Практические аспекты моделирования процессов оценки зрелости защиты информации

Степаненко Дмитрий Сергеевич
студент, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, dmitriy-stepanenko-2016@mail.ru,

Крылова Светлана Львовна
старший преподаватель, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, svet711@yandex.ru,

Ивлиев Сергей Николаевич
кандидат технических наук, доцент, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, ivliev_sn@mail.ru

Предложена методика оценки зрелости процессов информационной безопасности организации, построенная на основе адаптированной модели Capability Maturity Model Integration с учётом требований риск-ориентированного подхода, закреплённого приказом ФСТЭК России от 11 апреля 2025 г. № 117. Методика объединяет пятиуровневую шкалу зрелости, восемь критичных групп показателей, формулу расчёта коэффициента зрелости с учётом весового коэффициента процессной дисциплины и цветовую индикацию отклонения достигнутого уровня от целевого. Апробация методики на информационной системе действующей организации выявила неравномерность зрелости процессов: направления, требующие постоянной процедурной дисциплины, систематически отстают от направлений, закрываемых точечными техническими мерами. Полученные результаты могут применяться организациями различного профиля для приоритизации инвестиций в защиту информации и подготовки к переходу на риск-ориентированные требования регулятора.

Ключевые слова: информационная безопасность, оценка зрелости, модель CMMI, риск-ориентированный подход, коэффициент зрелости, целевой уровень зрелости, SSE-CMM, NIST CSF, критерии защищённости, управление информационными рисками.

Вступление

Нормативно-правовое регулирование информационной безопасности в Российской Федерации в 2024–2026 годах прошло через качественную трансформацию [1]: от перечня формальных требований к результативному, риск-ориентированному подходу [2, с. 99-109]. Знаковым событием этого процесса стало утверждение приказа ФСТЭК России от 11 апреля 2025 г. № 117, вступившего в силу с 1 марта 2026 года [3]. Документ вводит два взаимодополняющих показателя оценки состояния защиты информации: показатель текущей защищённости от базового уровня угроз (Кзи) и показатель уровня зрелости мероприятий по защите информации (Пзи). Тем самым регулятор фактически закрепил на уровне обязательного требования то, что ранее рассматривалось лишь как рекомендательная практика – организации обязаны не просто внедрить средства защиты, а подтвердить достаточность и системность процессов их эксплуатации.

Проблема, стоящая перед большинством операторов информационных систем, заключается в том, что формальное соответствие чек-листам регулятора не гарантирует фактической устойчивости к атакам. Такая ситуация в профессиональной среде получила название «бумажной безопасности»: аттестат соответствия получен, документы оформлены, а реальные процессы управления рисками, доступом и инцидентами либо отсутствуют, либо существуют номинально. [4, с. 20-21] Смещение акцента с факта наличия средств защиты на измеримое качество процессов их эксплуатации требует инструментария, который позволял бы не просто проверить выполнение отдельных пунктов, а количественно оценить зрелость организации в целом и по отдельным направлениям.

Зарубежная практика накопила значительный опыт построения подобных моделей [5, с. 42-46] – рамочная программа NIST Cybersecurity Framework 2.0 с её уровнями реализации (Tiers) [6], модель Capability Maturity Model Integration [7], специализированный стандарт ISO/IEC 21827 (SSE-CMM) для инженерии безопасности [8,9], а также COBIT 2019 для управления ИТ-процессами [10]. Модель зрелости SOC компании CYBEREASON [11,12]. Однако прямое применение этих моделей к российским организациям затруднено: они не учитывают специфику отечественной нормативной базы, терминологию регуляторов (ФСТЭК, ФСБ) и не дают привычного для российского аудита количественного показателя, сопоставимого по логике с Кзи и Пзи.

Целью настоящей работы является разработка модели и апробация методики оценки зрелости процессов информационной безопасности, адаптирующей принципы CMMI и SSE-CMM к практике российских организаций госсектора и позволяющей получить не только качественную характеристику («на каком уровне находится процесс»), но и количественный коэффициент, пригодный для мониторинга динамики во времени.

