ДЕНЕЖНЫЕ КРИТЕРИИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ПОДХОДА ОЦЕНКИ АКТИВОВ

Козырь Н. С.[1], Макарян А. С.[2], Оганесян Л. Л.[3]

DOI: 10.21681/2311-3456-2024-3-51-60

Цель исследования: *разработка критериев принятия риска информационной безопасности для подхода, основанного на оценке активов (ISO/IEC 27005).*

Методы исследования: *сделан анализ документов с участием ФСТЭК России, исследованы критерии принятия риска информационной безопасности (ИБ), определенных в стандарте ISO/IEC 27005 с учетом требований ГОСТ Р ИСО/МЭК 27001. На основе Международного стандарта аудита 320 даны рекомендации расчета уровня существенности ИБ, что должно стать основой для разработки критериев риска ИБ.*

Полученные результаты: *Критерии принятия риска для всех хозяйствующих субъектов должны базироваться на принципе существенности, которая составляет: 1% от совокупных активов; 1% от выручки или суммарных расходов (бюджет на год); 5% от прибыли (для коммерческих организаций). Показатель существенности может быть рассчитан для любой организации, включая бюджетные организации, где имеется показатель стоимости активов или сводный бюджет на год. Полученные выводы позволяют получить оценочную шкалу принятия рисков ИБ в денежном эквиваленте.*

Научная новизна: *исследование предлагает интеграцию экономических аспектов в процесс оценки критериев риска информационной безопасности, что позволяет организациям принимать обоснованные решения о приемлемости рисков, обосновывать бюджет ИБ, разрабатывать технико-экономическое обоснование проектов ИБ. Денежные критерии риска ИБ позволят реализовать подход ISO/IEC 27005 на основе активов.*

Вклад: *Козырь Н. С. – общая концепция исследования, структурирование, описание результатов, выводы; Макарян А. С. – систематизация нормативно-правовой документации в области рисков ИБ (ISO/IEC 27005, Методические документы и Приказы ФСТЭК); Оганесян Л. Л. – экономические аспекты риска ИБ (ГОСТ Р ИСО/МЭК 27001, МСА 320).*

Ключевые слова: *критерии риска ИБ, уровень существенности ИБ, экономика защиты информации, экономика риска ИБ, система менеджмента информационной безопасности, риск-менеджмент информационной безопасности, информационная безопасность, оценка риска ИБ, риски информационной безопасности.*

MONETARY INFORMATION SECURITY RISK CRITERIA BASED ON THE ASSET VALUATION APPROACH

Kozyr N. S.[4], Makaryan A. S.[5], Oganesyan L. L.[6]

The purpose: *to develop criteria for information security risk acceptance for an asset-based approach (ISO/IEC 27005).*

Research methods: *an analysis of documents with the participation of the FSTEC of Russia was made, the criteria for information security risk acceptance (IS) defined in the ISO/IEC 27005 standard were*

1 Козырь Наталья Сергеевна, кандидат экономических наук, доцент кафедры кибербезопасности и защиты информации, ФГБОУ ВО «Кубанский государственный технологический университет» (КубГТУ), г. Краснодар, Россия. E-mail: n_k_@mail.ru, ORCID 0000-0002-8323-0957.

2 Макарян Александр Самвелович, кандидат технических наук, доцент, заведующий кафедрой кибербезопасности и защиты информации, ФГБОУ ВО «Кубанский государственный технологический университет» (КубГТУ), г. Краснодар, Россия. E-mail: msanya@yandex.ru, ORCID 0000-0002-1801-6137.

3 Оганесян Левон Левонович, кандидат экономических наук, доцент, доцент кафедры кибербезопасности и защиты информации, ФГБОУ ВО «Кубанский государственный технологический университет» (КубГТУ), г. Краснодар, Россия. E-mail: oganesyan_levon@mail.ru, ORCID 0009-0004-5170-4515.

4 Natalia S. Kozyr, Ph.D. in Economics, Associate Professor of the Department of Cybersecurity and Information Protection, Kuban State Technological University (KubSTU), Krasnodar, Russia. E-mail: n_k_@mail.ru

5 Alexander S. Makaryan, Ph.D. in Engineering sciences, Associate Professor, Head of the Department of Cybersecurity and Information Protection, Kuban State Technological University (KubSTU), Krasnodar, Russia. E mail: msanya@yandex.ru

6 Levon L. Oganesyan, Ph.D. in Economics, Associate Professor of the Department of Cybersecurity and Information Protection, Kuban State Technological University (KubSTU), Krasnodar, Russia. E-mail: oganesyan_levon@mail.ru

studied, taking into account the requirements of GOST R ISO/IEC 27001. Based on the International Auditing Standard 320, recommendations are given for calculating the level of materiality of information security, which should become the basis for the development of information security risk criteria.

