ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-2-25-34 Обзорная статья /Review article

Проблемы управления рисками в сфере информационной безопасности

Г.М. Артамонов[1], В.В. Маслов[2], С.А. Резниченко[3]
[1,2,3]Финансовый университет при Правительстве Российской Федерации,
[1,2,3]125167, г. Москва, Ленинградский пр-т, 49/2, Россия,
[3]Национальный исследовательский ядерный университет «МИФИ»,
[3]115409, г. Москва, Каширское шоссе, 31, Россия,
[3]Российский государственный гуманитарный университет,
[3]125047, г. Москва, Миусская площадь, 6, Россия

Резюме. Цель. Целью исследования является сбор общедоступной информации для определения основных проблем, препятствующих эффективному управлению рисками информационной безопасности в сфере бизнеса. **Метод**. В качестве методов исследования используются: систематизация, описание и анализ. Необходимые данные формируются на основе информации, полученой по результатам анализа нормативно-правовой базы и исследований по заданной теме. **Результат.** Обоснована актуальность рассматриваемого вопроса; отмечается значительная эффективность риск-ориентированного подхода при управлении информационной безопасностью. Описаны ключевые этапы процесса менеджмента рисков информационной безопасности. Выявлены основные проблемы управления рисками информационной безопасности, характерные для отдельных этапов целостного процесса. **Вывод**. Материалы, представленные в работе, могут послужить базисом для дальнейших исследований по теме, а также для формирования рекомендаций по разрешению выявленных проблем.

Ключевые слова: информационная безопасность, ИБ бизнеса, СМИБ, риск-ориентированный подход, проблемы управления

Для цитирования: Г.М. Артамонов, В.В. Маслов, С.А. Резниченко. Проблемы управления рисками в сфере информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(2):25-34. DOI:10.21822/2073-6185-2023-50-2-25-34

Problems of risk management in the field of information security

G.M. Artamonov[1], V.V. Maslov[2], S.A. Reznichenko[3]
[1,2,3]Financial University under the Government of the Russian Federation,
[1,2,] 49 Leningradsky Prospekt, Moscow, 125993, Russia,
[3]National Research Nuclear University “MEPhI”
[3]31 Kashirskoe sh., 31, Moscow, 115409, Russia,
[3]Russian State University for the Humanities,
[3]Miusskaya Square, 6, Moscow, 125047, Russia

Abstract. Objective. The purpose of the study is to collect publicly available information to identify the main problems that hinder the effective management of information security risks in the business sector. **Method.** The following research methods are used: systematization, description and analysis. The necessary data are formed on the basis of information obtained from the analysis of the regulatory framework and research in the field. **Result.** In this paper, the relevance of the issue under consideration was substantiated; the significant effectiveness of the risk-based approach in information security management was noted. The key stages of the information security risk management process were described. Next, the main problems of information security risk management for all stages of the holistic process are identified. **Conclusion.** The conducted research is of an overview nature. The materials presented in the paper can serve as a basis for

further research on the topic, as well as for the formation of recommendations for resolving the identified problems.

Keywords: information security, business information security, ISMS, risk-based approach, management problems

For citation: G.M. Artamonov, V.V. Maslov, S.A. Reznichenko. Problems of risk management in the field of information security. Herald of Daghestan State Technical University. Technical Science. 2023; 50 (2): 25-34. DOI: 10.21822 /2073-6185-2023-50-2-25-34

Введение. Стремительное развитие информационных технологий привело к цифровизации подавляющего большинства аспектов жизни человека и росту ценности информации. Как следствие, повышается степень уязвимости личности, общества, бизнеса и государства информационной сфере. В противовес этому постепенно формируется и совершенствуется деятельность по обеспечению информационной безопасности (далее ИБ).

