УДК 330.131.7 : 004.75
DOI: 10.26456/2219-1453/2025.3.166–174

Управление информационной безопасностью организации на основе использования современных моделей менеджмента

Н.С. Васильев

ФГБОУ ВО «Тверской государственной университет», г. Тверь

Целью исследования является анализ современных моделей оценки уровня зрелости процессов в организациях в области информационной безопасности для выработки предложений по совершенствованию контроля и минимизации рисков при имплементации основных доменов современных стандартов. Исследование системы стандартизации процессов управления информационной безопасностью показало, что целесообразно проводить комплексную оценку зрелости процессов с применением различных моделей. Научная новизна заключается в организационно–экономическом обосновании применения совокупности моделей, подходящих под оценку каждого домена на основе выбора наиболее эффективного метода проведения аудита и определения уровня зрелости процессов в организации в сфере информационной безопасности. На основе анализа моделей оценки зрелости процессов в области информационной безопасности на основе стандарта ГОСТ Р ИСО/МЭК 27001−2021 разработана авторская концепция в данной сфере, применение которой позволит организациям оперативно определять текущий уровень зрелости процессов, совершенствовать контроль и корректировку работ, минимизировать операционные риски. Реализации представленных предложений позволит снизить информационные и операционные риски организации в сфере информационной безопасности.

Ключевые слова: *менеджмент информационной безопасности, управление рисками, оценка зрелости процессов, системы менеджмента информационной безопасности, ITIL, COBIT.*

Введение. В современных условиях информационные технологии играют ключевую роль в обеспечении всех аспектов государственной и частной жизни. Пандемия COVID-19 стала катализатором перехода на информационно-коммуникационные платформы не только в сфере общения между людьми, но и во многих других областях, таких как производство и образование [2, с. 116]. Следует подчеркнуть, что автоматизация процессов в различных сферах делает их более прозрачными, оперативными, эффективными, надёжными, точными и предсказуемыми, что, в свою очередь, способствует улучшению благосостояния государства и граждан. Однако, наряду с этим возникают проблемы с обеспечением информационной безопасности этих систем, платформ и прочих активов организаций [3, с. 206]. Вызовы эффективной имплементации и организации работы системы обеспечения информационной безопасности на различных

уровнях управления в отраслях и сферах деятельности формируют ряд задач для современных систем менеджмента.

Методология исследования. В настоящее время существует множество методологий, применяемых для разработки и совершенствования систем обеспечения информационной безопасности (СОИБ). Однако, несмотря на их разнообразие и широкую популярность, они не всегда позволяют сделать обоснованный выбор конкретных мер и средств защиты информации. Эмпирические исследования, направленные на оценку эффективности систем и стандартов в данной сфере, ограничены, поскольку они начали проводиться сравнительно недавно. В случае некорректного использования методов и алгоритмов управления процессами СОИБ у руководства компаний может возникнуть ложное ощущение безопасности, что приведёт к недооценке реальных рисков и снижению уровня защищённости. Кроме того, следование стандартизированной методологии организации информационной безопасности потребует дополнительных финансовых расходов. Так Н.Н. Беденко относительно применения научно-методических подходов управления в сфере здравоохранения отмечает, что целесообразность тех или иных мер может оцениваться показателем продуктивности, определяемой как соотношение полученного результата от использования какого-либо вида ресурса к расходам [4, с. 100]. Многие российские и зарубежные ученые занимались исследованиями в области аудита системы менеджмента информационной безопасности, проведения оценки, анализа и измерений ее процессов: А.С. Бакшеев, Г.С. Джура, А.В. Дорофеев, Н.К. Козырь И.И. Лившиц, А.С. Марков, К.С. Чернышев и другие.

К.С. Чернышев поднимает проблему отсутствия единой системы, которая бы сопоставляла измерения уровней зрелости информационной безопасности организации с мировыми практиками и требованиями законодательства [5, с. 24]. А.В. Дорофеев и А.С. Марков в своей работе о концепциях менеджмента ИБ, выделяя основные элементы контроля работы СМИБ и акцентируя, что постоянное улучшение СМИБ является одним из ключевых принципов. [6, с. 69]. Г.С. Джура в своей работе по совершенствованию методического подхода к диагностике системы обеспечения информационной безопасности отмечает, что диагностика СОИБ представляет собой многоуровневый комплексный подход, зависящий от множества факторов. [2, с. 120]. Н.С. Козырь отмечает, что методическое обеспечение фокусируется на различных аспектах информационной безопасности. [7, с. 99]. M.M. Naumann, F. Pitz акцентируют внимание на отсутствии целостного подхода к процессу оценки уровней зрелости информационной безопасности организации и вытекающей из этого возможности измерение процесса, как непрерывного совершенствования [13, с. 496]. И.И. Лившиц отмечает необходимость выполнять измерений СМИБ с применением стандартов 2700-х серий [8, 9].