The results: *The criteria for risk acceptance for all business entities should be based on the principle of materiality, which is: 1% of total assets; 1% of revenue or total expenses (budget for the year); 5% of profit (for commercial organizations). The materiality indicator can be calculated for any organization, including budget organizations, where there is an asset value indicator or a consolidated budget for the year. The obtained conclusions allow us to obtain an estimated scale of information security risk acceptance in monetary terms.*

The novelty of the research: *the study suggests the integration of economic aspects into the process of assessing information security risk criteria, which allows organizations to make informed decisions about the acceptability of risks, justify the budget of information security, and develop a feasibility study of information security projects. The monetary risk criteria of the IB will allow the implementation of the ISO/IEC 27005 asset-based approach.*

Contribution: *Kozyr N. S. – the general concept of the study, structuring, description of the results, conclusions. Makaryan A. S. – systematization of regulatory and legal documentation in the field of information security risks (ISO/IEC 27005, Methodological documents and Orders of the Federal State Technical Committee); Oganesyan L. L. – economic aspects of information security risk (GOST R ISO/IEC 27001, ISA 320).*

Keywords: *information security risk criteria, information security materiality level, information security economics, information security risk economics, information security management system, information security risk management, information security, information security risk assessment, information security risks.*

Введение

Исследование восполняет пробел в части методического обоснования к разработке критериев риска на основе подхода оценки активов, что является актуальной задачей для обеспечения информационной безопасности (ИБ) организаций. В России обеспечение ИБ сфокусировано на выполнении требований законодательства и соответствующих приказов регуляторов, в основном это Федеральная служба по техническому и экспортному контролю (ФСТЭК), и исполнение всех приказов сводится к модели угроз с выбором соответствующих средств защиты информации. Вместе с этим, в стандарте ГОСТ Р 59503-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации» обозначен подход по внедрению экономической модели как ключевого элемента процесса принятия решений в соответствии с комплексом стандартов ИСО/МЭК 27000 (ГОСТ Р 59503-2021 идентичен ISO/IEC TR 27016).

В России сохраняется проблема в части определения «границ» безопасности информационной системы на уровне национальных стандартов ГОСТ Р и регламента в сфере информационной безопасности[7], а значимость экономических аспектов информационной безопасности недооценивается специалистами в сфере защиты информации [1]. Напротив, современные тенденции в области системы менеджмента информационной безопасности характеризуются обновлением существующих, и разработкой новых стандартов ИСО/МЭК 27xxx, охватывающих актуальные сферы технологического развития глобального мира с акцентом на денежной стоимости риска и оценке активов.

Так, в зарубежных публикациях приводятся данные об обеспечении ИБ на основе комплексного управления системой риск-менеджмента ISO/IEC 27xxx [2], что в целом позволяет повысить уровень организационного развития хозяйствующего субъекта [3]. В трудах российских авторов сделано обзор зарубежных методик риск-менеджмента [4] и возможность их применения в российской практике обеспечения ИБ [5]. При этом отсутствие возможности денежной оценки рисков – распространенная проблема, в том числе, для зарубежных методик риск-менеджмента ИБ (COBIT for Risk, CRAMM, FRAP, OCTAVE), в работах ученых [6, 7].

В России анализ рисков рассматривается в контексте разработки модели угроз [8], с соответствующим анализом программного обеспечения [9]. В работе ученых (С. А. Никулин, С. С. Никулин) приведен математический аппарат определения риска, который основывается на принципах вероятности угроз и ущерба, без критериев содержательного наполнения (ГОСТ Р ИСО/МЭК 27005-2010), а негативные события обозначены буквенными параметрами

7 Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. № 2(4). С. 42–48.

без количественного расчета[8]. Также есть научные публикации, посвященные решению прикладных задач комплексного управления рисками (Н. И. Касперская [10], М. М. Путято и А. С. Макарян [11]).

Говоря о прикладных решениях в части критериев оценки безопасности информационных технологий, также следует отразить проблему с методическим обеспечением, которое характеризуется эволюционным отставанием от зарубежных аналогов. Так, в национальных стандартах России имеется три части ГОСТ Р 15408 (Критерии оценки безопасности информационных технологий), при этом за рубежом применяется пять частей ISO/IEC 15408, которые прошли два этапа эволюции. Действующие стандарты ГОСТ Р 15408 для применения нуждаются в гармонизации с ГОСТ Р ИСО/МЭК 27005[9]. В настоящее время нет универсальной методики, которая решила бы задачи мониторинга, анализа, оценки и предотвращения рисков и угроз системы защиты информации [12]. Основной пробел в методическом обеспечении оценки рисков ИБ является денежная оценка критериев, которая позволит сформировать систему риск-менеджмента с учетом ресурсных возможностей организации. В этой связи представленное исследование посвящено экономике критериев риска ИБ и определению существенности в денежном эквиваленте, что позволит реализовать подход оценки риска на основе активов.

Методология исследования

Методология исследования «Денежные критерии риска информационной безопасности на основе подхода оценки активов» предопределена следующей логикой: обеспечение ИБ для хозяйствующих субъектов преимущественно базируется на требованиях регулятора ФСТЭК, где исполнением приказов является составление модели угроз и выбор соответствующих средств защиты информации; ФСТЭК принимает активное участие в составе Технического комитета по стандартизации ТК 362 «Защита информации» в разработке национальных стандартов, и проект ГОСТ Р ИСО/МЭК 27005:2022 размещен на официальном сайте (в документе говорится о критериях риска, основанных на подходе оценки активов); для формирования методической основы определения критериев риска необходимо провести мониторинг действующих документов в этой области, включая ГОСТ Р ИСО/МЭК 27001:2021.

Таким образом, в работе рассмотрена методика оценки угроз безопасности информации ФСТЭК России на предмет содержания экономических аспектов риска, сделан анализ существующих критериев оценки информационной безопасности. Особое внимание уделено национальному стандарту ГОСТ Р ИСО/МЭК 27001-2021 в части раздела оценки рисков. Основой для рекомендаций послужило исследование денежного аспекта критериев принятия рисков в ИСО/МЭК 27005. В результате были сформированы пороговые значения критериев риска информационной безопасности в денежном эквиваленте на основе международного стандарта аудита 320.