Как и любая другая целенаправленная и систематизированная работа, защита информации нуждается в управлении для того, чтобы быть рациональной, оперативной и плодотворной. Под управлением ИБ и синонимичными словосочетаниями далее в статье будет пониматься следующее: руководство деятельностью по обеспечению информационной безопасности (governance of information security);система, с помощью которой контролируется и управляется деятельность организации в области обеспечения информационной безопасности [1,стр. 5]. При проведении исследования упор был сделан на изучение управления ИБ в сфере бизнеса, вопросы, затрагивающие ИБ личности, государства и общества не рассматривались. Тем не менее, независимо от того, на защиту какого объекта направлена деятельность по защите информации, повышение ИБ не является самоцелью. Это связано с тем, что финансовые затраты на обеспечение безопасности часто могут быть не только неоправданными, но и вовсе неподъёмными. Особенно это актуально для малых и средних коммерческих организаций. Система ИБ - лишь механизм предотвращения ущерба. Ввиду вышесказанного, ключевым вопросом построения и управления такой системы становится: какой уровень защиты необходимо обеспечить для конкретной организации?

На сегодняшний день существует два основных подхода к решению этого вопроса [2. стр. 7].

1. Достижение определённого уровня ИБ. Как правило, желаемый уровень безопасности достигается путём реализации определённого набора требований (стандарты, руководящие документы) и внедрения защитных мер против всех основных видов угроз. Такой путь имеет целый ряд недостатков. В частности, он не только не позволяет, определить эффективный уровень защиты информационной системы, но и корректно оценить существующий с позиции потенциального ущерба, а также должным образом обосновать внедрение тех или иных защитных мер. Ключевым же недостатком является неэффективный расход ресурсов, как финансовых, так и человеческих.

2. Подход, связанный с оценкой и управлением рисками. Ключевым для этого подхода является принцип разумной достаточности. Ввиду того, что главной целью определено не достижение того или иного уровня защиты, а снижение рисков, появляется возможность приоритезации при распределении ресурсов. Как следствие, основное внимание уделяется устранению наиболее опасных для бизнеса уязвимостей. Более того, данный путь способствует согласованию целей высшего руководства компании по снижению рисков с работой департамента ИБ.

Представленные ниже схемы (рис. 1 - 2) наглядно демонстрируют принцип разумной достаточности, обеспечивающий большую эффективность второго подхода. Таким образом, применение риск-ориентированного подхода позволяет добиться значительного большего коэффициента полезного действия системы ИБ, нежели при первом варианте, путём соблюдения баланса между затратами на защитные меры и их эффектом, а также за счёт повышения эффективности взаимодействия специалистов ИБ с иными подразделениями организации и её руководством.

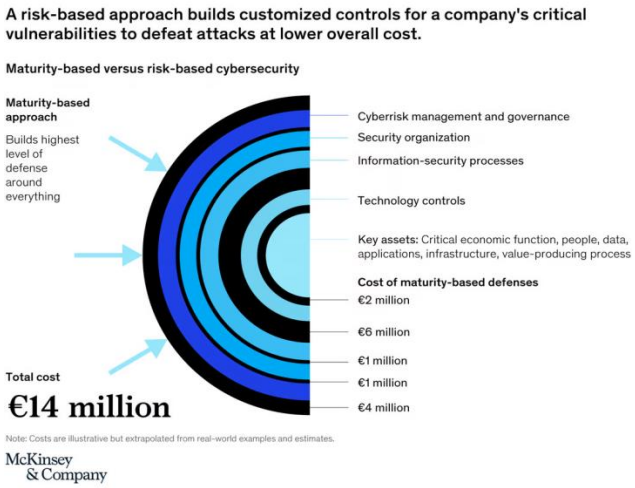

Рис. 1. Подход направленный на достижение определённого уровня ИБ [3]
Fig. 1. Maturity-based approach