Таким образом, под информационной безопасностью принято понимать состояние защищённости ресурсов информационной системы в условиях потенциальных угроз в информационном пространстве. В

настоящее время в связи с текущей геополитической обстановкой количество угроз подобного характера кратно возросло. В связи с этим процесс организации информационной безопасности в государственных и коммерческих организациях нуждается в управлении [12, с. 64]. В ходе исследования применялись методы анализа, синтеза, контент–анализа и другие.

Результаты исследования

Система менеджмента информационной безопасности в организации строится на основе концепции бизнес-риска и служит основой для разработки, внедрения, контроля, анализа, поддержки и улучшения системы информационной безопасности. СМИБ охватывает различные аспекты, такие как структура системы, политика, планирование, обязанности, методы, процедуры, процессы и ресурсы организации.

В Российской Федерации базой для создания системы управления информационной безопасностью является стандарт ГОСТ Р ИСО/МЭК 27001—2021 «Системы менеджмента информационной безопасности» [1]. Стандарт предоставляет возможность установить границы системы управления информационной безопасностью, что позволяет внедрить СМИБ в рамках определённых критически важных бизнес-процессов, а при необходимости — распространить её действие на другие процессы. На практике для большинства выявленных рисков принимается решение об их минимизации путем внедрения контролей. ГОСТ Р ИСО/МЭК 27001—2021 содержит Приложение А, в котором приведены 114 контролей, распределенных по следующим 14-ти доменам

Фактически по каждому разделу стандарта должна проводится своя оценка зрелости процессов с целью определения областей риска и направлений оптимизации. Аудит рисков может проводиться с помощью моделей оценки зрелости процессов. Специалисты по безопасности сосредотачиваются исключительно на размере организации, не принимая во внимание уровень ее организационного и технологического развития. Однако важно понимать, что каждая организация уникальна, и подходы к управлению рисками должны адаптироваться к конкретным условиям. Например, субъекты малого бизнеса могут не иметь ресурсов для проведения глубокого анализа рисков, как это делается в крупных корпорациях. В таких случаях стоит рассмотреть возможность использования более простых и быстрых методов оценки, которые позволят выявить основные угрозы без значительных затрат времени и ресурсов. Ответ на этот вопрос может быть предоставлен моделью зрелости, основанной на оценке уровня зрелости процессов безопасности. Данная модель помогает организациям определить, на каком этапе развития находятся их процессы и какие шаги необходимо предпринять для их улучшения. Если уровень зрелости организации невысок, то детальная проработка процедуры оценки рисков может оказаться нецелесообразной. В рамках исследования проведено сопоставление моделей оценки зрелости процессов с ГОСТ Р ИСО/МЭК 27001—2021 (табл. 1.).

Таблица 1

Рекомендации по применению моделей оценки зрелости процессов с применением стандарта ГОСТ Р ИСО/МЭК 27001—2021 «Системы менеджмента информационной безопасности»

Домены	Модель оценки зрелости процессов	Обоснование применения модели	Использование модели при проведении оценки зрелости процессов
Политики информационной безопасности	O-ISM3	Модель является узкоспециализированной и применимой к сфере ИБ. Она включает метрики и критерии оценки процессов как основы разработки и внедрения эффективной политики ИБ	Модель требует, чтобы процессы СУИБ были задокументированы, измерялись и управлялись, используя различные метрики для оценки процессов, включая показатели эффективности.
Организация деятельности по информационной безопасности	CMMI	CMMI является универсальной моделью оценки уровня зрелости процессов. В данном домене организации ИБ, реализуется структурированный подход к оценке процессов управления.	Возможна оценка взаимодействия подразделения информационной безопасности с органами власти, подрядчиками, а также обеспечение внутреннего взаимодействия между отделами, включая зоны ответственности и безопасности дистанционной работы сотрудников.
Безопасность, связанная с персоналом	SSE-CMM	SSE-CMM фокусируется на аспектах управления человеческими ресурсами в контексте безопасности, включая обучение и осведомленность сотрудников о рисках .	SSE-CMM позволяет провести комплексную оценку безопасности, связанную с персоналом, позволяя оценить эффективность подбора квалифицированного персонала, обучение внутри организации и обязанности сотрудников.
Менеджмент активов	PCM	PCM позволяет оценить возможности управления активами в контексте информационной безопасности, что важно для эффективного менеджмента активов.	При оценке PCM на начальном этапе организации необходимо провести инвентаризацию всех своих информационных активов и провести самооценку по уровням. В соответствии с уровнями PCM требуется документирование процессов управления активами включая оценку рисков.
Управление доступом	NIST Cybersecurity Framework	Фреймворк предоставляет рекомендации по управлению доступом и может быть адаптирован для оценки зрелости процессов контроля доступа.	Фреймворк позволяет оценить более строгие меры аутентификации или улучшенные системы мониторинга.
Криптография	ISO/IEC 21827	Стандарт, описывающий наиболее полные рекомендации по внедрению криптографических мер.	Стандарт позволяет определить уровень зрелости процесса, используя метрики при оценке процедур управления ключами, количественных методов при оценке рисков, а также процесса выбора и внедрения криптографических средств.
Физическая безопасность и защита от	BPMM	BPMM помогает оценить уровень зрелости процессов физической безопасности и	Оценка уровня зрелости может проводиться по организации зон безопасности,

