss} \times I_{infr} \times (0,6 + 0,3)$$

$$V = I_{cvss} \times I_{infr} \times 0,9$$

I_{infr} — показатель, характеризующий влияние уязвимости на функционирование информационных систем.

I_{infr} определяется по следующей формуле:

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

где:

— k, l, p — статичные весовые коэффициенты;

— K, L, P — значения показателей.

K — показатель, характеризующий тип компонента информационной системы, подверженного уязвимости. Для наглядности распределим угрозы по уровням информационной системы.

Поскольку рассмотренные угрозы нацелены на нарушение доступности, а непрерывный доступ к данным является приоритетной функцией ГИС, классификация уязвимых компонентов должна отражать эту критичность. Исходя из этого следует, что по типу компонента ИС стоит выбрать пункт «Уязвимости подвержены компоненты системы, обеспечивающие реализацию важных процессов (бизнес–процессов), функций, полномочий». Этому выбору соответствуют значения коэффициентов: $K = 1,1$, а произведение $k \times K = 0,55$.

L — показатель, характеризующий количество уязвимых компонентов информационной системы. В контексте уязвимостей, влияющих на доступность информации в ИС значение тяжело «спрогнозировать». Показатель сильно связан с архитектурой конкретной ГИС. Поэтому примем $L = x$, где $x : \{0,1; 0,12; 0,16; 0,2\}$.

Таблица 1.

Распределение угроз по уровням ИС

Типичные методы воздействия на доступность	На что направлена угроза?	Компонент ИС
DDoS (L3/L4), физическое повреждение кабелей, перехват сессий.	Каналы связи, маршрутизаторы, коммутаторы.	Сетевая инфраструктура
Перегрев, перепады напряжения, износ дисков.	Серверы, процессоры, оперативная память, СХД	Аппаратная часть
Эксплуатация 0–day уязвимостей, переполнение буфера.	Операционные системы, СУБД, веб-серверы	Программный уровень
Шифрование (Ransomware), удаление, порча индексов БД.	Базы данных, конфигурационные файлы, бэкапы	Данные
Блокировка доступа администраторов, фишинг.	АРМ (рабочие места) сотрудников, учетные записи	Пользовательский уровень

P — показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы или периметра сегмента информационной системы (в случае сегментирования информационной системы), или, иными словами, наличие удаленной доступности до уязвимого элемента ИС. Для информационных систем типа ГИС разумнее всего считать данное значение равным 0,33 (цель ГИС — непрерывная работы; угрозы доступности — DDoS, внешний нарушитель; $P = 1,1$, а $p \times P = 0,33$).

Таким образом:

$$V = I_{cvss} \times (0,55 + x + 0,33) \times (0,6 + 0,3)$$

$$V = I_{cvss} \times (0,88 + x) \times 0,9$$

С учетом того, что $L = x$:

— Для $x = 0,1$ (10 % компонентов от общего числа компонентов в информационной системе подвержено исследуемой угрозе)

$$V = I_{cvss} \times 0,882$$

— Для $x = 0,12$ (10 %–50 % компонентов от общего числа компонентов в информационной системе подвержено исследуемой угрозе)

$$V = I_{cvss} \times 0,9$$

— Для $x = 0,16$ (50 %–70 % компонентов от общего числа компонентов в информационной системе подвержено исследуемой угрозе)

$$V = I_{cvss} \times 0,936$$

— Для $x = 0,2$ (более 70 % компонентов от общего числа компонентов в информационной системе подвержено исследуемой угрозе)

$$V = I_{cvss} \times 0,972$$

Таким образом, для компонентов ГИС, доступных из сети интернет, обеспечивающих реализацию важных процессов ИС основным показателем, характеризующим критичность уязвимости (используемой в реальных атаках) связанной с угрозой доступности, будет являться I_{cvss}. Не зная точных данных об архитектуре, моделируемой ИС, но имея набор всех возможных значений параметра L, можно предположить, что для уязвимостей в ГИС, связанных с угрозами доступности

$$V \approx I_{cvss} \times 0,92,$$

где, 0,92 взято как среднеарифметическое значение от $(0,882;0,9;0,936;0,972)$ Для $I_{cvss} > 5,43$ показатель V принимает значения ВЫСОКОЕ (от 5 до 8) и КРИТИЧЕСКОЕ (больше 8).

Стоит отметить, критичность показателя I_{at}. Если предположить, что показатель I_{at} равен 0,3 (имеются сведения о наличии средств эксплуатации (эксплойта) уязвимости), то

$$V = I_{cvss} \times I_{infr} \times 0,6$$

$$V = I_{cvss} \times (0,88 + x) \times 0,6$$

— Для $x = 0,1$

$$V = I_{cvss} \times 0,558$$

— Для $x = 0,12$

$$V = I_{cvss} \times 0,6$$

— Для $x = 0,16$

$$V = I_{cvss} \times 0,624$$

— Для $x = 0,2$

$$V = I_{cvss} \times 0,648$$

$$V \approx I_{cvss} \times 0,61,$$

где, 0,61 взято как среднеарифметическое значение от $(0,558;0,6;0,624;0,648)$.

При таком значении I_{at} для $I_{cvss} > 8,1$ показатель V принимает значения ВЫСОКОЕ (от 5 до 8). При $I_{at} = 0,3$ для уязвимостей с $Icvss > 3,27$ показатель V принимает значение СРЕДНЕЕ (от 2 до 5). В реальных условиях функционирования ГИС показатель критичности уязвимости связанной с угрозой доступности выше НИЗКОГО неприемлем.