Используемые сокращения в публикации:

СМИБ система менеджмента информационной безопасности;

МСА Международный стандарт аудита;

ОКУД Общероссийский классификатор управленческой документации.

Методика оценки угроз безопасности информации ФСТЭК России: экономические аспекты риска

В этом разделе представлен детальный анализ «Методики оценки угроз безопасности информации» ФСТЭК России на предмет содержания слова «риск» (в документе упоминание «риск» встречается

Раздел методики угроз ИБ	Содержание компонента риска
2.3. Исходными данными для оценки угроз безопасности информации являются:	ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором
2.7 Для оценки угроз безопасности информации рекомендуется привлекать специалистов, обладающих следующими знаниями и умениями:	а) основ оценки рисков, а также основных рисков от нарушения функционирования систем и сетей и нарушения безопасности обрабатываемой информации (далее – информационные риски)
	ж) оценивать информационные риски
3.2. Исходными данными для определения негативных последствий от реализации угроз безопасности информации являются:	д) результаты оценки рисков (ущерба), проведенной обладателем информации или оператором
3.3. На основе анализа исходных данных определяются событие или группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к:	в) возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора

Рис. 1. Содержание компонентов риска в методике угроз ИБ в разделе 2 (порядок оценки угроз) и разделе 3 (определение негативных последствий)

8 Никулин С. А., Никулин С. С. Методика количественной оценки величины риска обеспечения информационной безопасности автоматизированных систем управления и связи // Вестник Воронежского института ФСИН России. 2016. № 1. С. 44–51.

9 Барабанов А. В., Марков А. С., Цирлов В. Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5(13). С. 2–10.

34 раза)[10]. Следует отметить, что в ряде случаев вместе с риском встречается рекомендация по оценке финансового компонента возможных последствий от нежелательных инцидентов информационной безопасности. Все ссылки в этом разделе относятся к структуре анализируемого документа.

В методическом документе «Методика оценки угроз безопасности информации» ФСТЭК России говорится о необходимости оценки риска и его последствий (рис. 1).

Однако следует отметить и то, что в ситуации отсутствия результатов оценки рисков (ущерба) методический документ предлагает вариант определения возможных негативных последствий от реализации угроз ИБ на основе экспертной оценки специалистов (раздел 3.4). Вместе с этим, результаты оценки ущерба (рисков) относятся к категории исходных данных для определения возможных актуальных нарушителей (раздел 5.1.2). В описании актуальных нарушителей (раздел 5.1.4) говорится о том, что к таковым относятся все, чьи действия «могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба)». На рис. 2 представлены компоненты риска, которые содержатся в приложении 1, 2 и 3 методического документа ФСТЭК России.

Примеры сопоставления возможных целей реализации угроз безопасности информации с видами ущерба (риска) и возможными негативными последствиями о реализации угроз представлены в приложении 5 Методики угроз ФСТЭК России. В Приложении 7 сделано соотнесение целей видам риска (ущерба) по видам нарушителей и возможных негативных последствий на объекты воздействия.

Несмотря на то, что риски – неотъемлемый компонент методического документа по оценке угроз, ФСТЭК России не дает конкретных инструкций по их оценке. Вместе с этим, о важности анализа риска говорится в руководящем документе по разработке профилей защиты и заданий по безопасности[11]: «если анализ рисков не выполнен должным образом, объект оценки будет не в состоянии обеспечить

10 Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021) [электронный ресурс]. Режим доступа: https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf. (дата обращения: 01.02.2024)

11 Руководство по разработке профилей защиты и заданий по безопасности. Руководящий документ (Гостехкомиссия России, 2003 год). [электронный ресурс]. Режим доступа: https://fstec.ru/files/576/--2003-482/1040/--2003-.pdf. (дата обращения: 01.02.2024).

