УДК 33 DOI: 10.14451/1.239.434

Исследование основных подходов к управлению информационной безопасностью на предприятии

© 2024 **Мягков Иван Андреевич**
Аспирант, кафедра предпринимательства и конкуренции, факультет Бизнеса. Университет Синергия, Москва, Россия.
E-mail: sann60@mail.ru

© 2024 **Трубин Александр Евгеньевич**
Доцент, кандидат экономических наук, заведующий кафедры Цифровой Экономики. Университет Синергия, Москва, Россия.
E-mail: ATrubin@synergy.ru

Ключевые слова: информационная безопасность, управление информационной безопасностью, система менеджмента информационной безопасности (СМИБ), оценка рисков, метод анализа иерархий, организационные методы, технические методы, правовые методы, киберугрозы, защита информации.

Данная статья посвящена исследованию основных подходов к управлению информационной безопасностью на предприятии. Рассматриваются ключевые аспекты формирования системы менеджмента информационной безопасности (СМИБ) в условиях современных вызовов и угроз. Анализируются организационные, риск-ориентированные, технические и правовые методы обеспечения информационной безопасности. Особое внимание уделяется применению метода анализа иерархий как эффективного инструмента принятия решений в области защиты информации. Обсуждаются принципы построения СМИБ, включая оценку рисков, распределение ответственности и интеграцию безопасности в бизнес-процессы организации. Подчеркивается важность комплексного подхода к управлению информационной безопасностью для обеспечения устойчивого развития предприятия в современной информационной экономике.

В современном мире, характеризующемся глобальными трансформациями социально-экономических систем и стремительным технологическим прогрессом, наблюдается закономерное усиление внимания к проблематике информационной безопасности как на международном, так и на национальном уровнях. Это обусловлено беспрецедентным ростом объемов информации, сопровождающим новую фазу научно-технического развития и обострение экономической конкуренции. В данном контексте обеспечение информационной безопасности приобретает первостепенное значение и включает в себя комплекс мероприятий, направленных на защиту всех этапов информационного цикла: от создания данных до их хранения, обработки

и распространения.

Информация в современных условиях представляет собой критически важный экономический ресурс, являющийся фундаментом для социального, экономического, технологического и интеллектуального прогресса организаций и общества в целом. В контексте глобализации и развития информационного общества особую роль приобретают территориальные компьютерные сети различного масштаба — от локальных до глобальных. Их появление и развитие обусловлено достижениями в области информационных технологий и продиктовано необходимостью эффективного обмена информацией для оптимизации управленческих процессов.

В рамках организационного менеджмента, рассматривающего экономические системы как объект управления, информационные процессы приобретают особое значение. Организация, будучи стабильной формальной, социальной структурой, осуществляет трансформацию экономических ресурсов в готовую продукцию или услуги с целью удовлетворения потребностей потребителей и максимизации прибыли. В ходе этих процессов формируется многоуровневая информационная структура, включающая данные, информацию и знания, которая может быть концептуализирована как информационная пирамида менеджмента организации. Данная пирамида отражает иерархию и взаимосвязь различных типов информации, используемых в процессе принятия управленческих решений и обеспечения эффективного функционирования организации в условиях современной информационной экономики [5].

В текущих условиях процесс управления приобретает ключевое значение во всех аспектах человеческой деятельности. Особую актуальность данный вопрос имеет в контексте промышленных предприятий, где управленческая структура характеризуется высокой степенью сложности и многоуровневой иерархией. В рамках данной структуры осуществляется множество взаимосвязанных процессов, направленных на обеспечение эффективного функционирования организации в целом.

Одним из критически важных элементов в системе управления современным предприятием является менеджмент информационной безопасности. Данное направление представляет собой комплексный и многогранный процесс, интегрированный в общую систему корпоративного управления. Он охватывает широкий спектр мероприятий, начиная от разработки концептуальных основ и формирования нормативно-правовой базы и заканчивая практической реализацией стратегических планов по созданию, поддержанию и совершенствованию системы защиты информационных ресурсов организации. Эффективное управление информационной безопасностью в современных условиях становится одним из ключевых факторов, определяющих конкурентоспособность и устойчивость развития предприятия в долгосрочной перспективе.

