

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ,
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004

DOI: 10.17212/2782-2230-2026-3-84-98

**РАЗРАБОТКА МОДЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ
ИНФРАСТРУКТУРНЫМИ УЯЗВИМОСТЯМИ
С УЧЕТОМ ИХ ПРИОРИТЕТА***

С.А. ГЛАДЫШЕВ¹, С.А. ГОЛУБЬ²

¹ РФ, 630008, г. Новосибирск, ул. Кирова, 23, ЗАО «Группа компаний С7», специалист по информационной безопасности. E-mail: s.galdyshev@s7.ru

² РФ, 630008, г. Новосибирск, ул. Кирова, 23, ЗАО «Группа компаний С7», специалист по информационной безопасности. E-mail: s.golub@s7.ru

В статье рассматриваются современные подходы к построению процесса управления уязвимостями в ИТ-инфраструктуре организаций с акцентом на приоритизацию уязвимостей и активов. Описываются ключевые этапы процесса: инвентаризация, выявление и оценка уязвимостей, приоритизация и устранение, а также мониторинг эффективности мер. Особое внимание уделено критериям классификации и приоритизации активов с учетом их бизнес-значимости, уровня доступа, последствий компрометации и сетевой доступности. Среди методов оценки уязвимостей анализируются существующие стандарты (CVSS 3.1), особенности zero day, доступность публичных эксплойтов и использование данных о трендах эксплуатации. Отмечается недостаточность стандартных методик приоритизации, предлагаются возможные усовершенствования, в том числе автоматизация с помощью современных сканеров и технологий машинного обучения. Разработанная модель приоритизации интегрируется в жизненный цикл процесса управления уязвимостями, закрепленный методическим документом ФСТЭК России, за счет чего формируется итоговая группировка из пяти групп приоритизации, возникающая на пересечении приоритета актива и критичности уязвимости и определяющая срок устранения, не превышающий регуляторный норматив. Эффективность разработанной модели оценивается с использованием отечественных нормативных метрик – операционных показателей методического документа ФСТЭК, коэффициента защищенности информации (КЗИ) и показателя зрелости процессов защиты информации (ПЗИ), что позволяет напрямую увязать результаты внедрения модели с требованиями регулятора. Полученные результаты могут быть использованы как готовое решение или в качестве основы для построения детализированного процесса управления уязвимостями с перспективой дальнейшей автоматизации.

* Статья получена 20 августа 2026 г.

Ключевые слова: управление уязвимостями, ИТ-инфраструктура, приоритизация уязвимостей, приоритизация активов, CVSS, уязвимости нулевого дня, доступность эксплойтов, оценка рисков, автоматизация безопасности, машинное обучение

ВВЕДЕНИЕ

Процесс управления уязвимостями является важнейшим аспектом кибербезопасности, который согласно [1] состоит из следующих этапов: мониторинга уязвимостей и оценки их применимости, оценки уязвимостей (определение уровня критичности), определения методов и приоритетов устранения, устранения уязвимостей.

Внедрение этого процесса в корпоративную инфраструктуру напрямую зависит от особенностей конечной инфраструктуры, а также информационных систем и средств защиты информации. Ключевой информационной системой процесса управления уязвимостями является сканер уязвимостей, парадигма использования которого рекомендуется вендорами с учетом технических возможностей предоставляемого решения. Так, Qualys реализует парадигму VMDR, объединяющую обнаружение активов, оценку, приоритизацию по бизнес-контексту и устранение в рамках единой платформы с непрерывным агентным сканированием [2]. Tenable предлагает гибридную модель – единый сканирующий движок Nessus, расширенный агентным и безагентным сбором данных, включая оценку облачных конфигураций [3]. Модуль Rapid7 в продукте InsightVM делает акцент на рискориентированной приоритизации через собственную метрику (VPR) и агентную непрерывную оценку конечных узлов без необходимости периодического сетевого сканирования [4]. В российской практике аналогичную парадигму предлагает Positive Technologies в продукте MaxPatrol VM, реализующем сбор данных об активах, выявление и приоритизацию уязвимостей на основе технологии Security Asset Management [5].