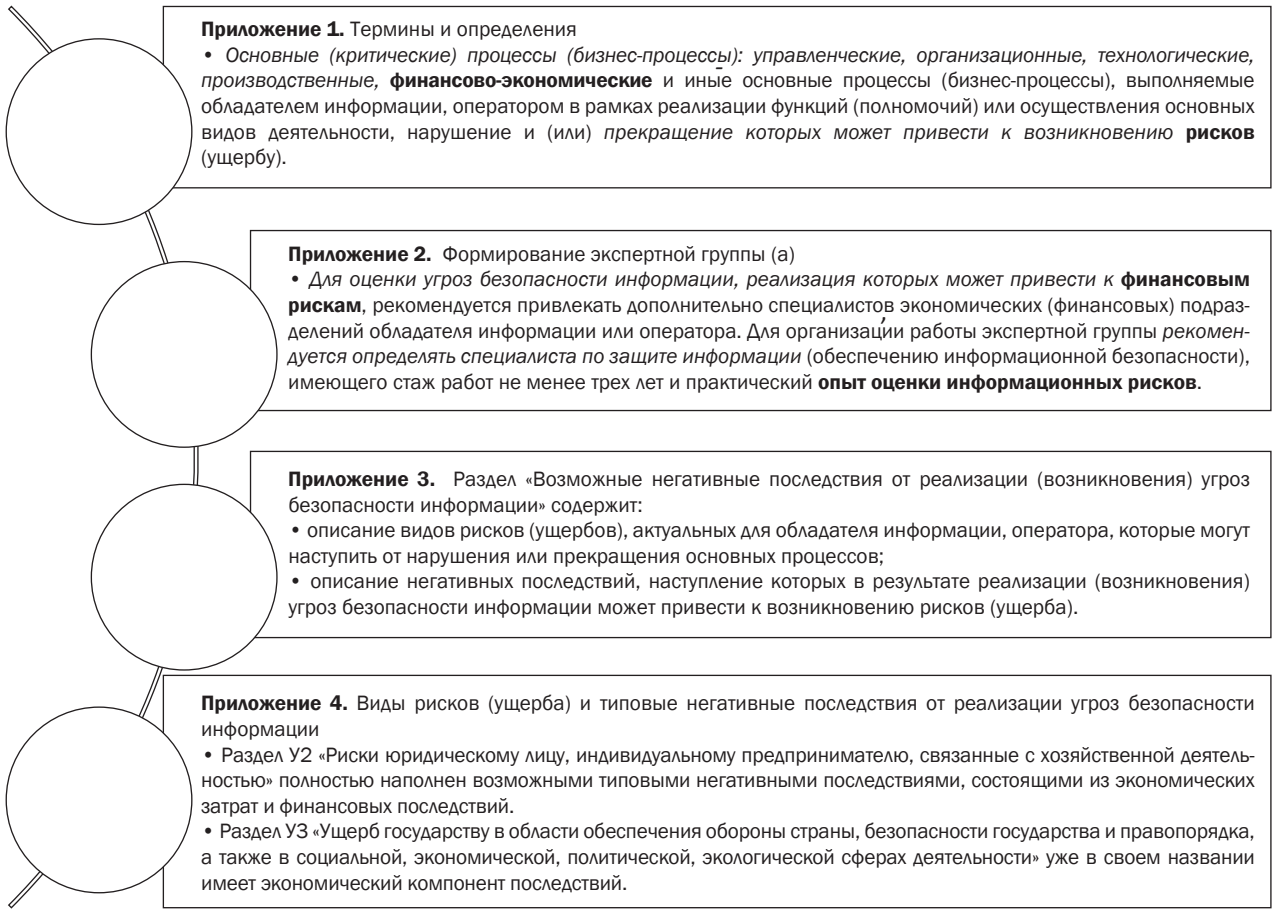

Рис. 2. Обзор приложений методики угроз ФСТЭК России на предмет описания категории риска

адекватную защиту, в результате чего активы организации могут остаться подверженными соответствующему риску». Наряду с этим отмечается, что рекомендации по организации процесса идентификации угроз активам – это один из самых трудоемких этапов анализа риска организации, и не включены в руководство по разработке профилей защиты и заданий по безопасности, в связи с чем, в документе изложены только общие принципы идентификации угроз.

За рубежом аспекты риска информационной безопасности являются предметом национальной системы стандартизации (NIST – США, BS – Англия), где активно переведены (или адоптированы) международные стандарты ISO/IEC, включая серию 27xxx «Менеджмент риска информационной безопасности». Несмотря на развитую систему стандартизации РФ, тема рисков имеет локальный характер, что осложняет развитие методического обеспечения информационной безопасности для хозяйствующих субъектов.

Критерии оценки безопасности ИТ и менеджмент риска ИБ в национальных стандартах ГОСТ Р

Важно отметить, что ФСТЭК России – ключевая организация в регулировании ИБ с активным участием в разработке национальных стандартов РФ (в составе деятельности технического комитета по стандартизации «Защита информации», ТК 362)[12].

Полный перечень активности ФСТЭК России в составе ТК по разработке национальных стандартов ГОСТ Р представлен на официальном сайте (раздел «стандарты), на рис. 3 представлены документы, которые содержат критерии оценки информационной безопасности (ГОСТ Р 15408) и категорию «риск» (ГОСТ Р 27005). Несмотря на то, что стандарты ГОСТ Р 15408 не соотносятся напрямую с риском информационной безопасности, но в национальной системе стандартизации нет других, которые бы содержали «критерии» оценки безопасности, что подтверждает общую проблему для разработки критериев риска – отсутствие методической документации.

Иллюстрация показывает, что в России применяются национальные стандарты ГОСТ Р 15408, которые отстают по составу и эволюционному развитию от международных ISO/IEC 15408, что в свою очередь отражается на методическом обеспечении оценки рисков информационной безопасности. Эволюционное отставание национальной системы стандартизации было отмечено в работе, посвященной анализу новых пакетов нормативных методических документов ФСТЭК России[13].

