

Н. С. Демин¹✉, В. В. Селифанов¹

Оценка эффективности системы защиты значимого объекта критической информационной инфраструктуры на основе сравнительного анализа методик оценки

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: nikita.demin.1996@inbox.ru

Аннотация. В работе выполнено исследование подходов к оценке эффективности обеспечения информационной безопасности объектов критической информационной инфраструктуры Российской Федерации. Проведен сопоставительный анализ методики, утвержденной ФСТЭК России 11 ноября 2025 года, и положений ГОСТ Р 57580.2, регламентирующих процедуры оценки соответствия в области защиты информации. Установлено, что методика ФСТЭК носит преимущественно нормативно-контрольный характер и ориентирована на подтверждение соответствия минимально допустимому уровню защищенности, при этом характеризуется ограниченным набором оцениваемых показателей и недостаточной интеграцией с требованиями приказа ФСТЭК России № 239. В противоположность этому, из сферы финансового сектора взят ГОСТ Р 57580.2 реализующий развернутый процессный подход, включающий качественную оценку состояния и зрелости механизмов обеспечения безопасности. Обоснована необходимость модернизации методики ФСТЭК посредством расширения состава оцениваемых процессов и заимствования элементов качественной оценки.

Ключевые слова: критическая информационная инфраструктура, информационная безопасность, оценка эффективности, ФСТЭК России, ГОСТ Р 57580.2, зрелость процессов, методика оценки

N. S. Demin¹✉, V. V. Selifanov¹

Assessment of the Effectiveness of the Critical Information Infrastructure Protection System Based on Comparative Analysis of Assessment Methods

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: nikita.demin.1996@inbox.ru

Abstract. This paper examines approaches to assessing the effectiveness of information security at critical information infrastructure facilities in the Russian Federation. A comparative analysis is provided of the methodology approved by the Federal Service for Technical and Export Control (FSTEC) of Russia on November 11, 2025, and the provisions of GOST R 57580.2 which regulate compliance assessment procedures in the field of information security. It was established that the FSTEC methodology is primarily normative and control-oriented in nature and is focused on confirming compliance with the minimum permissible level of security. However, it is characterized by a limited set of assessed indicators and insufficient integration with the requirements of FSTEC Order No. 239. In contrast, GOST R 57580.2, adopted from the financial sector, implements a comprehensive process-based approach that includes a qualitative assessment of the state and maturity of security mechanisms. The need to modernize the FSTEC methodology by expanding the range of processes assessed and adopting elements of a qualitative assessment is substantiated.

Keywords: critical information infrastructure, information security, performance assessment, FSTEC of Russia, GOST R 57580.2, process maturity, assessment methodology

Введение

Когда говорят о критической информационной инфраструктуре (КИИ), обычно имеют в виду не просто набор информационных систем, а гораздо более сложную конструкцию – по сути, основу функционирования целых отраслей [1]. При этом важно понимать, что сбои в таких системах редко остаются локальными: чаще они «цепляют» связанные процессы и могут приводить к вполне ощутимым последствиям, в том числе экономическим.

Ситуация дополнительно усложняется тем, что в последние годы резко выросла степень цифровизации. Автоматизированные системы управления технологическими процессами (АСУ ТП) используются повсеместно, и зависимость от них уже трудно переоценить [2]. Даже кратковременные отклонения в их работе могут восприниматься как критические.

На этом фоне изменился и сам характер угроз. Если раньше атаки чаще носили массовый характер, то сейчас наблюдается другая тенденция: воздействия становятся более адресными. В ряде случаев злоумышленники заранее анализируют структуру объекта, его архитектуру, а иногда и организационные особенности [3]. Соответственно, требования к системе защиты тоже меняются.

Возникает вполне логичный вопрос – как оценить, насколько такая система действительно эффективна. Формальное наличие защитных механизмов уже не дает полной картины. Гораздо важнее понять, работают ли они в реальных условиях и способны ли противостоять актуальным угрозам [4].