Однако предлагаемые методы построения процесса управления уязвимостями имеют ряд проблем, связанных с автоматизацией процесса, его внедрением в корпоративную инфраструктуру и приоритизацией выявленных уязвимостей. Большинство существующих решений автоматизируют лишь отдельные этапы процесса, а не полный цикл от обнаружения до подтвержденного устранения [6], а передача рутинных операций триажа автономным программным агентам пока не имеет достаточной эмпирической валидации [7]. Встраивание сканирования в CI/CD-конвейеры разработки требует согласования нескольких разнородных инструментов, что снижает эффект автоматизации на практике [8]. Формальные метрики приоритизации не учитывают контекст конкретной организации [9] и остаются внутренне противоречивыми: оценки одной и той же уязвимости в разных системах скоринга существенно

расходятся [10], единой общепринятой таксономии метрик приоритизации не выработано [11], что подтверждается масштабом всей базы NVD [12]. Наконец, эмпирические исследования показывают, что фактический уровень автоматизации в организациях заметно ниже декларируемого вендорами [13], социотехнические барьеры внедрения изучены меньше технических [14], а искусственный интеллект в реальном процессе управления уязвимостями выступает не нейтральным инструментом, а «соисполнителем» организационной рутины, изменяющим саму координацию команд [15], что в очередной раз подчеркивает потребность в использовании единой модели процесса с установленными метриками.

Основой задачей всех вышеупомянутых исследований помимо упрощения внедрения процесса управления уязвимостями в корпоративную инфраструктуру является повышение эффективности этого процесса. Этот показатель в отечественных компаниях оценивается через несколько взаимодополняющих показателей. На операционном уровне это соблюдение сроков устранения, установленных методическим документом ФСТЭК [1]: критический уровень – не более 24 часов, высокий – 7 дней, средний – 4 недели, низкий – 4 месяца, при этом сам уровень критичности определяется по отдельной методике оценки уязвимостей [16]. С вступлением в силу приказа ФСТЭК № 117 (с 01.03.2026) появляется формальный количественный норматив – коэффициент защищенности информации (КЗИ): значение от 0 до 1 рассчитывается не реже одного раза в полгода как взвешенная сумма 16 частных показателей по четырем группам мер, при этом устранение уязвимостей выделено в отдельный частный показатель (к32) в составе наиболее весомой группы «Защита информационных систем» [17]. Дополнительно тот же приказ вводит показатель зрелости процессов защиты информации (ПЗИ) – рассчитывается один раз в два года и оценивает не факт защищенности, а устойчивость и повторяемость самих процессов, включая управление уязвимостями [18].

Исходя из этого целью проводимого исследования является разработка модели процесса управления инфраструктурными уязвимостями, в основу которой ляжет метод приоритизации уязвимостей с учетом инфраструктурных особенностей. Для оценки эффективности разработанной модели будут использоваться отечественные метрики, закрепленные в соответствующих нормативных документах.

1. ОПИСАНИЕ МЕТОДА ПРИОРИТИЗАЦИИ УЯЗВИМОСТЕЙ

Для разработки эффективного метода приоритизации уязвимостей будут сформулированы стандартные критерии, свойственные каждой инфраструктуре с возможностью их адаптации. Целевой метод предполагает две основные

метрики приоритизации уязвимости: критичность актива, на котором находится уязвимость, и критичность самой уязвимости.

Приоритизацию активов информационной инфраструктуры предлагается осуществлять на основе критериев из табл. 1.

Таблица 1

Table 1

Критерии приоритизации активов информационной инфраструктуры

Prioritization criteria for information infrastructure assets

Критерий	Описание
Влияние на бизнес-процессы	Определяет, насколько отказ или компрометация актива приведет к прерыванию или остановке ключевых процессов организации
Уровень обрабатываемой или хранимой информации	Учитывается наличие в активе критически важных, конфиденциальных или персональных данных
Степень значимости в процессах инфраструктур	Оценивается, насколько актив необходим для функционирования других систем (например, является ли он центральным звеном или вспомогательным компонентом)
Доступ к управлению или конфигурации	Активы с административным доступом (например, контроллеры доменов) имеют более высокую критичность
Последствия компрометации или сбоя	Оценивается масштаб ущерба для организации: потеря данных, нарушение работы, финансовые, репутационные и правовые риски
Доступность резервирования и возможность быстрой замены	Если актив легко восстановить или заменить без значимых последствий, его критичность считается низкой
Сетевая доступность	Определяет уровень доступности актива из внешних и внутренних сетей: активы, находящиеся в открытом доступе для большого числа пользователей или доступные из внешних сетей (например, через интернет), обладают более высокой степенью критичности из-за повышенного риска атаки

На основе указанных в табл. 1 критериев формируется 3 основных приоритета активов: высокий, средний, низкий. К активам *высокого приоритета* относятся целевые и ключевые системы.