Методология оценки зрелости

Выбор методологической основы

Сопоставление подходов к оценке защищённости информационных систем показывает принципиальное различие между моделью формального соответствия (Compliance) и моделью зрелости (Maturity). Первая опирается на нормативную базу и фиксирует состояние системы в конкретный момент – по факту прохождения аудита или аттестации; вторая рассматривает безопасность как непрерывно совершенствующийся процесс, интегрированный в деятельность организации, и потому лучше отражает реальную способность противостоять развивающимся угрозам.

Из доступных международных фреймворков в качестве методологической базы выбрана связка CMMI и SSE-CMM (ISO/IEC 21827). Такое решение обусловлено тремя обстоятельствами. Во-первых, CMMI даёт привычную для внутреннего и внешнего аудита ступенчатую шкалу зрелости, интуитивно сопоставимую с логикой Пзи из приказа ФСТЭК № 117. Во-вторых, SSE-CMM специализирован именно на инженерии безопасности и охватывает весь жизненный цикл системы – от формирования концепции до вывода из эксплуатации, что делает его пригодным для декомпозиции на предметные группы показателей. В-третьих, COBIT 2019, обладая развитой моделью зрелости процессов на базе ISO/IEC 15504 [7], в данном случае используется не как основа, а как вспомогательный инструмент – для оценки обеспечивающих ИТ-процессов (управление изменениями, конфигурациями, инцидентами), которые формально выходят за рамки чисто защитных мероприятий, но влияют на их результативность.

Шкала зрелости

Важно отметить, что далее описанная модель оценки была сформирована до публикации проекта ФСТЭК по оценке уровня зрелости деятельности в области технической защиты информации в информационных системах [13].

Исходная (референсная) модель оценки зрелости информационной и кибербезопасности [14] разрабатывалась как универсальный инструмент для коммерческой ИТ-компании или крупной организации с развитой ИТ-инфраструктурой, собственными разработками, сложными бизнес-процессами и высокими требованиями к непрерывности услуг. Впоследствии она

была адаптирована для оценки уровня защиты ГИС, функционирующей в организации с локальной информационной системой, низким уровнем защищенности персональных данных (УЗ 3), отсутствием в системе ПО собственной разработки, эпизодическими подрядчиками и без формальных требований к непрерывности бизнеса.

За основу принята пятиуровневая шкала, структурно повторяющая логику классической модели зрелости процессов информационной безопасности и включающая 5 уровней.

Уровень 1 «Исходный» характеризует ситуацию, когда контроль не определён, либо определён частично, выполняется непоследовательно и в значительной степени зависит от компетенций и добросовестности конкретных сотрудников, а не от формализованного процесса. Уровень 2 «Повторяемый» отражает состояние, при котором меры контроля внедрены и выполняются структурированно и последовательно, однако без формального документального закрепления. Уровень 3 «Определённый» предполагает, что контроль документирован, выполняется по единому формализованному порядку и его выполнение может быть проверено и подтверждено. Уровень 4 «Управляемый и измеримый» вводит требование периодической оценки эффективности контроля с документированием результатов такой оценки и корректировкой при необходимости. Уровень 5 «Постоянное совершенствование» соответствует состоянию, при котором управление рисками и контроль обеспечиваются на уровне всей организации непрерывно, включая проактивное решение возникающих проблем, а не реагирование по факту инцидента.

Критичные группы показателей

Для практического применения методики частные показатели объединены в укрупнённые группы, что позволяет фокусировать оценку на процессах, наиболее критичных для конкретного типа организации, не теряя при этом системности. В рамках апробации использован набор из восьми групп.