В контексте современной информационной экономики организации обладают широким спектром информационных активов, представляющих собой ключевой фактор их конкурентоспособности и устойчивого развития. К числу наиболее значимых категорий таких активов относится стратегическая документация, отражающая долгосрочные и краткосрочные цели предприятия, а также его видение будущего. Данные документы, ввиду их высокой ценности и конфиденциальности, зачастую становятся объектом повышенного интереса со стороны конкурентов, что обусловливает необходимость их тщательной защиты [3].

Не менее важным информационным активом является совокупность данных о продуктах и услугах организации, а также ее интеллектуальная собственность, включая патенты и программное обеспечение. В условиях глобальной конкуренции и неравномерного соблюдения законодательства об авторском праве в различных юрисдикциях, защита этих активов приобретает критическое значение для сохранения конкурентных преимуществ компании. Особое место в структуре информационных активов занимают

коммерческие секреты и собственные знания организации, сформированные в процессе ее деятельности и представляющие собой уникальный источник конкурентного преимущества [8].

Значительную ценность представляет также текущая проектная документация, содержащая детальную информацию о разрабатываемых продуктах и услугах. Несанкционированный доступ к этим данным может позволить конкурентам ускорить вывод на рынок аналогичные предложения, что потенциально способно негативно повлиять на рыночные позиции организации. Отдельного внимания заслуживают персональные данные сотрудников, хранящиеся в кадровых подразделениях. Эта информация может быть использована злоумышленниками для шантажа или переманивания ценных кадров, что подчеркивает необходимость ее надежной защиты [14].

Наконец, важным информационным активом являются конфиденциальные данные клиентов, доверенные организации. Неспособность обеспечить должный уровень их защиты может привести не только к потере доверия клиентов, но и к нарушению законодательства в области информационной безопасности, что влечет за собой серьезные репутационные и финансовые риски. Таким образом, комплексное управление информационной безопасностью, охватывающее все перечисленные категории информационных активов, становится неотъемлемым элементом стратегии развития современной организации.

В современной парадигме управления предприятием информация рассматривается как стратегический ресурс, обладающий уникальными характеристиками и играющий ключевую роль в обеспечении конкурентоспособности организации. Подобно материальным активам, информационные ресурсы подлежат обработке, хранению и оценке, однако имеют ряд специфических особенностей. Информация, являясь нематериальным активом, тем не менее, требует значительных затрат на хранение, обработку и защиту, а также подвержена рискам повреждения, хищения или утраты. В этом контексте управление информационной безопасностью становится критически важным аспектом обеспечения непрерывности бизнес-процессов и устойчивого развития организации в целом [7].

Концептуальная основа информационной безопасности на уровне организации базируется на триаде фундаментальных принципов: конфиденциальность, целостность и доступность. Конфиденциальность предполагает реализацию комплекса мер, направленных на ограничение доступа к информации исключительно авторизованным пользователям, с возможностью имплементации дополнительных механизмов контроля для данных повышенного уровня риска. Целостность информации обеспечивается посредством внедрения систем управления, гарантирующих сохранение согласованности и точности данных на протяжении всего их жизненного цикла. Это достигается путем применения различных методов, включая строгий контроль доступа пользователей и предотвращение несанкционированных изменений или удаления информации [13].

Принцип доступности в контексте управления информационной безопасностью реализуется через разработку и внедрение процессов и процедур, обеспечивающих своевременный доступ авторизованных пользователей к необходимой информации. Это включает в себя широкий спектр мероприятий, начиная регулярным техническим обслуживанием и обновлением оборудования и программного обеспечения и заканчивая разработкой комплексных планов реагирования на инциденты и аварийного восстановления данных в случае кибератак. Таким образом, эффективное управление информационной безопасностью предполагает комплексный подход, охватывающий все аспекты работы с информационными ресурсами организации и направленный на минимизацию рисков и обеспечение устойчивости бизнес-процессов в условиях возрастающих киберугроз.