- При отказе или компрометации вызовут остановку/прерывание ключевых бизнес-процессов.
- Обработывают/хранят критически важную, особо конфиденциальную или персональную информацию.
- Являются центральным или основополагающим элементом инфраструктуры (точка отказа для многих систем).
- Обладают административным доступом либо средствами управления всей инфраструктурой.
- Компрометация данных влечет за собой максимальные негативные последствия: существенный финансовый, репутационный, правовой ущерб или нарушение регуляторных требований.

- Не подлежат быстрой замене или восстановлению без ущерба бизнесу.

- Доступны из внешних сетей или для большого числа пользователей.

Пример: контроллер домена, сервер баз данных с коммерческой тайной, шлюзовый сервер, сервер управления сетями, почтовый сервер компании.

Средний приоритет присваивается системам информационной безопасности и активам общего пользования.

- При отказе или компрометации оказывают влияние на бизнес-процессы, которые не приводят к полной остановке ключевой деятельности.

- Обработывают сведения средней чувствительности (например, служебную информацию, рабочие документы, общие корпоративные материалы).

- Являются важным компонентом, но не критической точкой отказа (например, поддерживающий сервер или функциональный сервис).

- Имеют ограниченные права управления или доступ к части инфраструктуры.

- Компрометация данных приведет к локальным потерям, нарушениям или необходимости восстановления.

- Могут быть быстро заменены/восстановлены с минимальным влиянием на бизнес-процессы.

- Сетевая доступность которых ограничена внутренней инфраструктурой или специально доверенными сегментами сети.

Пример: вспомогательные серверы, сервисы внутренней безопасности, рабочие станции ИБ-администраторов, серверы приложений внутри корпоративной сети.

К *низкому приоритету* относятся прочие активы: обычные рабочие станции, принтеры и другие периферийные устройства, сбой или потеря которых не приведет к значительным последствиям для организации. Однако стоит отметить, что распределение конкретных активов будет зависеть от организации конкретной инфраструктуры: тот или иной актив, указанный в примерах, может быть отнесен к другому уровню критичности. Перечень критериев является минимально достаточным, но может быть дополнен при необходимости.

Далее рассмотрим подход к приоритизации уязвимостей. Первым критерием критичности будет значение критичности классического подхода по распределению на категории: *critical, high, medium* и *low* по оценке CVSS 3.1. Одновременно стоит уделить внимание уязвимостям типа *zero day*, которым должен быть присвоен самый высокий приоритет при проработке. Под проработкой подразумевается оценка применимости в инфраструктуре, разработка и применение компенсирующих мер для исключения возможности эксплуатации уязвимости.

Также параметром оценки критичности уязвимости является совокупность способа ее эксплуатации (сетевой или не сетевой) и доступности актива (из внешней или не из внешней сети). Далее стоит обратить внимание на наличие публичного эксплойта для данной уязвимости. При сравнении двух уязвимостей с равным значением CVSS 3.1, находящихся на одном активе, та уязвимость, у которой опубликован эксплойт, будет иметь более высокий приоритет. Также стоит отметить значение конкретной уязвимости в трендовых списках. При наличии уязвимости в тренде наиболее эксплуатируемых уязвимостей (например, узнать эту информацию можно на ресурсе *cisa.kew*) необходимо повысить критичность ее уязвимости.

Без внимания не должны оставаться бюллетени и рекомендации регуляторов, в которых собраны актуальные уязвимости, способные повлечь за собой угрозу объектам критической информационной инфраструктуры. Наличие уязвимостей в информации от регуляторов должно служить фактором повышения критичности уязвимости, найденной в инфраструктуре.

В итоге все вышеперечисленные критерии приоритизации уязвимостей можно определить схемой, представленной на рисунке.

2. ОПИСАНИЕ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ С УЧЕТОМ МОДЕЛИ ПРИОРИТИЗАЦИИ

За основу модели процесса управления уязвимостями взят жизненный цикл процесса, закрепленный методическим документом ФСТЭК [1] и состоящий из пяти этапов: 1) мониторинг уязвимостей и оценка их применимости,

2) оценка уязвимостей, 3) определение методов и приоритетов устранения, 4) устранение уязвимостей и 5) контроль устранения. Встроим в этот цикл описанную выше модель приоритизации по активам (табл. 1) и по уязвимостям (рисунок) и рассмотрим, как это меняет содержание каждого этапа и какая группировка уязвимостей формируется в результате.