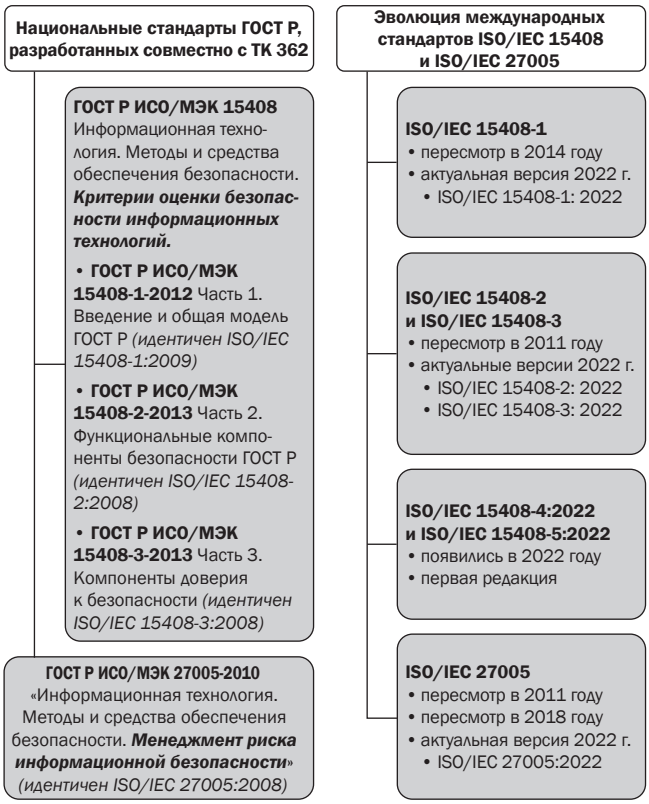

Рис. 3. Сравнительный анализ национальных стандартов ГОСТ Р и актуальных редакций международных стандартов ISO/IEC

Так, например, в международный стандарт ISO/IEC 15408-1:2009 в 2014 году были внесены правки, а в 2022 году принята новая версия стандарта[14].

Аналогичные эволюционные изменения коснулись второй и третьей части ISO/IEC 15408, в 2011 году были исправлены ошибки. В настоящее время действует международные стандарты 2022 года ISO/IEC 15408-2:2022[15] и ISO/IEC 15408-3:2022[16]. В 2022 году появилась четвертая и пятая части зарубежного стандарта ISO/IEC 15408, которые посвящены описанию методов и мероприятий оценки безопасности информационных технологий[17] и определению пакетов требований безопасности[18].

12 Марков А. С., Цирлов В. Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. 2017. № 1(22). С. 53–61. DOI 10.21681/2412-8163-2017-1-53-61.

13 Барабанов А. В., Марков А. С., Цирлов В. Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264–270.

14 ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1: Introduction and general model [электронный ресурс]. Режим доступа: https://www.iso.org/ru/standard/72891.html (дата обращения: 01.02.2024).

15 ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 2: Security functional components [электронный ресурс]. Режим доступа: https://www.iso.org/ru/standard/72892.htm (дата обращения: 01.02.2024).

16 ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 3: Security assurance components [электронный ресурс]. Режим доступа: https://www.iso.org/ru/standard/72906.html (дата обращения: 01.02.2024).

17 ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 4: Framework for the specification of evaluation methods and activities [электронный ресурс]. Режим доступа: https://www.iso.org/standard/72913.html (дата обращения: 01.02.2024).

18 ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 5: Pre-defined packages of security requirements [электронный ресурс]. Режим доступа: https://www.iso.org/ru/standard/72917.html (дата обращения: 01.02.2024).

Особого внимания заслуживает национальный стандарт ГОСТ Р ИСО/МЭК 27005-2010 (на основе ISO/IEC 27005:2008), который нуждается в пересмотре. Международный стандарт ISO/IEC 27005 за 15 лет трижды изменился, в 2011 и 2018 года пересмотрен, а в 2022 году принята новая редакция. Этот документ применим ко всем организациям, независимо от типа, размера или сектора. Действующая редакция ISO/IEC 27005:2022 направлена не только на выполнение требования стандарта ISO/IEC 27001 (действия по устранению рисков информационной безопасности), но и позволяет выполнять мероприятия по управлению рисками информационной безопасности (в частности, оценку рисков информационной безопасности и их обработку)[19].

Надо отметить, что осенью 2023 года на сайте ФСТЭК появился проект национального стандарта ГОСТ Р ИСО/МЭК 27005-2022 (идентичен ISO/IEC 27005:2022)[20]. В настоящее время не обозначены сроки рассмотрения и перспективы принятия проекта, тем не менее, далее в исследовании рассмотрен этот документ, на предмет выявления критериев риска информационной безопасности на основе подхода оценки активов. Учитывая, что стандарты 27xxx серии раскрывают те или иные аспекты ГОСТ Р ИСО/МЭК 27001, контекст риска необходимо определить место и роль риск-менеджмента в стандарте, на основе которого осуществляется сертификация в соответствии с ISO/IEC 27001:2022.

Национальный стандарт ГОСТ Р ИСО/МЭК 27001-2021: оценка рисков информационной безопасности

В настоящее время в РФ действующей редакцией является ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (национальный

19 ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks [электронный ресурс]. Режим доступа: https://www.iso.org/standard/80585.html (дата обращения: 01.02.2024).

20 Проект ГОСТ Р ИСО/МЭК 27005-2022 Информационная безопасность, кибербезопасность и защита частной жизни. Руководство по управлению рисками информационной безопасности. Требования и руководства [электронный ресурс]. Режим доступа: https://fstec.ru/files/1135/-------27005/2138/----27005----------.pdf (дата обращения: 01.02.2024).