Самое большое влияние на уровень критичности уязвимости оказывает показатель I_{at}. Он зависит от качества анализа киберугроз и принимает значения $I_{at}\{0,6;0,3;0,1\}$. Вводимые средства защиты информации в ИС будут влиять на показатели I_{infr} и I_{imp}. В контексте применения методики для расчета эффективности СЗИ системы можно рассмотреть следующие сценарии:

1. Оценка эффективности межсетевых экранов и сегментации (параметр P). Методика вводит параметр P (доступность из Интернета):
— Без СЗИ сервер доступен напрямую ($P = 1,1$).
— С СЗИ (например NGFW/VPN), если оно настроено так, что уязвимый компонент скрыт за VPN или доступ к уязвимому порту заблокирован извне, параметр P меняется на 0,6 (недоступно из сети «Интернет»).
— Эффективность СЗИ в данном контексте измеряется снижением итогового балла V почти в 2 раза (1,1 против 0,6). Если внедрение NGFW позволяет перевести критические уязвимости в разряд «высоких» или «средних», инвестиция оправдана.
2. Оценка систем управления конфигурациями и доступом (параметры K и H)
— Параметр K (тип компонента): если с помощью СЗИ (например, PAM–системы или VDI) вы изолируете критические бизнес–процессы от уязвимых пользовательских АРМ, вы гарантируете, что уязвимость на АРМ ($K = 0,25$) не влияет на критический процесс ($K = 0,55$).
— Параметр H (последствия): если используется «песочница» или система контроля запуска приложений (AppLocker), которая блокирует «Выполнение произвольного кода» ($H = 0,5$), снижая последствия до простого «Отказа в обслуживании» ($H = 0,26$), это также демонстрирует эффективность СЗИ в снижении итогового риска.

На основе данных о назначении и классе защищенности ИС производится оценка показателя эффективности применяемых мер безопасности. Базовый показатель состояния системы (ρ) определяется выражением:

$$\rho = I_{infr} \times (I_{at} + I_{imp})$$

Итоговая эффективность внедрения средств защиты (Δ) рассчитывается как разность показателей системы в конечном (t_2) и начальном (t_1) состояниях:

$$\Delta = \rho(t_1) - \rho(t_2)$$

где t_1 — период до модернизации СЗИ, а t_2 — после.

Пример расчета: В момент t_1 состояние системы ρ принимает значение 0,8. В момент t_2, что соответствует введению в работу системы средств защиты информации, состояние системы ρ принимает значение 0,3. Итоговая эффективность будет равна:

$$\Delta = 0,8 - 0,3 = 0,5.$$

Анализ показывает, что методика ФТСЭК России является гибким инструментом, сочетающим качественную оценку рисков с строгим математическим аппаратом. Несмотря на сложность внедрения, для критически важных систем, таких как ГИС, она позволяет обоснованно управлять приоритетами безопасности. Переход к данной методике трансформирует процесс обеспечения безопасности из реактивного «латания дыр» в стратегическое управление рисками. Главная ценность — возможность математически доказуемого снижения класса критичности уязвимостей в зависимости от применяемых к информационной системе средств защиты (межсетевых экранов, песочниц, систем разграничения доступа). Это позволяет легитимно увеличивать регламентные сроки на устранение уязвимостей (например, переводя их из 24-часового режима в плановый), снижая нагрузку на ИТ-персонал и предотвращать остановку критических бизнес–процессов государственных информационных систем.

ЛИТЕРАТУРА

1. ФСТЭК России. Методика оценки уровня критичности уязвимостей программного обеспечения и программно-аппаратных средств. — Утверждена ФСТЭК России 30 июня 2025 г. — М., 2025.
2. Федеральный закон от 27.07.2006 № 149–ФЗ «Об информации, информационных технологиях и о защите информации».
3. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
4. Банк данных угроз безопасности информации (БДУ ФСТЭК России). — URL: [https://bdu.fstec.ru/] (https://bdu.fstec.ru/) (дата обращения: 16.02.2026).
5. ГОСТ Р 56546–2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. — М.: Стандартинформ, 2015.
6. Common Vulnerability Scoring System v3.1: Specification Document. — FIRST.Org, Inc. — URL: (https://www.first.org/cvss/v3.1/specification–document).
7. Марков А.С., Цирлов В.Л. Опыт и проблемы оценки серьезности уязвимостей программного кода // Вопросы кибербезопасности. — 2021. — № 2(42). — С. 48–57.
8. Баранов А.П., Бочков М.В. Методика адаптивной оценки критичности уязвимостей в автоматизированных системах управления // Проблемы информационной безопасности. Компьютерные системы. — 2022. — № 3. — С. 15–23.
9. Костров Д.В., Смирнов А.А. Оценка эффективности систем защиты информации в государственных информационных системах на основе риск–ориентированного подхода // Информация и безопасность. — 2023. — Т. 26, № 2. — С. 189–198.
10. Григина И.В., Попов А.Д. Моделирование угроз доступности информации в облачных сегментах государственных информационных систем // Безопасность информационных технологий. — 2022. — Т. 29, № 1. — С. 65–76.
11. Астеров Д.В. Подходы к количественной оценке эффективности мер по обеспечению безопасности значимых объектов КИИ // Защита информации. Инсайд. — 2021. — № 4(100). — С. 34–39.
12. Лукацкий А.В. Риск–ориентированное управление уязвимостями: от CVSS к реальным приоритетам // Вопросы защиты информации. — 2020. — № 4. — С. 12–18.
13. Саматов К.М. Проблемы реализации требований ФСТЭК России по контролю уязвимостей в крупных инфраструктурах // Information Security / Информационная безопасность. — 2023. — № 5. — С. 22–25.

Журнал «Современная наука: актуальные проблемы теории и практики»