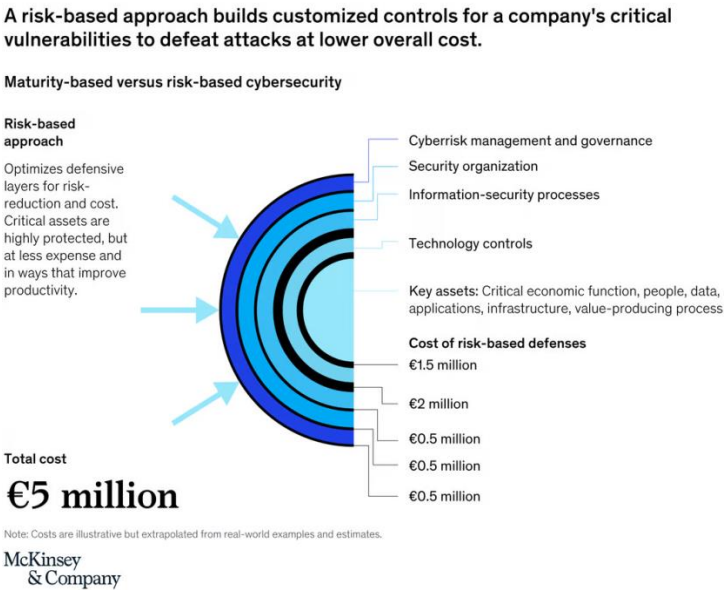

Рис. 2 Риск-ориентированный подход [3]
Fig. 2 Risk-based approach

Постановка задачи. С учётом всего вышесказанного, риск-ориентированный подход к руководству деятельностью по обеспечению ИБ представляется наиболее актуальным и разумным. Необходимость и даже обязательность реализации механизмов управления рисками в каждой СМИБ отмечается, не только в нормативных документах [1,5], но и специалистами [3, 6]. Однако при выборе такого пути существует свой перечень осложнений, препятствующих внедрению и применению необходимых для управления рисками механизмов.

Цель данного исследования заключается в определении основных проблем, препятствующих эффективному управлению рисками информационной безопасности в сфере бизнеса, посредством сбора и анализа общедоступной информации.

Методы исследования. Понимание процесса менеджмента рисками имеет ключевое значение при поиске проблем, осложняющих его реализацию. В целом, представление о данном процессе глобально совпадают и опираются на методологию Plan-Do-Check-Act (PDCA), также известную как цикл Деминга-Шухарта. В частности, подход PDCA принят в стандарте ISO 27001 [9]. Рис. 3 демонстрирует, как этапы процесса менеджмента риска соотносятся с циклом PDCA. Различные нормативно-правовые документы предлагают свой перечень этапов в процессе менеджмента рисков ИБ (рис.4).

Процесс СМИБ	Процесс менеджмента риска ИБ
Планирование	Установление контекста Оценка риска Планирование обработки риска Принятие риска
Осуществление	Реализация плана обработки риска
Проверка	Проведение непрерывного мониторинга и переоценки рисков
Действие	Поддержка и усовершенствование процесса менеджмента риска ИБ

Рис. 3. Соотношение СМИБ и процесса менеджмента риска информационной безопасности [5]

Fig. 3. The relationship between the information security management system and the information security risk management process

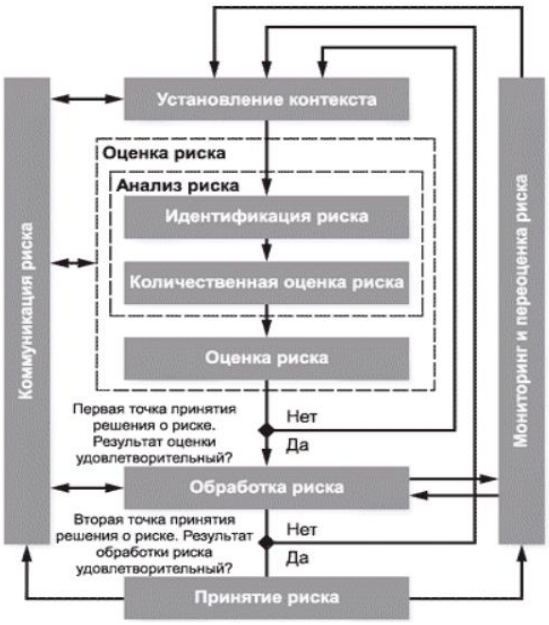

Рис. 4. Процесс менеджмента риска информационной безопасности [5]

Fig. 4. The process of information security risk management

Например, стандарт ISO/IEC 27005 выделяет следующие этапы:

1. Установление контекста. В рамках данного процесса изучаются все сведения компании, имеющие вес при выборе подхода к управлению рисками. На основе этих сведений вырабатываются критерии оценки рисков и возможного негативного влияния, критерии принятия рисков. Также важно учесть границы процесса управления рисками и необходимые для его осуществления ресурсы.