Группа «Роли и разделение обязанностей» фиксирует, закреплена ли ответственность за защиту информации за конкретными сотрудниками, как распределены права и обязанности и исключена ли ситуация, при которой один и тот же специалист одновременно создаёт данные и предоставляет себе доступ к ним. Группа «Управление рисками» [15, с. 41-49] описывает наличие регулярной процедуры выявления угроз, оценки вероятности и последствий их реализации, а также документированного принятия остаточных рисков руководством. Группа «Персонал и осведомлённость» [16, с. 83-90] охватывает процессы первичного и повторного обучения сотрудников, ознакомления с правилами обработки персональных данных под подпись и фиксации критически важных знаний, чтобы функционирование системы не зависело от одного человека. Группа «Управление доступом» объединяет процессы создания и блокировки учётных записей, требования к паролям, порядок хранения административных паролей и периодическую проверку соответствия предоставленных прав фактическим служебным обязанностям. Группа «Управление данными и персональными данными» относится к классификации информации, контролю передачи и уничтожения носителей и назначению ответственных за данные в подразделениях. Группа «Техническая безопасность» включает эксплуатацию антивирусных средств, обновление операционных систем, сегментацию сети, сбор и анализ журналов событий и учёт сертификатов средств криптографической защиты информации. Группа «Резервирование и непрерывность» описывает регулярность резервного копирования, раздельное хранение копий, тестирование процедур восстановления и наличие резервных каналов и источников питания. Группа «Физическая безопасность» охватывает меры защиты помещений с ИТ-оборудованием от несанкционированного доступа, пожара, затопления и иных внешних воздействий.

Фрагмент одной из группы частных показателей показан на рисунке 1.

Область	ID	Имя элемента управления	Описание риска	Уровень зрелости на основе оценки риска	Контроль Цель	Уровень зрелости индикация 1	Уровень зрелости индикация 2
						Исходный «Первоначальный контроль не определен или определен лишь частично и/или осуществляется непоследовательно и в значительной степени зависит от отдельных лиц.	Повторяемый Меры контроля внедрены и осуществляются структурированным и последовательным, но неформальным образом.
Управление рисками	RM.01	Структура управления информационными рисками	Структура управления информационными рисками и контролем не соответствует общеорганизационной модели управления рисками, что приводит к неправильному толкованию рисков и/или неспособности достичь ИТ-целей.	3	Была создана структура управления информационными рисками, которая соответствует целям организации и структуре управления рисками (предприятия).	– Нет назначенного ответственного за управление рисками. – Нет даже черновика методики или политики. – Оценка рисков проводится от случая к случаю, без какой-либо структуры.	– Назначен ответственный за управление рисками (обычно системный администратор или ответственный за ИБ). – Существует черновик (рабочий документ), описывающий подход к оценке рисков (например, в виде пометки или текстового файла). – Обучение проведено в рабочем порядке (устные инструкции). – Результаты оценки фиксируются (пусть даже кратко) и докладываются руководителю (устно или простой справкой). – Положение о рисках (отдельный регламент) не утверждено.
	RM.02	Оценка риска	Неотъемлемые и остаточные риски не (своевременно) идентифицированы и не оценены. Вероятность и воздействие не определены, что делает невозможной реализацию планов действий и отличающих мер контроля или инициатив по снижению риска.	2	Оценки рисков проводятся для определения фактических профилей рисков относительно целей деятельности администрации. Вероятность и влияние всех выявленных рисков оцениваются на регулярной основе с использованием качественных и количественных методов.	– Угрозы и риски не выявляются или выявляются случайно. – Нет реестра рисков. – Вероятность и последствия не оцениваются.	– Раз в год проводится выявление актуальных угроз (на основе типового перечня). – Используется простая качественная шкала: вероятность (низкая/средняя/высокая), последствия (низкие/средние/высокие). – Ведётся реестр рисков (Excel) с полями: угроза, вероятность, последствия, интегральный уровень, меры, ответственный. – Владельцы рисков уже назначены (из RM.01). – Результаты оценки (реестр) предоставляются руководителю (в электронном виде или на бумаге).