Домены	Модель оценки зрелости процессов	Обоснование применения модели	Использование модели при проведении оценки зрелости процессов
воздействия окружающей среды		защиты активов от внешних угроз.	предотвращению несанкционированного физического доступа и предотвращению потерь.
Безопасность при эксплуатации	ITIL	ITIL охватывает процессы управления ИТ, такие как управление инцидентами, проблемами, изменениями и другими аспектами, которые могут включать безопасность.	С помощью ITIL в данном домене возможна оценка средств резервного копирования, защиты от потери данных и оценка обеспечения безопасности эксплуатации средств обработки информации.
Безопасность системы связи	CCSMM	CCSMM ориентирована на безопасность коммуникаций и может быть использована для оценки зрелости процессов защиты информации при передаче.	Возможна оценка обеспечения безопасности в сетях организации, поддержания безопасности информации при обмене внутри организации и другими субъектами.
Приобретение, разработка и поддержка систем	CMMI	CMMI является универсальной моделью оценки уровня зрелости процессов, в контексте ИБ позволяет предоставить структурированный подход к оценке процессов управления.	CMMI позволяет провести оценку процессов, относящихся к разработке и поддержке систем, включая управление требованиями и тестирование. Прогресс отслеживается с помощью периодических оценок, таких как SCAMPI.
Взаимоотношения с поставщиками	COBIT	COBIT предлагает лучшие практики для управления ИТ-процессами и взаимодействием с поставщиками, что позволяет оценить зрелость процессов управления операциями с внешними партнерами.	Модель требует, чтобы проводилась оценка защиты активов организации, к которым имеют доступ подрядчики, поддержание согласованного уровня ИБ с подрядчиком.
Менеджмент инцидентов информационной безопасности	ITIL	ITIL предоставляет структурированный подход к управлению инцидентами, что позволяет эффективно реагировать на инциденты ИБ и улучшать процессы их обработки.	Оценка управления инцидентами информационной безопасности, анализ инцидентов, оценка реагирования линий блока ИБ в организации, оценка обязанностей и процедур реагирования.
Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации	ISO 22301	В рамках планирования непрерывности бизнеса, позволяет учитывать меры по защите информации, включая разработку стратегий обеспечения доступности и целостности данных во время инцидентов.	Стандарт позволяет сопоставить контроли в данном домене и более детально провести оценку обеспечения доступности средств обработки информации, реализации и проверке непрерывности работы инфраструктуры.
Соответствие	O-ISM3	Модель помогает обеспечить соответствие нормативным требованиям в области ИБ и управлять юридическими аспектами.	Модель позволяет определить уровень зрелости процессов соответствия политик ИБ актуальным регламентам, реализация политик.

Источник: составлено автором на основе [1, 5, 10, 11].

Таким образом, анализ моделей оценки зрелости процессов в области информационной безопасности на основе стандарта ГОСТ Р ИСО/МЭК 27001—2021 позволяет выделить наиболее перспективные из них к использованию в современных социально–экономических условиях (табл. 2).