2. Оценка риска. Цель данного этапа - получить качественную или количественную оценку рисков и провести их приоритезацию с учётом их опасности. Этот этап включает подпроцессы: идентификация, анализ и оценивание рисков. При проведении идентификации рисков необходимо: составить перечень информационных активов, определить и классифицировать актуальные уязвимости и угрозы с учётом их источника, собрать информацию о текущем уровне ИБ и имеющихся средствах защиты информации, выявить возможные последствия реализации инцидентов.

В процессе анализа рисков выбирается используемая методология, оценивается перечень идентифицированных на предыдущем этапе угроз через потенциальные последствия от их реализации для бизнеса, а также вероятность их реализации, далее рискам присваиваются значения опасности. Наконец, на этапе оценивания рисков, посредством сравнения полученных уровней рисков с критериями, выработанными на этапе установления контекста, рискам присваивают приоритеты.

3. Разработка плана обработки рисков. Результатом данного этапа является сформированный план обработки перечня приоритизированных рисков, составленного в процессе оценки рисков. Должны быть выбраны меры защиты с учётом их стоимости, чётко определены временной интервал и приоритетность обработки рисков, а также определены остаточные риски. Существует несколько вариантов обработки рисков. Снижение рисков - изменение защитных мер, по итогам которого остаточный риск оценён как приемлемый. Сохранение риска - принятие решение не предпринимать действий по обработке риска, в связи с тем, что уровень его опасности соответствует критериям принятия риска. Предотвращение риска - решение отказаться от определенной деятельности или условия, вызывающего риск. Такой вариант выбирается, когда затраты компании на снижение слишком высоких рисков неоправданно превышают выгоду от деятельности, с которой связан риск. Передача риска - передача ответственности за менеджмент конкретного риска стороне, способной на более эффективную его обработку.

4. Принятие рисков. В ходе этого этапа принимается и формально регистрируется решение о принятии рисков и ответственности за это решение. Важно учесть, что уровень остаточных рисков может не соответствовать критериям принятия. В случае если пересмотреть критерии принятия не представляется возможным, может возникнуть необходимость принять риски им не соответствующие, с обязательным обоснованием решения.

5. Реализация плана обработки рисков. В рамках данного этапа претворяется в жизнь разработанный план обработки рисков. Вводятся в эксплуатацию средства защиты, ведется юридическая работа с партнерами, до руководства доводится информация о рисках и их обработке.

6. Непрерывный мониторинг и переоценка рисков. В связи с возможными изменениями активов организации, перечня угроз и уязвимостей, вероятности реализации инцидентов и их последствий, необходим непрерывный мониторинг. Он может быть обеспечен с привлечением внешних сервисов. Выявление изменений влечёт аз собой переоценку рисков и пересмотр применяемых методов их обработки.

7. Поддержка и совершенствование процесса управления рисками ИБ. Процесс управления рисками также нуждается в постоянном мониторинге и совершенствовании, чтобы оставаться эффективным. Ввиду этого, важно следить, чтобы критерии и методы измерения и обработки рисков оставались релевантными. На данном этапе уделяется внимание изменениям в контексте (правовом, конкуренции, окружающей среды), перечне активов и их стоимости, критериям оценки и принятия рисков, доступности необходимых ресурсов. Любые изменения обязательно должны быть согласованы с заинтересованными сторонами. В случае необходимости нужно менять или совершенствовать текущий подход, методологию и инструменты управления рисками ИБ. При необходимости мониторинг может иметь результатом модификацию процесса управления рисками.