Оценка рисков информационной безопасности (ГОСТ Р ИСО/МЭК 27001-2021, раздел 6.1.2.)		
Организация должна определить и внедрить процесс оценки рисков информационной безопасности, который позволяет:	6.1.2 a) ***устанавливать и поддерживать критерии рисков информационной безопасности,*** включая	*1)* ***критерии принятия рисков информационной безопасности;***
		2) ***критерии для проведения оценки рисков информационной безопасности;***
	6.1.2 b) обеспечивать уверенность в том, что повторные оценки рисков информационной безопасности дают непротиворечивые, достоверные и сопоставимые результаты;	
	6.1.2 c) идентифицировать риски информационной безопасности, т.е.:	1) применять процесс оценки рисков информационной безопасности для идентификации рисков, связанных с нарушением конфиденциальности, целостности и доступности информации в рамках области действия системы менеджмента информационной безопасности;
		2) идентифицировать владельцев рисков информационной безопасности;
	6.1.2 d) проводить анализ рисков информационной безопасности, т.е.:	1) оценивать потенциальные последствия, которые могут произойти в результате реализации рисков информационной безопасности, идентифицированных в соответствии с 6.1.2 c) 1);
		2) оценивать реальную вероятность реализации рисков информационной безопасности, идентифицированных в соответствии с 6.1.2 c) 1);
		3) определять уровни рисков информационной безопасности;
	6.1.2 e) ***оценивать риски информационной безопасности,*** т.е.:	*1)* ***сравнивать результаты анализа рисков информационной безопасности с критериями рисков,*** *установленными в соответствии с 6.1.2 a);*
		2) ***определять приоритетность обработки проанализированных рисков информационной безопасности.***

Рис. 4. Содержание раздела 6.1.2 «Оценка рисков информационной безопасности» ГОСТ Р ИСО/МЭК 27001-2021

стандарт идентичен ISO/IEC 27001:2013). Несмотря на то, что в 2022 году вышла новая версия международного стандарта ISO/IEC 27001:2022, раздел «Оценка рисков информационной безопасности» (6.1.2) не содержит существенных изменений в сравнении с 2013 годом, в этой связи на иллюстрации показаны данные ГОСТ Р ИСО/МЭК 27001-2021 (рис. 4).

Так, структура оценки рисков ИБ начинается с необходимости установления критериев, которые позволяют оценить риски и в дальнейшем – использовать для принятия (раскрытие раздела анализа рисков содержится в ИСО/МЭК 27005). Завершается раздел 6.1.2 тоже процедурой анализа рисков на основе установленных критериев. Таким образом, слабым звеном в риск-менеджменте являются критерии, которые организации должны установить самостоятельно, и использовать в своей деятельности.

Денежный аспект критериев принятия рисков информационной безопасности в ИСО/МЭК 27005

Для анализа критериев принятия риска в представленном исследовании рассмотрен проект национального стандарта ГОСТ Р ИСО/МЭК 27005-2022, т.к. содержит новый подход, основанный на активах. Свод денежных и финансовых критериев риска информационной безопасности представлен в табл. 1.

Наряду с этим, в критериях последствий (раздел 6.4.3.2) предлагается использование логарифмической шкалы денежных последствий с комбинированием оценки уровня последствий в других областях (без финансовых аспектов). Также в документе говорится о том, что критерии принятия риска ИБ должны быть установлены, в том числе, с учетом финансовых ограничений (раздел 6.4.2).

В разделе «Мониторинг и анализ факторов, влияющих на риски» (раздел 10.5.2) акцентируется внимание на том, что риски не являются статичными, в связи с чем требуется постоянный пересмотр всех оценочных факторов, которые в том числе включают в себя появление новых активов с корректировкой их стоимости.

В приложении А описаны критерии риска информационной безопасности, где финансовые потери в денежных единицах и условная частота возникновения рискового события – неотъемлемые компоненты принятого порогового значения, выше которого риски считаются неприемлемыми (А.1).

Подход на основе активов подразумевает обязательную привязку оценки рисков с первичными бизнес активами и вспомогательными активами. В этой связи важно определить взаимосвязи между активами и понять их ценность, т.к. неправильная оценка стоимости активов приведет к неправильной оценке последствий, связанных с риском (А 2.2). Таким образом, критерии риска должны быть связаны со стоимостью активов, а пороговые значения для принятия риска необходимо устанавливать в денежном эквиваленте.

Пороговые значения критериев риска информационной безопасности в денежном эквиваленте

Денежный эквивалент пороговых значений риска информационной безопасности необходимо установить в соответствии со стандартом, который применяется в практике аудита финансовой отчетности РФ – МСА 320 «Существенность при планировании и проведении аудита» (МСА 320)[21].

По своей сути, подходы для определения уровня существенности в аудите и пороговые денежные критерии риска ИБ имеют одинаковую экономическую природу. Для определения критериев ИБ необходимо за основу взять один из трех показателей, которые присущи всем хозяйствующим субъектам независимо от формы собственности и вида экономической деятельности:

- 1% от совокупных активов организации;
- 1% от выручки или 1% от годового бюджета плановых расходов (для государственных и некоммерческих организаций);
- 3% от прибыли до налогообложения (или 5% от чистой прибыли).

Выбранный показатель является основой для расчета уровня существенности ИБ, который имеет денежный эквивалент для любого хозяйствующего субъекта. В табл. 2 представлены рекомендации по выбору целевого показателя для расчета критериев риска ИБ. Рекомендуется выбирать тот показатель, который даст максимальное значение.

Уровень существенности ИБ – это предельная величина совокупных рисков в денежной стоимости. Для формирования критериев риска в организации должен быть принят локальный нормативный акт с определением уровня значимости риска в привязке к денежной стоимости уровня существенности ИБ. Организации должны опираться на показатель «уровень существенности ИБ» при принятии решений о том, какие риски информационной безопасности им следует принять и какие меры по управлению рисками следует реализовать.