Таблица 2

Концепция выбора моделей оценки зрелости процессов в области информационной безопасности на основе стандарта ГОСТ Р ИСО/МЭК 27001—2021 «Системы менеджмента информационной безопасности»

Модель	Область применения	Ожидаемый результат	Показатели оценки
ITIL	Менеджмент инцидентов ИБ и эксплуатации средств обработки данных	Определение вектора совершенствования в управлении инцидентами и корректировка	Время реакции на инциденты. Количество не выявленных инцидентов. Процент инцидентов, расследованных до конца.
O-ISM3	Процессы, связанные с организацией политик ИБ и проверки соответствий	Определение текущего уровня зрелости процессов в создании политик ИБ	Частота пересмотра и обновления политик. Процент сотрудников, ознакомленных с политиками ИБ. Уровень соблюдения политик ИБ.
CMMI	Процессы, связанные с организацией деятельности по ИБ, разработке и поддержанию систем	Определение текущего уровня зрелости процессов в организации деятельности по ИБ	Отклонение в планах и затратах на ИБ. Процент мер ИБ, заложенных при проектировании и разработке системы.
CCSMM	Процессы, связанные с безопасностью систем связи	Определение текущего уровня зрелости процессов связанных с безопасностью систем связи	Своевременность обновлений и патчей. Качество обслуживания.
SSE-CMM	Безопасность, связанная с персоналом	Определение вектора совершенствования работы с персоналом	Процент сотрудников, прошедших обучение по ИБ.Частота проведения тренингов. Уровень знаний сотрудников по ИБ.
PCM	Менеджмент активов	Определение текущего уровня зрелости процессов при управлении активами	Процент активов с актуальными патчами.
BPMM	Процессы, связанные с обеспечением безопасности от воздействия окружающей среды	Определение вектора совершенствования безопасности от воздействия окружающей среды	Количество инцидентов, связанных с физической безопасностью. Частота проверок систем физической безопасности.
ISO22301	Аспекты ИБ, связанные с непрерывностью процессов;	Определение вектора совершенствования аспектов непрерывности процессов	Наличие планов восстановления после сбоев. Уровень потерь данных.
COBIT	Взаимоотношения с поставщиками	Определение текущего уровня зрелости процессов взаимодействия с поставщиками	Количество инцидентов безопасности, связанных с поставщиком. Процент успешно решенных проблем в установленный срок. Количество выявленных уязвимостей у поставщиков в срок.

Модель	Область применения	Ожидаемый результат	Показатели оценки
ISO/IEC21827	Процессы, связанные с криптографией	Определение вектора совершенствования криптографических процессов	Криптографическая стойкость. Процент успешных атак.
NISTCybersecurityFramework	Процессы, связанные с управлением доступом	Определение текущего уровня зрелости процессов, связанных с управлением доступом	Процент учетных записей с избыточными правами. Время реакции на запросы предоставления/отзыва доступа. Количество инцидентов, связанных с несанкционированным доступом.

Источник: составлено автором на основе [10, 11].

Следование выше представленным рекомендациям выбора моделей оценки зрелости процессов в области информационной безопасности позволит обеспечить эффективность всей системы менеджмента в организации, а также создать организационно–экономические основы формирования специальной системы оценки результативности протекания процессов в данной сфере.

Заключение. На основе анализа моделей оценки зрелости процессов в области информационной безопасности на основе стандарта ГОСТ Р ИСО/МЭК 27001—2021 разработана авторская концепция в данной сфере, применение которой позволит организация оперативно определять текущий уровень зрелости процессов, совершенствовать контроль и корректировку работ, минимизировать операционные риски. В рамках решения проблемы эффективного управления оценочными процедурами в области зрелости процессов по обеспечению информационной безопасности организации предложена авторская концепция на основе сопоставления разделов стандарта и моделей оценки уровня зрелости процессов, что должно позволить устранить потенциальные риски и оптимизировать организацию деятельности в данной сфере. Вектор будущих исследований будет заключаться в выборе и обосновании методологических подходов к оценке результатов данной работы в целях разработки системы показателей, адекватно отражающих полученные результаты.

Список литературы

1. ГОСТ Р ИСО/МЭК 27000–2021 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология: [Электр, ресурс] URL: https: // pqm-online.com/assets/files/lib/std/gost-iso-mek-27000-2021.pdf (дата обращения: 28.11.24).
2. Джура Г.С. Совершенствование методического подхода к комплексной диагностике системы обеспечения информационной безопасности органа государственной власти // Новое в экономической кибернетике. 2020. №3-4. С. 115–124.
3. Гундорова М.А., Калинина А.В. Цифровизация: возможности и угрозы //Вестник Тверского государственного университета. Серия: Экономика и управление. 2024. № 3(67). С. 202–210.