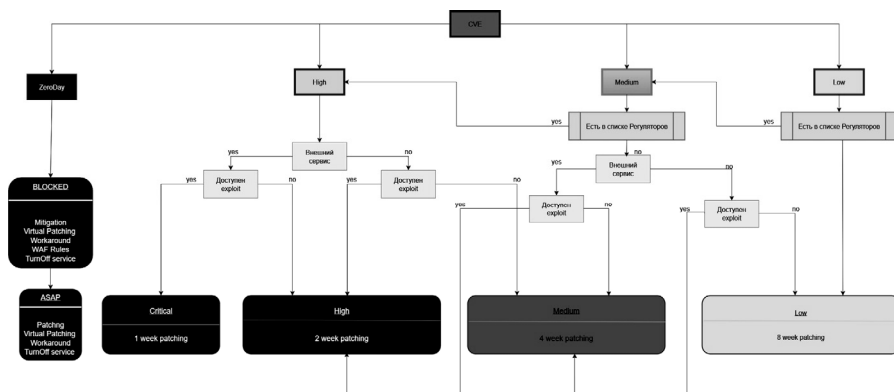


Схема приоритизации уязвимостей

Vulnerability prioritization scheme

На этапе мониторинга уязвимостей и оценки их применимости к стандартному сбору данных из БДУ ФСТЭК и иных источников уязвимостей добавляется процесс инвентаризации активов с присвоением каждому активу приоритета по критериям табл. 1 (высокий, средний, низкий). Это позволяет уже на входе связывать каждую обнаруженную уязвимость не только с ее собственными характеристиками, но и с критичностью актива, на котором она найдена.

На этапе оценки уязвимостей применяется схема, представленная на рисунке: уязвимость классифицируется по значению CVSS 3.1 (critical/high/medium/low), после чего эта базовая оценка корректируется тремя дополнительными факторами: 1) принадлежностью к уязвимостям типа zero day, 2) наличием уязвимости в бюллетенях регуляторов и 3) доступностью публичного эксплойта. Результатом этапа является итоговая категория критичности уязвимости, полученная не только из CVSS, но и с учетом реальной вероятности и актуальности эксплуатации.

Ключевое отличие описываемой модели реализовано на этапе определения методов и приоритетов устранения: именно здесь категория критичности

уязвимости (со второго этапа) пересекается с приоритетом актива (с первого этапа), формируя итоговую группу приоритизации с закреплённым сроком устранения. Правило пересечения формулируется следующим образом: базовым сроком устранения для каждого уровня критичности уязвимости служит норматив ФСТЭК [1] (критический – 24 часа, высокий – 7 дней, средний – 4 недели, низкий – 4 месяца); для уязвимостей на активах высокого приоритета этот срок ужесточается на одну ступень (высокий уровень критичности – 3 суток вместо 7 дней, средний – 7 дней вместо 4 недель, низкий – 4 недели вместо 4 месяцев), тогда как для активов среднего приоритета норматив ФСТЭК применяется без изменений, а для активов низкого приоритета уязвимости средней и низкой критичности устраняются в пределах того же норматива, но по остаточному принципу – после устранения уязвимостей той же категории критичности на более приоритетных активах. Ни при каких условиях итоговый срок не может превышать норматив ФСТЭК для соответствующего уровня критичности уязвимости: понижение приоритета актива не является основанием для нарушения регуляторных сроков, но может быть основанием для их ужесточения.

В результате пересечения трех уровней приоритета активов и четырёх категорий критичности уязвимостей формируется группировка из пяти итоговых групп приоритизации, представленная в табл. 2.

Таблица 2

Table 2

Итоговая группировка приоритетов устранения уязвимостей

Final grouping of vulnerability remediation priorities

Приоритет актива / Критичность уязвимости	Critical	High	Medium	Low
Высокий	Группа 1 (≤ 24 ч)	Группа 2 (≤ 3 сут.)	Группа 3 (≤ 7 дн.)	Группа 4 (≤ 4 нед.)
Средний	Группа 1 (≤ 24 ч)	Группа 3 (≤ 7 дн.)	Группа 4 (≤ 4 нед.)	Группа 5 (≤ 4 мес.)
Низкий	Группа 1 (≤ 24 ч)	Группа 3 (≤ 7 дн.)	Группа 5 (≤ 4 мес., в очереди последний)	Группа 5 (≤ 4 мес., в очереди последний)

Таким образом, вместо единственного основания для приоритизации (критичность уязвимости по CVSS), используемого в базовом варианте методики ФСТЭК, предложенная модель формирует пять групп приоритизации на пересечении критичности уязвимости и приоритета актива, на котором она обнаружена. Такая группировка не нарушает регуляторных нормативов сроков устранения [1] – итоговый срок для любой уязвимости не может быть больше официального норматива для ее уровня критичности, но позволяет обоснованно сокращать сроки для уязвимостей на наиболее значимых активах инфраструктуры и выстраивать очередность устранения внутри одной регуляторной группы сроков. Этапы устранения уязвимостей и контроля устранения (четвертый и пятый этапы цикла ФСТЭК) выполняются далее в соответствии с присвоенной группой. На этапе контроля собираются метрики эффективности процесса.