Рис. 1 Фрагмент модели оценки с группой «Управление рисками»

Приведённый перечень не является исчерпывающим – в рамках методики может быть предусмотрена более полная модель показателей, из которой укрупнённые группы формируются под структуру и приоритеты конкретной организации, что обеспечивает возможность применения данного подхода за пределами конкретного случая апробации.

Формула расчета коэффициента зрелости

Оценка зрелости отдельного направления вычисляется на основе бинарных ответов на контрольные критерии, сгруппированные по уровням шкалы. Для направления i коэффициент зрелости определяется выражением

$$C S_i = \sum_{u=1}^{U} \frac{\sum_{1}^{L} S_l}{L},$$

Где U – число оцениваемых уровней (не превышающее целевой уровень зрелости данного направления), L – количество контрольных критериев на уровне, а S_l – бинарная оценка отдельного критерия (0 или 1). Итоговая оценка по организации в целом рассчитывается как среднее по всем N направлениям с учётом штрафного коэффициента процессной дисциплины:

$$CS = \frac{\sum_{i=1}^{N} CS_i \times K_{proc_i}}{N},$$

где Kproc принимает значение 0,9 при неполном выполнении требований к зрелости процессов для соответствующего направления и 1,0 – при их полном выполнении. Введение штрафного коэффициента обеспечивает более тонкую дифференциацию направлений, формально набравших одинаковое количество баллов по контрольным вопросам, но отличающихся качеством документирования и повторяемости самого процесса.

Порядок расчёта подчинён четырём ограничениям, которые определяют, как именно частные оценки складываются в итоговый показатель. Первое ограничение состоит в том, что подтверждение минимального гигиенического уровня зрелости, который равен, например, двум, по организации в целом требует достижения этого уровня по каждому направлению без исключения: высокая оценка «сильных» направлений не может компенсировать хотя бы одно направление, не достигшее уровня 2,0. Второе ограничение требует, чтобы уровень зрелости по направлению подтверждался только при одновременном выполнении двух условий – положительных ответах на все вопросы уровня и соответствии зрелости самого процесса. Третье ограничение предписывает не учитывать в итоговой оценке значения, превышающие целевой уровень зрелости конкретного направления: организация должна сначала достичь целевого уровня по всем направлениям и только затем инвестировать в его дальнейшее повышение. Четвёртое ограничение вводит принцип последовательного подтверждения – сведения о достижении очередного уровня зрелости учитываются лишь после полного подтверждения предыдущего, что исключает «перепрыгивание» через уровни за счёт отдельных сильных показателей.

Цветовая индикация зон защищенности

Для перевода численного результата в форму, удобную для принятия управленческих решений, методика предусматривает цветовую классификацию зон защищённости. Целевой уровень зрелости каждого направления устанавливается по итогам предварительной оценки рисков и может принимать значения от 1 до 5. Уровни 1 и 2, соответствующие низкому и незначительному риску, маркируются зелёным цветом – для их контроля достаточно базовых, зачастую неформальных мер. Уровень 3, соответствующий среднему риску, маркируется жёлтым цветом и требует документированного, проверяемого контроля. Уровень 4 соответствует высокому риску и обозначается оранжевым цветом: помимо формального контроля необходима регулярная оценка его эффективности. Уровень 5, соответствующий критическому риску, маркируется красным цветом и требует высшей степени зрелости – непрерывного совершенствования и интеграции с общим управлением рисками организации.

Помимо цвета целевого уровня, для каждого отдельного показателя рассчитывается цвет текущего состояния – путём сопоставления достигнутого уровня с целевым. Зелёная зона фиксируется, если текущий уровень равен целевому или превышает его; жёлтая – если текущий уровень в точности соответствует целевому, но без запаса прочности; оранжевая – если отставание составляет ровно один уровень и требует планового усиления контроля; красная – если отставание составляет два уровня и более, что означает практическое отсутствие контроля риска и необходимость немедленных корректирующих мер. Такая индикация превращает набор разрозненных баллов в наглядную карту приоритетов, понятную не только специалистам по информационной безопасности, но и руководству, принимающему решения о распределении ресурсов.