Несмотря на существенные преимущества, которые автоматизация данных предоставляет организациям, системы управления информаци-

онной безопасностью сталкиваются с рядом широко распространённых угроз. Одной из ключевых проблем является недостаточная степень автоматизации, сопровождающаяся ограниченным контролем корректности выполняемых действий. Это может привести к повышенной уязвимости системы к ошибкам и несанкционированным операциям. Внутренние угрозы также учитывает риски, связанные с недовольными сотрудниками, включая даже бывших работников, которые могут осуществлять кражи, подделки, удаление или модификацию данных, а также повреждение оборудования и иной инвентаризации [12].

Кроме того, инфраструктурные угрозы представляют существенную опасность, так как чрезвычайные ситуации, такие как пожары, наводнения и аварии, способны серьезно нарушить функционирование систем управления информационной безопасностью. Программные вирусы дополняют спектр потенциальных угроз, способных нанести значительный ущерб информационным системам. Уязвимости интегрированных систем управления информационной безопасностью свидетельствуют о слабых местах, которые могут быть эксплуатированы злоумышленниками для достижения несанкционированного доступа или нарушения работы организации [1].

Внешние угрозы, заключающиеся в несанкционированных воздействиях из интернета, направлены на получение доступа к ресурсам организации или на нарушение её деятельности. Помимо преднамеренных атак, существенную роль играют ошибочные и случайные (непреднамеренные) действия персонала организации. Такие действия могут вызвать непроизводительные затраты ресурсов и времени, привести к разглашению конфиденциальной информации через интернет или вызвать сбои в работе подсистем взаимодействия с интернетом, что, в свою очередь, негативно сказывается на общей функциональности организации [2].

Важными компонентами достижения и оценки конфиденциальности, целостности и доступности информации являются учет изменений, их тщательная оценка, классификация рисковых событий, а также адаптация системы управления информационной безопасностью к изменяющимся внешним и внутренним факторам. Систематизация собранной информации и оценка текущего состояния системы управления информационной безопасностью, а также достижение целей организации возможны исключительно при использовании специализированных методик. Применение таких методов позволяет обеспечить более точное и обоснованное прогнозирование ожидаемых результатов процессов, а также эффективное управление ими на основе достоверных фактов и данных [3].

Организационные методы представляют собой фундаментальный подход, базирующийся на принципе ответственности и приверженности высшего руководства целям информационной безопасности. Данная группа методов охватывает широкий спектр управленческих практик, включая анализ требований к информационной безопасности, разработку стратегических планов их реализации, осуществление административного контроля над внедряемыми системами защиты, а также формирование политики и стратегии в области информационной безопасности и управления рисками. Эти методы создают основу для интеграции принципов информационной безопасности в общую систему управления организацией.

Риск-ориентированные методы представляют собой комплексный подход к координации деятельности по управлению и контролю за организацией в контексте информационных рисков. Эта группа методов включает в себя разработку и применение методологий оценки рисков, а также стратегий по их минимизации и управлению, учитывающих специфику деятельности организации и особенности ее организационной структуры. Данный подход позволяет организациям эффективно идентифицировать, анализировать и приоритизировать потенциальные угрозы информационной безопасности, что способствует оптимальному распределению ресурсов и принятию обоснованных решений в области защиты

информации.

Технические методы образуют инструментальную базу для реализации организационных и риск-ориентированных подходов, предоставляя конкретные практики и средства управления информационной безопасностью. Эта группа методов включает в себя широкий спектр защитных мер, направленных на обеспечение конфиденциальности, целостности и доступности информации, снижение уязвимостей систем, ограничение воздействия инцидентов и облегчение процессов восстановления информационных активов. Технические методы служат практическим воплощением стратегических решений, принятых на организационном уровне, и обеспечивают реализацию мер по минимизации рисков, идентифицированных в рамках риск-ориентированного подхода.

Правовые методы дополняют вышеуказанные группы, обеспечивая нормативно-правовую основу для функционирования СМИБ. Эти методы направлены на интеграцию и соблюдение правовых норм в области информационной безопасности в повседневную деятельность организации. Они включают в себя разработку внутренних политик и процедур, соответствующих требованиям законодательства, а также мониторинг изменений в нормативно-правовой базе и адаптацию СМИБ к новым правовым реалиям. Таким образом, комплексное применение организационных, риск-ориентированных, технических и правовых методов позволяет создать эффективную и гибкую систему управления информационной безопасностью, способную адекватно реагировать на современные вызовы и угрозы в информационной сфере [6].