3. ОЦЕНКА ЭФФЕКТИВНОСТИ МОДЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

Эффективность предложенной модели оценивается метриками, закрепленными в отечественных нормативных документах.

На операционном уровне применимы показатели, прямо следующие из методического документа [1]: доля уязвимостей, устраненных в срок, установленный для присвоенной группы приоритизации (см. табл. 2); количество уязвимостей, не устраненных в срок, в разрезе групп; процент покрытия активов инфраструктуры сканером уязвимостей; количество обнаруженных и устраненных уязвимостей за выбранный период. Поскольку предложенная модель присваивает каждой уязвимости не только категорию критичности, но и конкретную группу с фиксированным сроком устранения, перечисленные показатели могут рассчитываться отдельно для каждой из пяти групп табл. 2, что дает более детальную картину эффективности процесса, чем усредненный показатель по всей организации.

На уровне формального норматива применим коэффициент защищенности информации (КЗИ), вводимый приказом ФСТЭК № 117 и методикой его расчета [17]. Устранение уязвимостей учитывается в КЗИ отдельным частным показателем «к32» в составе группы «Защита информационных систем» с наибольшим весовым коэффициентом ($R3 = 0,35$) среди всех групп показателей [17, 18]. Так как частный показатель «к32» обнуляется при повторном (в течение 12 месяцев) невыполнении соответствующей меры, а обнуление одного показателя обнуляет весь весовой коэффициент группы [17], для организации критически важно демонстрировать устойчивое соблюдение сроков устранения уязвимостей, а не разовое соответствие. Прямое соответствие структуры предложенной модели (группы приоритизации с фиксированными и не превышающими норматив ФСТЭК сроками) требованиям к частному

показателю «к32» позволяет использовать данные модели непосредственно как основание для расчета и подтверждения этого показателя при очередной (не реже одного раза в полгода) оценке КЗИ.

На уровне зрелости процессов применим показатель зрелости процессов защиты информации (ПЗИ), также вводимый приказом ФСТЭК № 117 [17, 18] и рассчитываемый не реже одного раза в два года. Показатель ПЗИ оценивает не факт защищенности, а устойчивость и повторяемость самих процессов защиты, включая управление уязвимостями. Формализация процесса приоритизации в виде фиксированных критериев (см. табл. 1), детерминированной схемы оценки уязвимостей (см. рисунок) и однозначной матрицы групп (см. табл. 2) переводит процесс управления уязвимостями из категории решений, принимаемых экспертом ситуативно, в категорию документированной и воспроизводимой процедуры, т. е. напрямую отвечает на тот критерий, по которому оценивается ПЗИ.

Представленные в этом разделе выводы носят методический характер: количественная оценка прироста значений КЗИ и ПЗИ, а также фактического сокращения доли просроченных уязвимостей при внедрении модели требует апробации на данных конкретной организации и является предметом дальнейшего исследования. При этом уже на уровне структуры модели видно, что все ее элементы: приоритизация активов, многофакторная оценка уязвимостей, группировка со сроками устранения – напрямую соответствуют перечню показателей, по которым эффективность процесса управления уязвимостями оценивается регулятором, что отличает предложенную модель от универсальных существующих на рынке решений.

ЗАКЛЮЧЕНИЕ

В настоящей статье описана модель приоритизации уязвимостей, показана ее интеграция в жизненный цикл процесса управления уязвимостями, закрепленный методическим документом ФСТЭК. Ключевым результатом этой интеграции стало формирование итоговой группировки из пяти групп приоритизации (см. табл. 2), возникающей на пересечении приоритета актива и критичности уязвимости. Такая группировка не нарушает регуляторных сроков устранения, установленных методическим документом ФСТЭК, но позволяет обоснованно ужесточать их для наиболее значимых активов инфраструктуры и выстраивать очередность устранения внутри одной регуляторной группы сроков, т. е. переводит приоритизацию с единственного основания (критичности уязвимости) на два взаимодополняющих основания одновременно.

Разработанная модель адаптивна: она может использоваться как готовое решение для широкого круга организаций или служить отправной точкой для построения специализированных процессов в сложных инфраструктурах с учетом уникальных особенностей. Модель позволяет добавлять в нее крите-

рии оценки критичности уязвимости, используя заданный вектор рассмотрения метрик CVSS 3.1 и иных факторов целевой инфраструктуры, влияющих на критичность обнаруженной уязвимости.