Использование конкретных значений критериев существенности позволяет организациям более четко определить и оценить риски информационной безопасности, что способствует более эффективному управлению ими и снижению потенциальных убытков.

21 Международный стандарт аудита 320 «Существенность при планировании и проведении аудита» [электронный ресурс]. Режим доступа: https://minfin.gov.ru/ru/document/?id_4=116584 (дата обращения 01.02.2024).

Таблица 1

Денежно-финансовые содержательные компоненты в документе «Проект национального стандарта ГОСТ Р ИСО/МЭК 27005-2022»

п/п	Раздел и название 27005-2022	Связь с 27001:2022	Денежный и финансовый компоненты содержания рисков ИБ в проекте стандарта ГОСТ Р ИСО/МЭК 27005:2022
1	6.4 Установление и поддержание критериев риска информационной безопасности 6.4.3 Критерии для оценки риска информационной безопасности		
1.1	6.4.3.2 Критерии последствий	6.1.2 a) 2)	При определении критериев последствий следует особенно учитывать возможность (опасность): f) потери деловой и ***финансовой ценности***.
			Максимальная сумма, которую организация готова списать в течение финансового года, и ***минимальная сумма*** за тот же период, которая вынудила бы ее к ликвидации, могут создать реалистичные верхние и нижние пределы шкалы критериев последствий организации, которые представлены в ***денежном выражении***.
1.2	6.4.3.4 Критерии для определения уровня риска	6.1.2 a) 2)	Критерии уровня риска могут быть качественными (например, очень высокий, высокий, средний, низкий) или количественными (например, выраженными в терминах ожидаемой ***величины денежных потерь***, гибели людей или доли рынка за определенный период времени).
			Риски могут быть количественно определены как ***ожидаемый годовой убыток***, т. е. ***средняя денежная стоимость последствий*** за год, принятых в течение следующего года.
2	7.3 Анализ рисков информационной безопасности		
2.1	7.3.1 Общие положения	6.1.2 d) 1) 6.1.2 d) 2)	Методы анализа рисков, учитывающие последствия и их вероятность, могут быть обоснованы значениями показателей: a) качественными, которые используют качественную шкалу квалификационных признаков (например, высокий, средний, низкий); b) количественными, которые используют количественную шкалу с числовыми значениями (например, ***денежная стоимость***, частота или вероятность возникновения); c) полуколичественными, которые используют совокупность качественных и количественных шкал с присвоенными значениями.
2.2	7.3.4 Определение уровней риска	6.1.2 d) 3)	Уровень риска определяется как комбинация оцененной вероятности и оцененных последствий для соответствующих сценариев риска. Альтернативные расчеты могут включать ***стоимость актива***, а также их вероятность и оценку последствий.
2.3	7.4.1 Сравнение результатов анализа рисков с критериями риска	6.1.2 e) 1)	Уровни риска могут быть согласованы на основе консенсуса между владельцами рисков, деловыми и техническими специалистами. Важно, чтобы владельцы рисков хорошо понимали ***последствия материализации рисков***, за которые они несут персональную ответственность
3	9 Реализация		
3.1	9.1 Процесс оценки риска информационной безопасности	6.1.2 a)	Если существует годовой ***бюджетный цикл***, то могут потребоваться ***запросы на финансирование*** в определенные периоды бюджетного года.
			Следует заранее запланировать оценку риска: a) своевременно подавать предложения по обработке рисков и заявки на ***финансирование***; b) заранее провести переоценку рисков в соответствии с предполагаемыми ***бюджетными ассигнованиями***.
4	10 Применение взаимозависимых процессов СМИБ		
4.1	10.7 Корректирующие действия	н/д	План обработки рисков должен быть пересмотрен с учетом: выявленных трудностей при внедрении средств контроля (например, технические или ***финансовые проблемы***, несоответствия внутренним или внешним факторам, таким как соображения конфиденциальности).
4.2	10.8 Постоянное совершенствование	н/д	Организация должна регулярно проверять критерии, используемые для измерения риска. Деятельность по мониторингу и обзору должна охватывать (но не ограничиваться): правовой и экологической сферой; сферой конкуренции; подход к оценке риска; ***стоимость активов*** и их категории; критерии последствий; критерии вероятности; критерии оценивания риска; критерии принятия риска; общую ***стоимость владения***; необходимые ресурсы.