В то же время, NIST SP 800-39 выделяет всего 4 этапа [7]:

1. Определение рисков.
2. Оценка рисков.
3. Реагирование на риск.
4. Мониторинг рисков.

Однако кардинальных различий с уже рассмотренными этапами ISO/IEC 27005 нет.

Многие специалисты также отдельно выделяют этапы менеджмента остаточных рисков, такой подход отображает рис. 5.

Помимо вышеописанных этапов, важно выделить процесс коммуникации риска, который фактически является сквозным и связан со всеми подпроцессами. Термин был введён в ISO/IEC Guide 73:2002 г, пересмотрен в ISO Guide 73:2009. Данному процессу уделяется особое внимание, как специалистами в сфере управления рисками, так и в нормативно-правовых документах [5,6,7]. Эффективный обмен информацией, касающейся менеджмента риска, играет ключевую роль в принятии решений. Этот процесс обеспечивает уверенность,

что заинтересованные лица и лица, отвечающие за менеджмент риска ИБ, понимают базис для принятия решений иотносительно тех или иных действий.

Рис. 5. Цикл процесса управления рисками [11]
Fig. 5. Risk management process cycle

Отдельно необходимо отметить важность таких аспектов, как организационная культура и доверие к контрагентам [7, с. 28-31].

Организационная культура — это ценности, убеждения, нормы, которые влияют на принятие решений со стороны высших руководителей и отдельных членов организации. Также культура отражает готовность организации внедрять новые технологии. Ввиду этого, культура организации напрямую влияет на деятельность по управлению рисками. Поскольку компания обычно не имеет прямого контроля над деятельностью своих партнеров, степень доверия к контрагентам и учёт присущей им организационной культуры также имеет большое значение.

Таким образом, учёт данных факторов - не менее важный процесс при управлении рисками. В каждом из рассмотренных подпроцессов менеджмента рисков ИБ существуют проблемы и сложности, которые без уделения им должного внимания, препятствуют повышению эффективности системы управления информационной безопасности.

Обсуждение результатов. Рассмотрим выявленные проблемы по порядку этапов, на которых они дают о себе знать.

Установление контекста.

1. Недостаток понимания. Может быть сложно полностью понять и охватить контекст организации, ее бизнес-процессы, цели, структуру и культуру, особенно в крупных организациях или в сложных международных средах.

2. Неполнота информации. Недостаточность или неактуальность информации о существующих угрозах, уязвимостях, ресурсах и правовых требованиях может затруднять правильную оценку рисков.

3. Различные точки зрения. У разных заинтересованных сторон могут быть разные взгляды на контекст и приоритеты, что может вызвать разногласия при определении рисков и принятии решений.

4. Ограниченные ресурсы. Недостаток финансовых, человеческих и технических ресурсов может затруднять сбор и анализ информации, а также реализацию мер по управлению рисками.

5. Сложность изменений. Быстрые изменения в технологической среде и бизнес-процессах могут затруднять поддержание актуальности контекста и его соответствия текущим реалиям.

6. Недостаток экспертизы. Отсутствие квалифицированных специалистов в области управления рисками информационной безопасности может затруднить анализ и понимание контекста организации.

Оценка риска.

1. Недостаточность данных: Недостаток качественных данных о существующих угрозах, уязвимостях, воздействиях и вероятностях может затруднять точную оценку рисков.

2. Сложность квантификации: Определение количественных значений для факторов риска, таких как вероятность возникновения событий и потенциальный ущерб, может быть сложной задачей, особенно в отношении информационных систем.

3. Субъективность: Оценка рисков может зависеть от субъективных мнений и предположений экспертов, что может привести к неправильным или неоднозначным результатам.

4. Устаревание оценки: Оценка риска должна быть регулярно обновляема, поскольку угрозы и уязвимости могут меняться со временем. Однако, недостаток ресурсов или непостоянство оценочных процедур могут привести к устареванию оценки риска.

5. Неучет неизвестных рисков: Существуют потенциальные риски, которые еще не были идентифицированы или не были полностью поняты. Это может привести к непредсказуемым последствиям и неполной оценке рисков.