Процедура апробации

Разработанная методика была применена к информационной системе действующей организации (ГИС): по каждой из восьми критичных групп

ответственными специалистами заполнялся набор контрольных критериев, соответствующих уровням составленной шкалы, после чего результаты агрегировались по приведённым выше формулам с учётом всех четырёх ограничений и переводились в цветовую индикацию.

Пример оценки согласно выдвинутым по направлению критериям показан в таблице 1.

Таблица 1
Критичные группы показателей, взятые для оценки группы «Физическая безопасность»

Критерий	Оценка	Выполнение
[PH.01-L1] Серверная закрывается на ключ, но ключ хранится у одного человека, журнал не ведется.	1	Да
[PH.01-L2] Серверная закрывается на ключ, ключ хранится у ограниченного круга лиц.	1	Да

Окончание таблицы 1

[PH.01-L2] В серверной установлен огнетушитель и датчик дыма.	1	Да
[PH.01-L2] Ведется журнал посещений серверной (дата, время, цель, ФИО).	1	Да
[PH.02-L2] При увольнении сотрудника ключи от серверной сдаются обязательно.	1	Да
[PH.01-L3] Установлена система видеонаблюдения за входом в серверную с хранением записей не менее 30 дней.	1	Нет
Итог по направлению	2,0	Кгос = 1,0

Такой порядок позволил проверить работоспособность механизма на практике, а не только на теоретическом уровне.

Результаты

Основным результатом работы является собственно работающий механизм оценки – совокупность адаптированной пятиуровневой шкалы, набора из восьми критичных групп показателей, формулы расчёта коэффициента зрелости с учётом коэффициента процессной дисциплины и правил цветовой индикации, переводящих количественную оценку в приоритеты для управленческих решений. В отличие от разрозненных чек-листов, применяемых при формальном комплаенсе, предложенный механизм даёт единый сопоставимый показатель как по отдельным направлениям, так и по организации в целом, а установленные ограничения (запрет компенсации слабых направлений сильными, обрезание пиков, последовательное подтверждение уровней) не позволяют завысить итоговую оценку за счёт отдельных удачно реализованных мер.

Подробно составленная диаграмма с выделенными направлениями, достигнутыми и целевыми уровнями по каждому направлению представлена на рисунке 2.