Международный стандарт ГОСТ Р ИСО/МЭК 27000-2021 [4] вводит концепцию СМИБ, которая представляет собой интегральный компонент общей системы управления, основанный на риск-ориентированном подходе. СМИБ охватывает весь жизненный цикл обеспечения информационной безопасности, включая этапы разработки, внедрения, функционирования, мониторинга, анализа, поддержки и непрерывного совершенствования защитных механизмов.

Современное предприятие, может быть, концептуализировано как совокупность взаимосвязанных процессов, часть из которых непосредственно ориентирована на достижение основных бизнес-результатов, в то время как другие выполняют вспомогательную функцию, обеспечивая поддержку ключевых операций. Данная концепция, известная как процессный подход, зарекомендовала себя в качестве эффективного инструмента для построения высокоэффективных систем управления организацией. В рамках этой методологии все аспекты деятельности предприятия рассматриваются через призму взаимосвязанных и взаимодействующих процессов, что позволяет оптимизировать управленческие решения и повысить общую эффективность функционирования организации [9].

Для обеспечения непрерывного совершенствования качества функционирования предприятия в контексте процессного подхода широко применяется цикл Деминга-Шухарта, также известный как PDCA (Plan-Do-Check-Act). Этот циклический алгоритм управления включает четыре последовательных этапа: планирование, осуществление, проверку и действие. Данная методология предполагает двухуровневую структуру управления, охватывающую как отдельные бизнес-процессы, так и их совокупность на уровне всей организации. Такой подход обеспечивает комплексное и согласованное управление всеми аспектами деятельности предприятия [15].

Принципы процессного подхода и цикла PDCA находят свое применение и в сфере управления информационной безопасностью. В этом контексте этап планирования включает всесторонний анализ текущей ситуации в организации, определение стратегических целей и задач в области информационной безопасности, а также разработку детальных планов по их достижению. Этап осуществления подразумевает практическую реализацию разработанных планов и внедрение соответствующих мер защиты. Проверка представляет собой комплекс мероприятий по изме-

рению и контролю эффективности внедренных мер, оценке степени достижения поставленных целей. Заключительный этап — действие — включает в себя анализ выявленных отклонений от запланированных результатов, корректировку существующих процессов и разработку стратегий по улучшению будущих показателей информационной безопасности. Таким образом, применение процессного подхода и цикла PDCA в управлении информационной безопасностью позволяет создать адаптивную и эффективную систему защиты, способную своевременно реагировать на изменяющиеся угрозы и соответствовать динамично развивающимся бизнес-требованиям.

Группа стандартов ГОСТ Р ИСО/МЭК 27000 представляет собой комплексный набор рекомендаций и требований, охватывающих все аспекты создания, внедрения и мониторинга СМИБ. Данные стандарты подчеркивают критическую важность интеграции СМИБ в общую структуру управления организацией, что позволяет учитывать вопросы информационной безопасности на всех этапах разработки и функционирования бизнес-процессов, информационных систем и средств управления. Такой подход обеспечивает необходимую гибкость и адаптивность СМИБ, позволяя ей эволюционировать в соответствии с изменяющимися потребностями и целями организации.

Фундаментальные принципы построения системы управления, применимые как к предприятию в целом, так и к его информационной безопасности, характеризуются универсальностью и не зависят от специфики деятельности организации. Однако это не означает, что СМИБ должна быть идентичной для всех предприятий. Напротив, эффективная система менеджмента информационной безопасности должна быть тщательно спроектирована с учетом индивидуальных особенностей организации, включая ее бизнес-цели, структуру, масштабы деятельности и ключевые бизнес-процессы. Более того, при разработке СМИБ необходимо принимать во внимание требования и ожидания всех заинтересованных сторон, включая клиентов, партнеров, поставщиков и регулирующие органы.