6. Ограниченные ресурсы: Оценка риска требует времени, экспертизы и ресурсов. Ограничения в этих областях могут привести к поверхностной или неполной оценке риска.

7. Недостаток участия заинтересованных сторон: Оценка риска может быть неполной, если не все заинтересованные стороны принимают в ней участие. Разнообразие мнений и взглядов важно для более полного понимания рисков.

Планы обработки риска.

1.Недостаток конкретных мер: Иногда может быть сложно определить конкретные меры для снижения рисков или не хватает информации об эффективности определенных мер.

2. Неправильная расстановка приоритетов: Некорректное определение и установление приоритетов в обработке рисков может привести к неэффективному использованию ресурсов и недостаточной защите от наиболее значимых угроз.

3. Ошибки при выборе контрмер: Неправильный выбор контрмер или их неправильная реализация может привести к недостаточной защите или созданию новых уязвимостей.

4. Ограниченные ресурсы: Ограничения в финансовых, человеческих и технических ресурсах могут ограничить возможности организации в реализации необходимых мер по обработке рисков.

5. Сложность изменений: Внедрение новых мер по обработке рисков может требовать изменений в бизнес-процессах, системах и культуре организации, что может быть сложно и сопряжено с сопротивлением со стороны персонала.

6. Недостаток экспертизы: Отсутствие квалифицированных специалистов в области информационной безопасности может затруднять выбор и реализацию эффективных мер по обработке рисков.

7. Сложность координации: Обработка рисков может требовать сотрудничества и координации различных отделов и заинтересованных сторон в организации, что может быть вызовом.

Принятие рисков.

1. Неправильная оценка рисков: Недостаточная или неправильная оценка рисков может привести к принятию неподходящих решений. Это может быть вызвано недостаточностью данных, субъективностью оценки или ошибками в оценочных методиках.

2. Неправильное понимание последствий: Неполное или неправильное понимание потенциальных последствий и воздействий рисков может привести к недооценке их серьезности или пренебрежению.

3. Недостаточное участие заинтересованных сторон: Если не все заинтересованные стороны принимают участие в принятии рисков, это может привести к упущению значимых мнений и информации, а также создать недоверие и сопротивление.

4. Несоответствие политикам и стандартам: Принятие рисков, которые не соответ-

ствуют установленным политикам и стандартам информационной безопасности, может нарушать правила и регуляторные требования, а также повышать уровень риска для организации.

5. Недостаток информации: Недостаток достоверной информации о рисках и соответствующих мероприятиях может затруднить принятие обоснованных решений.

6. Влияние эмоций и субъективности: Принятие рисков может подвергаться влиянию эмоций, предубеждений и субъективных оценок, что может исказить рациональное принятие решений.

7. Недостаточная готовность к управлению последствиями: Неправильное или недостаточное планирование и подготовка к управлению последствиями рисков может привести к нежелательным и неожиданным последствиям.

Реализация плана.

1. Недостаток ресурсов: Ограниченность финансовых, человеческих или технических ресурсов может затруднить успешную реализацию мер по обработке рисков.

2. Неправильное планирование: Недостаточное или неправильное планирование реализации мер может привести к нереализуемым или неэффективным действиям по обработке рисков.

3. Недостаточная координация: Отсутствие эффективной координации между различными заинтересованными сторонами, отделами или командами может затруднить согласованное выполнение плана обработки рисков.

4. Сложность внедрения: Реализация некоторых мер по обработке рисков может быть сложной из-за изменений в процессах, технологиях или культуре организации.

5. Изменение контекста: Возможные изменения в контексте организации, включая технологические изменения или изменения в целях и приоритетах, могут потребовать пересмотра и адаптации плана обработки рисков.

6. Отсутствие мониторинга и реагирования: Недостаточное или отсутствие системы мониторинга, анализа и реагирования на изменения в рисках может привести к недооценке или игнорированию новых или возросших угроз и уязвимостей.