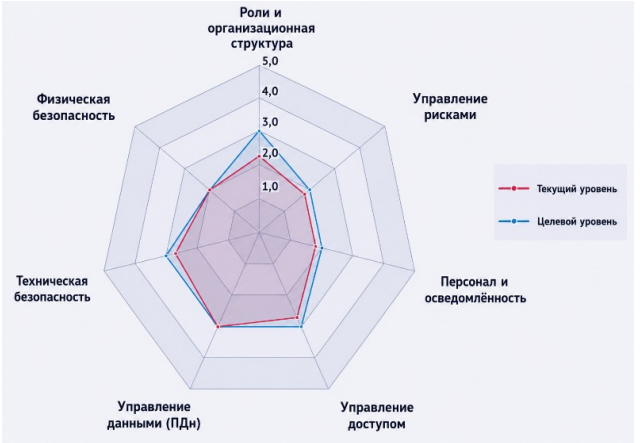


Рис. 2 Диаграмма по результатам оценки зрелости информационной безопасности

Апробация методики на реальной информационной системе подтвердила её практическую применимость и одновременно выявила устойчивую закономерность, характерную, по всей видимости, не только для рассмотренного случая, но и для организаций со сходной структурой ИТ-процессов. Направления, зрелость которых определяется однократным внедрением технического средства – прежде всего «Техническая безопасность» (антивирусная защита, сегментация сети, обновление программного обеспечения), – как правило, быстрее достигают устойчивого уровня 2–3, поскольку соответствующие меры реализуются точечно и не требуют постоянного пересмотра. Напротив, направления, зрелость которых зависит от регулярно повторяемой процедуры, а не от разового технического решения, склонны отставать. К числу таких направлений в первую очередь относится «Управление рисками»: регулярная переоценка угроз и документирование остаточного риска требуют организационной дисциплины, которую сложнее поддерживать, чем однократно настроенный технический контроль. Похожая картина характерна для группы «Резервирование и непрерывность» – само по себе выполнение резервного копирования почти всегда присутствует, тогда как регулярное тестирование процедур восстановления, что и является признаком более высокого уровня зрелости, реализуется значительно реже.

Отдельно апробация подтвердила уязвимость направления «Роли и разделение обязанностей» в организациях с ограниченным штатом ИТ-специалистов: совмещение функций создания данных и предоставления доступа к ним одним и тем же сотрудником, прямо обозначенное методикой как антипаттерн, чаще возникает не из-за игнорирования требований, а из-за объективной нехватки кадров, способных разделить эти функции. Направление «Персонал и осведомлённость» в среднем демонстрирует промежуточный результат: первичный инструктаж и ознакомление с правилами обработки данных, как правило, проводятся, тогда как повторное обучение и документирование критичных знаний носят менее системный характер. Таким образом, цветовая карта, полученная по итогам апробации, стабильно указывает на процессные, а не технические направления как на источник наибольшего числа оранжевых и красных зон, что отличается от интуитивного представления, при котором в первую очередь усиливают именно технические средства защиты.

Выводы

В рамках исследования разработан и апробирован механизм оценки зрелости процессов информационной безопасности организации, адаптирующий модели CMMI и SSE-CMM к отечественной нормативной практике и логике риск-ориентированного подхода, закреплённого приказом ФСТЭК России № 117 [1]. Механизм включает пятиуровневую шкалу зрелости, восемь критичных групп показателей, формулу расчёта коэффициента зрелости с учётом штрафного коэффициента процессной дисциплины и четырёх ограничений, исключающих завышение итоговой оценки, а также систему цветовой индикации, переводящую количественный результат в приоритеты для управленческих решений.

Апробация методики на информационной системе действующей организации подтвердила её работоспособность и выявила устойчивую закономерность: направления, зависящие от регулярно повторяемых организационных процедур – управление рисками, тестирование резервного копирования, разделение ролей при ограниченном штате специалистов, – систематически демонстрируют более низкую зрелость по сравнению с направлениями, закрываемыми точечными техническими решениями. Этот вывод согласуется с общей логикой перехода российского регулирования от формального комплаенса к оценке результативности и указывает на то, что дальнейшее повышение защищённости организаций лежит не столько в области закупки новых технических средств, сколько в области выстраивания устойчивых, документированных и регулярно проверяемых процессов. Направлением дальнейших исследований представляется интеграция предложенной методики с результатами практических испытаний защищённости, что позволит снизить зависимость итоговой оценки от субъективности самооценки и приблизить её к требованиям показателя Пзи в его полном объёме.

Литература

1. Российская Федерация. Законы. О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам передачи и обработки персональных данных : Федеральный закон № 233-ФЗ. – Москва, 2025. – Текст : электронный. – URL: https://www.consultant.ru/ document/ cons_doc_LAW_418443/
2. Козырь Н. С. Методические подходы риск-менеджмента информационной безопасности // Научные труды КубГТУ (Электронный сетевой политематический журнал). – 2023. – № 4. – С. 99–109.
3. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений : Приказ ФСТЭК России от 11.04.2025 № 117.
4. Ермачков, Д. И. Разработка воспроизводимой методики оценки ПЗИ для объектов ТЭК / Д. И. Ермачков, Д. И. Правиков // Кибернетика и информационная безопасность "КИБ-2025" : Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. Том 1. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 20-21. – EDN QUPSTU.
5. Лившиц И. И., Бакшеев А. С. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры // Вопросы кибербезопасности. – 2022. – № 6 (52). – С. 40–52. – DOI: 10.21681/2311-3456-2022-6-40-52.
6. National Institute of Standards and Technology. NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD : NIST, 2024. – 32 p.
7. CMMI Institute. CMMI Model V3.0: Improving Performance and Building Capability. – Pittsburgh, PA : CMMI Institute, 2023. – 210 p.
8. International Organization for Standardization. ISO/IEC 21827:2008. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM). – Geneva : ISO, 2008. – 130 p. [in English]
9. International Organization for Standardization. ISO/IEC 33001:2015 (ISO/IEC 15504). Information technology – Process assessment – Concepts and terminology. – Geneva : ISO, 2015.