Таблица 2

Показатели для расчета уровня существенности риска информационной безопасности

п/п	Показатель	Применимость для хозяйствующих субъектов	Пояснение по расчету критерия
1	1% от совокупных активов	Крупный корпоративный бизнес с широко развитой сетью структурных подразделений	*Для коммерческих организаций:* Документ «Бухгалтерский баланс (ОКУД 0710001)», рассчитать 1% от показателя «БАЛАНС» (код строки 1600 или 1700, т.к. значения равны)
2	1% от выручки или 1% от годового бюджета плана расходов	Некоммерческие организации, Малый и средний бизнес, Индивидуальные предприниматели, Крупный корпоративный бизнес с высокой нормой прибыли (низкая доля расходов, например – управляющая компания). Ниже приведены примеры хозяйствующие субъекты	У каждой организации есть отчет о финансовых результатах, или утвержденный бюджет доходов, или перечень утвержденных расходов. Расчетный показатель не обязательно называется «выручка», по сути – для расчета берется объем финансового потока поступивших денежных средств за календарный год. Рассчитать 1% от показателя:
		– Коммерческие организации	«Выручка» (код строки 2110),: документ «Отчет о финансовых результатах (ОКУД 0710002)»
		– Некоммерческие организации (НКО)	«Текущие расходы – всего» (код строки 41), документ «Сведения о деятельности некоммерческой организации (ОКУД 0608032)»
		– Государственные внебюджетные фонды	«Доходы бюджета – всего» (код строки 010), или «Расходы бюджета - всего» (код строки 200) документ «Отчеты об исполнении бюджетов государственных внебюджетных фондов (ОКУД 0503317)»
		– Индивидуальные предприниматели и малый бизнес без обязательных форм отчетности	Объем поступивших денежных средств на официальный расчетный счет за календарный год
		– Другие организации	Поступившие денежные средства за календарный год с учетом источников финансирования дефицита бюджетов
3	5% от чистой прибыли	Коммерческие организации с низкой долей основных средств и высокой нормой прибыли	*Для коммерческих организаций:* Документ «Отчет о финансовых результатах (ОКУД 0710002)», рассчитать 5% от показателя «Чистая прибыль» (код строки 2400)

Заключение

Практическая значимость исследования состоит в том, что оно предоставляет организациям конкретные рекомендации по определению критериев принятия риска, основанных на принципе существенности и оценке активов. Полученные значения критериев существенности (1% от совокупных активов, 1% от выручки или суммарных расходов на год, 5% от чистой прибыли) могут быть использованы в практике для технико-экономического обоснования проектов и обоснования бюджета на информационную безопасность. Уровень существенности ИБ – это расчетная величина, имеет конкретное значение для каждой организации и выражена в денежной форме.

Так, например, компоненты риска из методики оценки угроз безопасности информации ФСТЭК России должны быть просуммированы, и итоговое значение необходимо сравнить с уровнем существенности ИБ в конкретной организации. Если сумма стоимости рисков ниже, чем принятый уровень существенности, значит, сохранится общее финансовое благополучие организации, и возможные инциденты не окажут влияние на непрерывность деятельности хозяйствующем субъекта.

Уровень существенности ИБ применим для реализации национальных стандартов ГОСТ Р 15408, т.к. предоставляет обоснование для сравнения критериев оценки информационной безопасности с финансовыми возможностями организации. Для практической реализации национального стандарта ГОСТ Р ИСО/МЭК 27001-2021 – расчет уровня существенности позволяет определить критерии принятия и проведения оценки рисков информационной безопасности.

Таким образом, решается методическое обеспечение реализации подхода, основанного на активах, и принять в РФ национальный стандарт, который будет идентичен актуальному документу ISO/IEC 27005:2022 «Информационная безопасность, кибербезопасность и защита частной жизни. Руководство по управлению рисками информационной безопасности. Требования и руководства».

Литература

1. *Козырь Н. С., Оганесян Л. Л. Экономические аспекты информационной безопасности. – Москва: ЮРАЙТ, 2023. 131 с.*
2. *Razikin Kh., Soewito B. Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework // Egyptian Informatics Journal. 2022. Vol. 23. No 3. P. 383-404. DOI 10.1016/j.eij.2022.03.001.*
3. *Schmid M., Pape S. Aggregating corporate information security maturity levels of different assets // IFIP Advances in Information and Communication Technology. 2020. Vol. 576. P. 376-392. DOI: 10.1007/978-3-030-42504-3_24.*
4. *Маслова М А. Научно-методические рекомендации по регулированию рисков нарушения информационной безопасности // Информация и безопасность. 2022. Т. 25. № 4. С. 513–520. DOI 10.36622/VSTU.2022.25.4.005.*
5. *Волкова Л. В., Макарова Д. В., Докучаев В. А. Использование метода CRAMM для оценки информационных рисков // Телекоммуникации и информационные технологии. 2021. Т. 8. № 1. С. 103–109.*
6. *Кортнев К. Методики управления рисками информационной безопасности и их оценки (часть 1, 14.05.2018) [электронный ресурс]. Режим доступа: https://safe-surf.ru/specialists/article/5193/587932/ (дата обращения 16.10.2023).*
7. *Кортнев К. Методики управления рисками информационной безопасности и их оценки (часть 2, 22.05.2018) [электронный ресурс]. Режим доступа: https://safe-surf.ru/specialists/article/5194/587935/?sphrase_id=45664 (дата обращения 16.10.2023).*
8. *Повышев А. А., Соколов А. Н., Мищенко Е. Ю. Универсальная классификация угроз безопасности информации и её применение для разработки модели угроз и оценки рисков // Вестник УрФО. Безопасность в информационной сфере. 2023. № 3(49). С. 68-80. DOI 10.14529/secur230307.*
9. *Баранова Е. К., Мурзакова А. А., Мурзакова Е. А. Сравнительный анализ программного обеспечения для анализа рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-10 // Информационные технологии и вычислительные системы. 2019. № 2. С. 75–83. DOI 10.14357/20718632190208.*
10. *Касперская Н. И. Анализ больших данных в ИБ предприятий. Перспективы развития // Защита информации. Инсайд. 2019. № 3(87). С. 34–43.*
11. *Путято М. М., Макарян А. С. Подходы к построению адаптивной системы защиты на основе корреляционного анализа статистических характеристик инцидентов информационной безопасности // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 2. С. 148–162.*
12. *Козырь Н. С. Методические подходы риск-менеджмента информационной безопасности // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2023. № 4. С. 99–109.*