7. Недостаток участия и осведомленности персонала: Недостаточная осведомленность и участие персонала в реализации мер по обработке рисков может снизить эффективность этих мер и повысить риск нарушений безопасности.

Мониторинг и переоценка.

1. Неполная или неправильная информация: Недостаток достоверной и актуальной информации о новых угрозах, уязвимостях и воздействиях может привести к неправильной оценке рисков.

2. Неправильная методология: Использование неправильных или недостаточно эффективных методологий для мониторинга и переоценки рисков может привести к искаженным или неполным результатам.

3. Ограниченные ресурсы: Недостаток времени, бюджета или экспертов может затруднить регулярный и полноценный мониторинг и переоценку рисков.

4. Сложность квантификации: Определение количественных значений для рисков и их изменений может быть сложной задачей, особенно при оценке информационных систем.

5. Недостаток автоматизации: Отсутствие автоматизированных инструментов и систем для мониторинга и переоценки рисков может затруднить и замедлить процесс их выполнения.

6. Недостаточная осведомленность и участие заинтересованных сторон: Неполное вовлечение заинтересованных сторон и персонала в процессы мониторинга и переоценки рисков может привести к неполным или неактуальным данным.

7. Недостаточная реакция на изменения: Неэффективная или отсутствующая система реагирования на обнаруженные изменения в рисках может привести к непредсказуемым последствиям и ухудшению общей безопасности.

Поддержка и совершенствование.

1. Недостаток ресурсов: Ограниченность финансовых, человеческих или технических ресурсов может затруднить эффективную поддержку и совершенствование процесса управления рисками.

2. Недостаточное понимание: Недостаточное понимание принципов и методик управления рисками информационной безопасности может привести к неправильной поддержке и неверным улучшениям процесса.

3. Недостаточное вовлечение и понимание высшего руководства: Отсутствие активной поддержки и понимания со стороны высшего руководства может затруднить привлечение необходимых ресурсов и реализацию улучшений в процессе управления рисками.

4. Недостаточная коммуникация и сотрудничество: Недостаточное обмен информацией, коммуникация и сотрудничество между различными заинтересованными сторонами и отделами организации может привести к несогласованным действиям и неполным улучшениям.

5. Отсутствие системы измерения и оценки: Отсутствие системы для измерения и оценки эффективности процесса управления рисками может затруднить определение прогресса и улучшений.

6. Сложность изменений: Реализация улучшений в процессе управления рисками может столкнуться с сопротивлением со стороны персонала и требовать изменений в бизнес-процессах и структуре организации.

Вывод. Данная работа носит обзорный характер и затрагивает наиболее значительные моменты управления рисками в информационной безопасности. На основании результатов исследования был составлен перечень основных проблем, возникающих при управлении рисками информационной безопасности. Он позволяет определить, какие сложности могут возникнуть на каждом из этапов управления и составить план мероприятий по их устранению или обходу.

Информация, представленная в статье может быть использована как базис для последующих исследований по направлению управления рисками информационной безопасности, а также формирования рекомендаций для более эффективной реализации риск-ориентированного подхода.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. - Москва: Стандартинформ, 2021. – 24 с.
2. Анникин И.В. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики. // Министерство образования и науки РФ. Федеральное ГБОУ высшего образования “Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ” - 2017. - С.6-46.
3. Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton, and Tobias Stähle. The risk-based approach to cybersecurity/ Официальный сайт. McKinsey & Company. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity#/ (дата обращения: 15.04.2023).
4. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. - Москва: Компания АйТи; ДМК Пресс, 2004. - 384 с.
5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. / Электронный фонд правовых и нормативно-технических документов. - URL: https://docs.cntd.ru/document/1200084141 (дата обращения:17.04.2023).
6. Cyber Risk Resources for Practitioners./Institute of Risk Management. - URL: https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf (дата обращения: 17.04.2023).
7. NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. / National Institute of Standards and Technology. - URL: https://csrc.nist.gov/publications/detail/sp/800-39/final (дата обращения: 17.04.2023).
8. Анализ международных документов по управлению рисками информационной безопасности. Часть 1. / Эксперт Руслан Рахметов // ХАБР. - URL: https://habr.com/ru/articles/495236/