4. Погорельцева О.А., Хатькова С.Е., Беденко Н.Н. Эффективность в здравоохранении: актуализация императивов и научно-методических подходов // Вестник Тверского государственного университета. Серия: Экономика и управление. 2024. № 1 (65). С. 99–115
5. Чернышев К.С. Комбинированный метод оценки зрелости системы менеджмента информационной безопасности с применением модели CMMI // Молодой ученый. 2023. № 36 (483). С. 24–28.
6. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. №1 (2). С. 67–73.
7. Козырь Н.С. Методические подходы риск-менеджмента информационной безопасности // Научные труды КУБГТУ. 2023. №4. С. 99–109.
8. Лившиц И.И. Обзор национальных и международных стандартов для категорирования объектов критической информационной инфраструктуры // Научно-технический вестник информационных технологий, механики и оптики. 2023. №3 (23). С. 519–529.
9. 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.
10. Менеджмент информационной безопасности: принципы, задачи и перспективы развития – [Электр, ресурс]. URL: https://safe.cnews.ru/articles/2022-0808_menedzhment_informatsionnoj_-bezopasnosti (дата обращения: 23.11.24)
11. Обзор уровня зрелости процессов ИБ: о трендах и методология – [Электр, ресурс], URL: https:// www.itsec.ru/articles/obzor-urovnya-zrelosti-protsessov-ib-o-trendakh-i-metodologiyakh?ysclid=m5bd4cipvc913753614 (дата обращения: 12.12.24)
12. Чегринцова С.В., Торская А.Н. Особенности управления организациями в современных условиях // Вестник Тверского государственного университета. Серия: Экономика и управление. 2023. №3 (64). С. 64–72.
13. Michael Matthias NAUMANN, Fabian PITZ, Georg Sven LAMPE, StelianMircea OLARU Approach of Determining Process Maturity in Information Security Management Systems // Proceedings of the 7th International Conference on Economics and Social Sciences (2024), ISSN 2704-6524. PP. 221–230.

Об авторе:

ВАСИЛЬЕВ Никита Сергеевич – аспирант кафедры экономики предприятия и менеджмента Института экономики и управления, ФГБОУ ВО «Тверской государственный университет», 170000, г. Тверь, ул. Желябова, д. 33**,** e-mail: mr.nikitausersan@gmail.com, SPIN-код: 7115-7342

Сведения о научном руководителе:

БЕДЕНКО Надежда Николаевна – доктор экономических наук, доцент, заведующий кафедрой экономики предприятия и менеджмента Института экономики и управления ФГБОУ ВО «Тверской государственный университет» (170000, г. Тверь, ул. Желябова, д. 33), e-mail: bednad@mail.ru, ORCID: 0000-0002-2808-1303, SPIN-код: 7848-3916.

Information security management of an organization based on the use of modern management models

N.S. Vasiliev

FGBOU VO “Tver State University”, Tver

The purpose of the study is to analyze modern models for assessing the level of maturity of information security processes in organizations in order to develop proposals for improving control and minimizing risks in the implementation of the main principles of modern standards. The study of the system of standardization of information security management processes has shown that it is advisable to conduct a comprehensive assessment of the maturity of processes using various models. The scientific novelty lies in the organizational and economic justification of the application of a set of models suitable for the assessment of each domain based on the choice of the most effective audit method and determining the level of maturity of the organization's processes in the field of information security. Based on the analysis of models for assessing the maturity of processes in the field of information security based on the GOST R ISO/IEC 27001-2021 standard, an author's concept in this area has been developed, the application of which will allow organizations to quickly determine the current level of process maturity, improve control and work adjustments, and minimize operational risks. The implementation of the presented proposals will reduce the information and operational risks of the organization in the field of information security.

Keywords: *information security management, risk management, process maturity assessment, information security management systems, ITIL, COBIT.*

About the author:

VASIL"EV Nikita Sergeevich – postgraduate student of the Department of Business Economics and Management of the Institute of Economics and Management, FGBOU VO “Tver State University”, 170000, Tver, Zhelyabova str., 33, e-mail: mr.nikitausersan@gmail.com, SPIN code: 7115-7342.

Information about the scientific supervisor:

BEDENKO Nadezhda Nikolaevna– Doctor of Economics, Associate Professor, Head of the Department of Enterprise Economics and Management, Institute of Economics and Management, FGBOU VO “Tver State University” (170,000, Tver, Zhelyabova str., 33), e-mail: bednad@mail.ru, ORCID: 0000-0002-2808-1303, SPIN code: 7848-3916.

Статья поступила в редакцию 12.10.2025 г.
Статья подписана в печать 15.10.2025 г.