В российской практике для этих целей используются разные подходы. Наиболее часто упоминаются методика ФСТЭК России (редакция 2025 года) [5] и стандарт ГОСТ Р 57580.2–2018 [6]. Дополнительно необходимо учитывать требования приказа ФСТЭК России № 239 [7], которые задают общий контур обеспечения безопасности КИИ. При этом сами методики, несмотря на схожую область применения, выстроены по разным принципам – и это важно учитывать.

Методика оценки эффективности ФСТЭК России

Если попробовать описать методику ФСТЭК России [5] «без формул», то она сводится к следующему: система защиты разбивается на отдельные элементы, и каждый из них оценивается через набор показателей.

Такие показатели отражают выполнение конкретных требований. Затем они группируются по направлениям, после чего формируется итоговая оценка защищенности $K_{зи}$. В расчетах учитываются весовые коэффициенты – это позволяет варьировать значимость отдельных направлений [7].

С одной стороны, все выглядит довольно логично. Есть четкая процедура, есть числовой результат, который можно интерпретировать. Для целей отчетности или контроля это, безусловно, удобно.

Источники данных тоже вполне понятны: результаты проверок, анализ документации, сведения о работе средств защиты [5, 8]. То есть формально оценка опирается на проверяемую информацию.

Но здесь возникает нюанс. Методика, по сути, фиксирует выполнение минимально установленных требований. Если требования выполнены – система считается защищенной. Насколько она устойчива к сложным сценариям атак – это уже не всегда очевидно [9].

Кроме того, не все процессы информационной безопасности получают достаточное внимание, наблюдается слабая интеграция с положениями приказа ФСТЭК России № 239. Например, управление уязвимостями или реагирование на инциденты учитываются, но скорее «по факту наличия», чем с точки зрения эффективности [7, 10]. На практике же именно эти процессы часто оказываются критичными.

Оценка соответствия по ГОСТ Р 57580.2

В ГОСТ Р 57580.2–2018 [6] логика построения оценки заметно отличается. Здесь система защиты рассматривается не как набор отдельных мер, а как совокупность процессов. Причем важно не только то, реализованы ли эти процессы, но и то, как именно они функционируют. Оценка проводится с учетом нескольких факторов: полноты внедрения, корректности выбора мер, согласованности процессов и устойчивости системы в целом [6, 11].

Отдельно вводится понятие зрелости процессов. Под ним понимается степень их формализации и управляемости, а также способность воспроизводиться в аналогичных условиях [12]. Это уже более «глубокий» уровень анализа. На практике это означает, что проверяется не только наличие регламентов, но и соответствие фактической деятельности этим регламентам, наличие механизмов контроля и, что немаловажно, способность системы адаптироваться к изменениям.

Такой подход дает более объемную картину. В ряде исследований отмечается, что именно процессная модель позволяет лучше выявлять реальные проблемы, а не только формальные несоответствия [13].

Сравнительный анализ методик

При сравнении двух подходов становится очевидно, что они решают разные задачи, хотя формально направлены на одно и то же. Методика ФСТЭК дает количественную оценку и позволяет быстро понять, выполнены ли требования [5]. Это ее сильная сторона. Но глубина анализа при этом ограничена. ГОСТ Р 57580.2, напротив, ориентирован на анализ процессов [6]. Здесь оценка менее «жесткая» в числовом смысле, зато позволяет увидеть, как система работает в целом.

Если упростить, различие можно сформулировать так: одна методика отвечает на вопрос «что сделано», другая – «как это работает». Различия проявляются и в деталях:

- уровень детализации анализа;

- учет изменений во времени;
- возможность выявления скрытых проблем;
- характер итоговой оценки.

При этом исследования показывают, что чисто количественные подходы не всегда отражают реальную устойчивость системы [14]. В то же время процессные модели лучше учитывают динамику и развитие системы защиты [15].