9. Анализ международных документов по управлению рисками информационной безопасности. Часть 2. / Эксперт Руслан Рахметов // ХАБР. - URL: https://habr.com/ru/articles/495986/
10. ГОСТ Р 51897-2011/Руководство ИСО 73:2009. Менеджмент риска. Термины и определения. / Электронный фонд правовых и нормативно-технических документов. - URL: https://docs.cntd.ru/document/1200088035 (дата обращения 20.04.2023).
11. Управление Рисками. / Кирилл Воротинцев. // Официальный сайт. Код Информационной Безопасности.- URL: https://codeib.ru/slides/slide/upravlenie-riskami-659 (дата обращения 20.04.2023).

References:

1. GOST R ISO/IEC 27000-2021. Information technology. Methods and means of ensuring security. Information security management systems. General overview and terminology. Moscow: Standartinform, 2021; 24. (In Russ)
2. Anikin I.V. Methods and algorithms for quantitative assessment and management of security risks in corporate information networks based on fuzzy logic. *Ministry of Education and Science of the Russian Federation. Federal State Educational Institution of Higher Education "Kazan National Research Technical University named after A.N. Tupolev-KAI*" 2017; 6-46. (In Russ)
3. Jim Boehm, Nick Curcio, Peter Merrath, Lucy Shenton, and Tobias Stähle. The risk-based approach to cybersecurity / Official website. McKinsey & Company. - URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity#/ (date of application:15.04.2023).
4. Petrenko S. A., Simonov S. V. Information risk management. Economically justified security. - Moscow: IT Company; DMK Press, 2004; 384. (In Russ)
5. GOST R ISO/IEC 27005-2010. Information technology. Methods and means of ensuring security. Information security risk management. / Electronic Fund of legal and regulatory documents. URL: https://docs.cntd.ru/document/1200084141 (date of application:17.04.2023). (In Russ)
6. Cyber Risk Resources for Practitioners. Institute of Risk Management. URL: https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf (date of application: 17.04.2023).
7. NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View /National Institute of Standards and Technology. - URL: https:csrc.nist.gov/publications/detail/sp/800-39/final (date of application: 17.04.2023).
8. Analysis of international documents on information security risk management. Part 1. / Expert Ruslan Rakhmetov.HABR. URL: https://habr.com/ru/articles/495236/ (date of application: 18.04.2023). (In Russ)
9. Analysis of international documents on information security risk management. Part 2. / Expert Ruslan Rakhmetov. HABR. URL: https:habr.com/ru/articles/495986/ (date of application: 18.04.2023). (In Russ)
10. GOST R 51897-2011/ISO 73:2009 Manual. Risk management. Terms and definitions. Electronic Fund of legal and regulatory documents. URL: https://docs.cntd.ru/document/1200088035 (date of application: 20.04.2023). (In Russ)
11. Risk Management. Kirill Vorotyntsev.Official website. Information Security Code. URL: https://codeib.ru/slides/slide/upravlenie-riskami-659 (date of application: 20.04.2023). (In Russ)

Сведения об авторах:
Артамонов Георгий Михайлович, студент, amenemuruart@gmail.com
Маслов Владимир Владимирович, студент, vladimirmaslov76@gmail.com
Резниченко Сергей Анатольевич, кандидат технических наук, доцент; rsa_5@bk.ru, ORCID.0000-0002-539-0457

Information about authors:
Georgy M. Artamonov, Student, amenemuruart@gmail.com
Vladimir V.Maslov, Student, vladimirmaslov76@gmail.com
Sergey A. Reznichenko, Cand.Sci. (Eng.), Assoc. Prof.; rsa_5@bk.ru, ORCID.0000-0002-539-0457

Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/Received 22.05.2023.
Одобрена после рецензирования/ Reviced 10.06.2023.
Принята в печать/Accepted for publication 10.06.2023.