Внедрение предложенной модели позволяет структурировать процесс устранения уязвимостей, эффективно расставлять приоритеты и оптимально использовать ресурсы компании для снижения рисков. Таким образом, статья формирует основу для построения результативной системы управления инфраструктурными уязвимостями, отвечающей современным требованиям безопасности и нормативным требованиям ФСТЭК России.

СПИСОК ЛИТЕРАТУРЫ

1. ФСТЭК России. Руководство по управлению уязвимостями программного обеспечения и программно-аппаратных средств в органе (организации). Методический документ. – М., 2023. – 29 с. – URL: <https://base.garant.ru/406955550/> (дата обращения: 07.09.2026).
2. Qualys VMDR – Vulnerability management, detection and response (official documentation). – URL: https://docs.qualys.com/en/vm/latest/about_qualys_vm_vmdr.htm (accessed: 07.09.2026).
3. Tenable Nessus vs Qualys VMDR vs Rapid7 InsightVM: Vulnerability scanner comparison for enterprise security teams (2026). – URL: <https://www.decryptiondigest.com/blog/tenable-nessus-vs-qualys-vmdr-vs-rapid7-insightvm-vulnerability-scanner-comparison> (accessed: 07.09.2026).
4. Rapid7 InsightVM vs Tenable Nessus 2026: Coverage, risk. – <https://www.decryptiondigest.com/blog/rapid7-vs-tenable-vulnerability-management> (accessed: 07.09.2026).
5. MaxPatrol VM – Positive Technologies. – <https://global.ptsecurity.com/en/products/mp-vm/> (accessed: 07.09.2026).
6. SEEMA: An automation framework for vulnerability assesement and penetration testing / Y. Tyagi, S. Shekhar, P. Abhishek, S. Bhardwaj // 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN). – Vellore, India, 2023. – P. 1–5. – DOI: 10.1109/ViTECoN58111.2023.10157032.
7. Automated CVE Triage: Ai-agent framework for scalable vulnerability triaging and security automation / N. Amirov, E. Huseynov, N. Aliyev, Ş. Bahtiyar // 2025 18th International Conference on Information Security and Cryptology (ISCTürkiye). – Ankara, Türkiye, 2025. – P. 1–6. – DOI: 10.1109/ISCTrkiye68593.2025.11224852.
8. Cyril H.P., Kumara S. DevSecOps-driven security integration in the software development lifecycle using CI/CD pipelines // 2026 IEEE 5th International

Conference on AI in Cybersecurity (ICAIC). – Houston, TX, USA, 2026. – P. 1–6. – DOI: 10.1109/ICAIC67076.2026.11395737.

9. Jung B., Li Y., Bechor T. CAVP: A context-aware vulnerability prioritization model // Computers and Security. – 2022. – Vol. 116. – P. 102639. – DOI: 10.1016/j.cose.2022.102639.

10. Conflicting scores, confusing signals: An empirical study of vulnerability scoring systems / V. Koscinski, M. Nelson, A. Okutan, R. Falso, M. Mirakhorli // Proceedings of 32nd ACM Conference on Computer and Communications Security (CCS) (ACM CCS 2025). – Taipei, Taiwan, 2025. – URL: <https://arxiv.org/pdf/2508.13644> (accessed: 07.09.2026).

11. A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges / Y. Jiang, N. Oo, Q. Meng, H.W. Lim, B. Sikdar // arXiv. – 2025. – URL: <https://arxiv.org/pdf/2502.11070> (accessed: 07.09.2026).

12. Fragmentation of CVSS scores in the NVD: A quantitative analysis of inconsistency across vulnerability scoring standards / M. Walkowski, M. Nowak, A. Balsam, K. Nowak, J. Oko, S. Sujecki // Computers and Security. – 2026. – Vol. 169. – P. 104978. – DOI: 10.1016/j.cose.2026.104978.

13. An empirical study of automation in software security patch management / N. Dissanayake, A. Jayatilaka, M. Zahedi, M.A. Babar // arXiv. – 2022. – URL: <https://arxiv.org/pdf/2209.01518> (accessed: 08.09.2026).

14. Software security patch management: A systematic literature review of challenges, approaches, tools and practices / N. Dissanayake, A. Jayatilaka, M. Zahedi, M.A. Babar // Information and Software Technology. – 2022. – Vol. 144. – DOI: 10.1016/j.infsof.2021.106771.

15. Saadallah M., Shahim A., Khapova S. Rethinking vulnerability management: How AI and automation reshape organizational routines and supports adaptive cybersecurity systems // Systems (MDPI). – 2026. – Vol. 14 (5). – P. 573. – DOI: 10.3390/systems14050573.

16. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: утв. ФСТЭК России 28.10.2022. – URL: <https://bazanpa.ru/fstek-rossii-metodika-ot28102022-h5766872/> (дата обращения: 08.09.2026).

17. Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов КИИ РФ: утв. ФСТЭК России 11.11.2025). – URL: <https://www.garant.ru/products/ipo/prime/doc/412956179/> (дата обращения: 08.09.2026).

18. Шелыгин И. Приказ ФСТЭК № 117: понятный разбор для бизнеса: КЗИ и ПЗИ – практическое значение показателей. – 2026. – URL: <https://passwork.ru/blog/prikaz-fstek-117/> (дата обращения: 08.09.2026).

Гладышев Сергей Александрович, специалист по информационной безопасности ЗАО «Группа компаний С7». Основное направление научных исследований – разработка автоматизированных сценариев моделирования атак информационной безопасности. E-mail: s.galdyshev@s7.ru

Голубь Сергей Андреевич, специалист по информационной безопасности ЗАО «Группа компаний С7». Основное направление научных исследований – разработка автоматизированных сценариев моделирования атак информационной безопасности. E-mail: s.golub@s7.ru

DOI: 10.17212/2782-2230-2026-3-84-98

Development of a process model for managing infrastructure vulnerabilities with regard to their priority*

S.A. Gladyshev¹, S.A. Golub²

¹ CJSC "Group of Companies S7", 23 Kirova Street, Novosibirsk, 630008, Russian Federation. Information Security Specialist. E-mail: s.galdyshev@s7.ru

² CJSC "Group of Companies S7", 23 Kirova Street, Novosibirsk, 630008, Russian Federation, Information Security Specialist. E-mail: s.golub@s7.ru

This article examines modern approaches to building a vulnerability management process within the IT infrastructure of organizations, with an emphasis on the prioritization of vulnerabilities and assets. The key stages of the process are described: inventory, vulnerability identification and assessment, prioritization and remediation, and monitoring the effectiveness of the measures taken. Particular attention is given to the criteria for classifying and prioritizing assets based on their business significance, access level, consequences of compromise, and network accessibility. Among the vulnerability assessment methods, the article analyzes existing standards (CVSS 3.1), the specifics of zero-day vulnerabilities, the availability of public exploits, and the use of exploitation trend data. The insufficiency of standard prioritization methods is noted, and possible improvements are proposed, including automation through modern scanners and machine learning technologies. The developed prioritization model is integrated into the vulnerability management lifecycle established by the methodological document of FSTEC of Russia, forming a resulting grouping of five prioritization groups derived from the intersection of asset priority and vulnerability criticality, each with a remediation deadline that does not exceed the regulatory requirement. The effectiveness of the developed model is assessed using domestic regulatory metrics – the operational indicators of the FSTEC methodological document, the information security coefficient (KZI), and the security process maturity indicator (PZI) – allowing the results of the model's implementation to be directly linked to regulatory requirements. The results obtained can be used as a ready-made solution or as a basis for building a more detailed vulnerability management process with a view to further automation.

Keywords: vulnerability management, IT infrastructure, vulnerability prioritization, asset prioritization, CVSS, zero-day vulnerabilities, exploit availability, risk assessment, security automation, machine learning

* Received 20 August 2026.