10. ISACA. COBIT 2019 Framework: Governance and Management Objectives. – Schaumburg, IL : ISACA, 2019. – 236 p.
11. Велигодский С.С., Милославская Н.Г. Методика оценки уровня зрелости центров управления сетевой безопасностью. Доклады Томского Государственного Университета Систем Управления и Радиоэлектроники. 2023, т. 26, № 2, с. 31–41. DOI: http://dx.doi.org/10.21293/1818-0442-2023-26-2-31-41. – EDN: KFNVTO.
12. Толстой А.И. Системотехника обеспечения безопасности объектов и информационной сфере. Вопросы кибербезопасности. 2024, № 5(63), с. 47–57. DOI: http://dx.doi.org/10.21681/2311-3456-2024-5-47-57. – EDN: NLAGBE.
13. Проект Методики оценки уровня зрелости деятельности в области технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. – Текст: электронный // ФСТЭК России – URL: https://fstec.ru/dokumenty/vse-dokumenty/proekty/proekt-metodicheskogo-dokumenta-5.
14. Методика оценки уровня зрелости кибербезопасности фокусных компаний Группы ПАО Сбербанк. – Текст : электронный // ПАО Сбербанк : официальный сайт. – URL: https://www.sberbank.ru/ru/person/ kibrary/ experts/metodika-ocenki-urovnya-zrelosti-kiberbezopasnosti-fokusnykh-kompanij-gruppy-pao-sberbank
15. Гаврилов А. В., Сизов В. А., Ярошенко Е. В. Методика оценки рисков информационной безопасности предприятия с использованием CASE-технологий // Открытое образование. – 2021. – Т. 25, № 5. – С. 41–49.
16. Конаков А. М., Лившиц И. И. The use of dynamic modeling methods to create an adaptive training system for specialists... // Вестник Дагестанского государственного технического университета. Технические науки. – 2024. – Т. 51, № 2. – С. 83–90. – DOI: 10.21822/2073-6185-2024-51-2-83-90

Practical aspects of modeling information security maturity assessment processes

Stepanenko D.S., Krylova S.L., Ivliev S.N.
National Research Mordovia State University named after N.P. Ogarev

JEL classification: C10, C50, C60, C61, C80, C87, C90

A methodology is proposed for assessing the maturity of an organization's information security processes, based on an adapted Capability Maturity Model Integration and the risk-based approach established by Order No. 117 of the FSTEC of Russia dated April 11, 2025. The methodology combines a five-level maturity scale, eight critical indicator groups, a maturity coefficient formula incorporating a process discipline weighting factor, and a color-coded indication of the deviation between the achieved and target levels. Testing of the methodology on the information system of an operating organization revealed uneven process maturity: areas requiring constant procedural discipline systematically lag behind those addressed by isolated technical measures. The results obtained can be used by organizations of various profiles to prioritize information security investments and prepare for the transition to the regulator's risk-based requirements.

Keywords: information security, maturity assessment, CMMI model, risk-based approach, maturity coefficient, target maturity level, SSE-CMM, NIST CSF, security criteria, information risk management.