Направления совершенствования методики ФСТЭК России

С учетом выявленных особенностей представляется обоснованным развитие методики ФСТЭК России по следующим направлениям:

1. Расширение перечня оцениваемых процессов. Необходимо обеспечить включение в модель оценки процессов, регламентированных приказом № 239, что позволит повысить полноту анализа [7].
2. Введение градаций зрелости. Целесообразно дополнить количественную оценку качественными характеристиками, отражающими уровень развития процессов [6].
3. Интеграция качественных методов. Использование элементов процессного анализа позволит повысить аналитическую ценность результатов оценки.
4. Уточнение системы показателей. Расширение набора индикаторов должно быть направлено на учет организационных и управленческих аспектов обеспечения безопасности.
5. Формирование комбинированной модели. Перспективным представляется построение гибридной модели, сочетающей количественную формализацию и качественную интерпретацию результатов.

Заключение

Таким образом, говорить о том, что одна из методик «лучше», было бы не совсем корректно. Скорее, они дополняют друг друга.

Методика ФСТЭК удобна, когда требуется формализованная оценка – например, в рамках проверок. Она дает понятный результат, но не всегда позволяет глубоко проанализировать ситуацию.

ГОСТ Р 57580.2–2018 дает более развернутое представление о состоянии системы, поскольку учитывает процессы и их зрелость. Однако его применение требует более детального анализа.

На практике наиболее обоснованным выглядит комбинированный подход. Сочетание количественной оценки и процессного анализа позволяет получить более реалистичную картину и, соответственно, принимать более взвешенные решения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ. – Текст : непосредственный.

2. ГОСТ Р ИСО/МЭК 27001–2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 2021–09–01. – Москва : Стандартинформ, 2021. – Текст : непосредственный.
3. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности. – Введ. 2011–01–01. – Москва : Стандартинформ, 2010. – Текст : непосредственный.
4. ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. – Geneva : ISO, 2016. – Текст : непосредственный.
5. Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : утв. ФСТЭК России 11 нояб. 2025 г. – Текст : непосредственный.
6. ГОСТ Р 57580.2–2018. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Ч. 2. Методика оценки соответствия. – Введ. 2019–01–01. – Москва : Стандартинформ, 2018. – Текст : непосредственный.
7. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 25 дек. 2017 г. № 239. – Текст : непосредственный.
8. Методические рекомендации по обеспечению информационной безопасности организаций банковской системы Российской Федерации / Банк России. – Москва, 2021. – Текст : непосредственный.
9. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. – Москва : ФОРУМ, 2020. – 416 с. – Текст : непосредственный.
10. Комаров, В. В. Оценка и мониторинг защищенности информационных ресурсов / В. В. Комаров, М. В. Буйневич // Информационные технологии и телекоммуникации. – 2023. – Т. 11, № 4. – С. 45–52. – Текст : непосредственный.
11. Анисимов, А. С. Оценка эффективности средств защиты информации / А. С. Анисимов, А. И. Козачок // Информационная безопасность. – 2021. – № 2. – С. 34–39. – Текст : непосредственный.
12. Кузнецов, В. М. Процессный подход к управлению информационной безопасностью / В. М. Кузнецов // Информационная безопасность. – 2020. – № 3. – С. 15–21. – Текст : непосредственный.
13. Полтавцева, М. А. Оценка защищенности систем обработки данных / М. А. Полтавцева, Д. П. Зегжда // Вопросы кибербезопасности. – 2025. – № 5. – С. 22–30. – Текст : непосредственный.
14. Голембиовский, М. М. Формализация оценки защищенности объектов КИИ / М. М. Голембиовский [и др.] // Информационная безопасность. – 2023. – № 4. – С. 27–33. – Текст : непосредственный.
15. Скрыль, С. В. Совершенствование процедур оценки защищенности КИИ / С. В. Скрыль [и др.] // Безопасность информационных технологий. – 2023. – № 2. – С. 41–48. – Текст : непосредственный.

© Н. С. Демин, В. В. Селифанов, 2026