REFERENCES

1. FSTEC of Russia. *Guidelines for the management of vulnerabilities in software and hardware within a government body (organization)*. Methodological document, 2023. 29 p. (In Russian). Available at: <https://base.garant.ru/406955550/> (accessed 07.09.2026).
2. *Qualys VMDR – Vulnerability Management, Detection and Response* (official documentation). Available at: https://docs.qualys.com/en/vm/latest/about_qualys_vm_vmdr.htm (accessed 07.09.2026).
3. *Tenable Nessus vs Qualys VMDR vs Rapid7 InsightVM: Vulnerability scanner comparison for enterprise security teams* (2026). Available at: <https://www.decryptiondigest.com/blog/tenable-nessus-vs-qualys-vmdr-vs-rapid7-insightvm-vulnerability-scanner-comparison> (accessed 07.09.2026).
4. *Rapid7 InsightVM vs Tenable Nessus 2026: Coverage, risk*. Available at: <https://www.decryptiondigest.com/blog/rapid7-vs-tenable-vulnerability-management> (accessed 07.09.2026).
5. *MaxPatrol VM – Positive Technologies* (product page). Available at: <https://global.ptsecurity.com/en/products/mp-vm/> (accessed 07.09.2026).
6. Tyagi Y., Shekhar S., Abhishek P., Bhardwaj S. SEEMA: An automation framework for vulnerability assessment and penetration testing. *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, Vellore, India, 2023, pp. 1–5. DOI: 10.1109/ViTECoN58111.2023.10157032.
7. Amirov N., Huseynov E., Aliyev N., Bahtiyar Ş. Automated CVE Triage: Ai-agent framework for scalable vulnerability triaging and security automation. *2025 18th International Conference on Information Security and Cryptology (ISCTürkiye)*, Ankara, Türkiye, 2025, pp. 1–6. DOI: 10.1109/ISCTrkiye68593.2025.11224852.
8. Cyril H.P., Kumara S. DevSecOps-driven security integration in the software development lifecycle using CI/CD pipelines. *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA, 2026, pp. 1–6. DOI: 10.1109/ICAIC67076.2026.11395737.
9. Jung B., Li Y., Bechor T. CAVP: A context-aware vulnerability prioritization model. *Computers and Security*, 2022, vol. 116, p. 102639. DOI: 10.1016/j.cose.2022.102639.
10. Koscinski V., Nelson M., Okutan A., Falso R., Mirakhorli M. Conflicting scores, confusing signals: An empirical study of vulnerability scoring systems. *Proceedings of 32nd ACM Conference on Computer and Communications Security (CCS) (ACM CCS 2025)*, Taipei, Taiwan, 2025. Available at: <https://arxiv.org/pdf/2508.13644> (accessed 07.09.2026).
11. Jiang Y., Oo N., Meng Q., Lim H.W., Sikdar B. A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges. *arXiv*, 2025. Available at: <https://arxiv.org/pdf/2502.11070> (accessed 07.09.2026).

12. Walkowski M., Nowak M., Balsam A., Nowak K., Oko J., Sujecki S. Fragmentation of CVSS scores in the NVD: A quantitative analysis of inconsistency across vulnerability scoring standards. *Computers and Security*, 2026, vol. 169, p. 104978. DOI: 10.1016/j.cose.2026.104978.

13. Dissanayake N., Jayatilaka A., Zahedi M., Babar M.A. An empirical study of automation in software security patch management. *arXiv*, 2022. Available at: <https://arxiv.org/pdf/2209.01518> (accessed 08.09.2026).

14. Dissanayake N., Jayatilaka A., Zahedi M., Babar M.A. Software security patch management: A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, 2022, vol. 144. DOI: 10.1016/j.infsof.2021.106771.

15. Saadallah M., Shahim A., Khapova S. Rethinking vulnerability management: How AI and automation reshape organizational routines and supports adaptive cybersecurity systems. *Systems (MDPI)*, 2026, vol. 14 (5), p. 573. DOI: 10.3390/systems14050573.

16. *Methodology for assessing the criticality level of vulnerabilities in software and hardware/firmware* (approved by FSTEC of Russia, 28.10.2022). (In Russian). Available at: <https://bazanpa.ru/fstek-rossii-metodika-ot28102022-h5766872/> (accessed 08.09.2026).

17. *Methodology for assessing the indicator of the state of technical information protection in information systems and ensuring the security of significant facilities of critical information infrastructure of the Russian Federation* (approved by FSTEC of Russia, 11.11.2025). (In Russian). Available at: <https://www.garant.ru/products/ipo/prime/doc/412956179/> (accessed 08.09.2026).

18. Shelygin I. *Prikaz FSTEC № 117: ponyatnyi razbor dlya biznesa: KZI i PZI – prakticheskoe znachenie pokazatelei* [Overview of FSTEC Order No. 117: KZI (Information Security Coefficient) and PZI (Security Process Maturity Indicator) – practical significance of the indicators]. 2026. Available at: <https://passwork.ru/blog/prikaz-fstek-117/> (accessed 08.09.2026).

Для цитирования:

Гладышев С.А., Голубь С.А. Разработка модели процесса управления инфраструктурными уязвимостями с учетом их приоритета // Безопасность цифровых технологий. – 2026. – № 3 (122). – С. 84–98. – DOI: 10.17212/2782-2230-2026-3-84-98.

For citation:

Gladyshev S.A., Golub C.A. Razrabotka modeli protsessu upravleniya infrastrukturnymi uyazvimostyami s uchetom ikh prioriteta [Development of a process model for managing infrastructure vulnerabilities with regard to their priority]. *Bezopasnost' tsifrovyykh tekhnologii = Digital Technology Security*, 2026, no. 3 (122), pp. 84–98. DOI: 10.17212/2782-2230-2026-3-84-98.