References

1. Russian Federation. Laws. On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Transfer and Processing of Personal Data: Federal Law No. 233-FZ. – Moscow, 2025. – Text: electronic. – URL: https://www.consultant.ru/document/cons_doc_LAW_418443/
2. Kozyr N. S. Methodological approaches to information security risk management // Scientific Works of KubSTU (Electronic Network Multidisciplinary Journal). – 2023. – No. 4. – P. 99–109.
3. On Approval of Requirements for the Protection of Information Contained in State Information Systems and Other Information Systems of State Bodies, State Unitary Enterprises, and State Institutions: Order of the FSTEC of Russia No. 117 dated April 11, 2025.
4. Ermachkov D. I., Pravikov D. I. Development of a reproducible methodology for assessing information protection measures for fuel and energy complex facilities // Cybernetics and Information Security "KIB-2025": Proceedings of the Third All-Russian Scientific and Technical Conference. In 2 volumes, Moscow, December 3–4, 2025. Volume 1. – Moscow: National Research Nuclear University MEPhI, 2025. – P. 20–21. – EDN QUPSTU.
5. Livshits I. I., Baksheev A. S. Study of methods for monitoring the level of information security at critical information infrastructure facilities // Cybersecurity Issues. – 2022. – No. 6 (52). – P. 40–52. – DOI: 10.21681/2311-3456-2022-6-40-52.
6. National Institute of Standards and Technology. NIST Cybersecurity Framework (CSF) 2.0. – Gaithersburg, MD : NIST, 2024. – 32 p.
7. CMMI Institute. CMMI Model V3.0: Improving Performance and Building Capability. – Pittsburgh, PA : CMMI Institute, 2023. – 210 p.
8. International Organization for Standardization. ISO/IEC 21827:2008. Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM). – Geneva : ISO, 2008. – 130 p. [in English]
9. International Organization for Standardization. ISO/IEC 33001:2015 (ISO/IEC 15504). Information technology – Process assessment – Concepts and terminology. – Geneva : ISO, 2015.
10. ISACA. COBIT 2019 Framework: Governance and Management Objectives. – Schaumburg, IL : ISACA, 2019. – 236 p.
11. Veligodsky S.S., Miloslavskaya N.G. Methodology for assessing the maturity level of network security management centers. Proceedings of Tomsk State University of Control Systems and Radioelectronics. 2023, vol. 26, no. 2, pp. 31–41. DOI: http://dx.doi.org/10.21293/1818-0442-2023-26-2-31-41. – EDN: KFNVTO.
12. Tolstoy A.I. Systems engineering for ensuring the security of facilities and the information sphere. Cybersecurity Issues. 2024, no. 5(63), p. 47–57. DOI: http://dx.doi.org/10.21681/2311-3456-2024-5-47-57. – EDN: NLAGBE.
13. Draft Methodology for Assessing the Maturity Level of Technical Information Protection Activities in Information Systems and Security Assurance for Significant Critical Information Infrastructure Objects of the Russian Federation. – Text: electronic // FSTEC of Russia – URL: https://fstec.ru/dokumenty/vse-dokumenty/proekty/proekt-metodicheskogo-dokumenta-5.
14. Methodology for Assessing the Cybersecurity Maturity Level of Focus Companies within the Sberbank Group (PJSC Sberbank). – Text: electronic // PJSC Sberbank: official website. – URL: https://www.sberbank.ru/ru/person/ki-brary/experts/metodika-ocenki-urovnya-zrelosti-kiberbezopasnosti-fokusnykh-kompanij-gruppy-pao-sberbank
15. Gavrilov A. V., Sizov V. A., Yaroshenko E. V. Methodology for Assessing Enterprise Information Security Risks Using CASE Technologies // Open Education. – 2021. – Vol. 25, No. 5. – P. 41–49.
16. Konakov A. M., Livshits I. I. The use of dynamic modeling methods to create an adaptive training system for specialists... // Herald of Dagestan State Technical University. Technical Sciences. – 2024. – Vol. 51, No. 2. – P. 83–90. – DOI: 10.21822/2073-6185-2024-51-2-83-90