В научном сообществе существует дискуссия относительно универсальности применения процессного подхода к управлению информационной безопасностью. Некоторые исследователи предлагают альтернативный ситуационный подход, особенно для организаций с недостаточно развитой системой информационной безопасности. Этот подход основывается на принятии решений на основе анализа текущей ситуации, включая оценку рисков с учетом внутренних и внешних факторов. Однако важно отметить, что ситуационный подход не противоречит процессному, а скорее дополняет его. Анализ ситуации может быть интегрирован в рамки отдельных бизнес-процессов, что позволяет более точно определить границы и контекст проводимого анализа [10].

Стандарты серии ГОСТ Р ИСО/МЭК 27000 отличаются гибкостью в отношении конкретных методов и подходов к обеспечению информационной безопасности. Это предоставляет организациям широкий спектр возможностей для реализации СМИБ, адаптированной к их уникальным потребностям и условиям. Организации могут выбирать различные подходы к разработке политики безопасности, использовать различные формальные модели информационной безопасности, применять разнообразные методы анализа и оценки рисков. Кроме того, стандарты позволяют гибко подходить к выбору конкретных административных, экономических и технических средств защиты информации, а также методов и инструментов для мониторинга и верификации состояния защищенности информационных систем.

Такая гибкость стандартов способствует созданию эффективных и адаптивных систем менеджмента информационной безопасности, которые могут эволюционировать вместе с организацией, отвечая на новые вызовы и угрозы в области информационной безопасности. Это особенно важно в контексте быстро меняющейся технологической среды и постоянно возникающих

новых киберугроз. Организации получают возможность выбирать и комбинировать различные методы и инструменты, наиболее соответствующие их текущим потребностям и стратегическим целям, обеспечивая тем самым оптимальный баланс между уровнем защищенности информационных активов и эффективностью бизнес-процессов.

В контексте управления информационной безопасностью выбор оптимальных средств защиты представляет собой сложную многокритериальную задачу, требующую применения передовых методов теории принятия решений. Среди широкого спектра доступных методологий особое внимание заслуживают метод сценариев, метод анализа иерархий, метод дерева решений, методы имитационного моделирования и подходы, основанные на нечеткой логике. Каждый из этих методов обладает своими уникальными преимуществами и может быть эффективно применен в зависимости от специфики конкретной ситуации и характера решаемой задачи.

Метод анализа иерархий (МАИ) выделяется среди прочих как особенно перспективный инструмент для решения задач в области управления информационной безопасностью. Этот метод опирается на строгий математический аппарат и имеет широкий спектр практических приложений, что делает его особенно привлекательным для специалистов в сфере информационной безопасности. Фундаментальная концепция МАИ заключается в структурировании проблемы в виде трехуровневой иерархической модели. На вершине этой структуры находится глобальная цель, которую необходимо достичь. Средний уровень иерархии занимают критерии, детализирующие и конкретизирующие поставленную цель. Нижний уровень представлен набором альтернативных решений, каждое из которых потенциально может привести к достижению цели [11].

Процесс применения МАИ включает в себя несколько ключевых этапов. После построения иерархической структуры проводится серия попарных сравнений элементов каждого уровня. Для этого формируются специальные матрицы сравнений, в которых эксперты оценивают относительную важность критериев или альтернатив. Важным аспектом метода является вычисление индекса согласованности суждений, что позволяет оценить степень непротиворечивости экспертных оценок. На основе заполненных матриц сравнения вычисляются весовые коэффициенты для каждого критерия и каждой альтернативы по отношению к критериям. Финальным этапом является агрегирование полученных оценок и выбор наиболее предпочтительной альтернативы, которая характеризуется наивысшим интегральным показателем.

Универсальность и гибкость метода анализа иерархий позволяют применять его для решения широкого спектра задач в области информационной безопасности на различных уровнях принятия решений. На стратегическом уровне МАИ может быть использован для выбора оптимальной формальной модели безопасности при проектировании комплексной системы защиты информации предприятия. На тактическом уровне метод эффективен при сравнении и выборе конкретных средств защиты информации для противодействия определенным типам угроз. На оперативном уровне МАИ может применяться для оценки и выбора оптимальных стратегий обработки информационных рисков.

Важно отметить, что эффективность применения метода анализа иерархий в значительной степени зависит от качества экспертных оценок и корректности построения иерархической структуры. Поэтому при использовании МАИ в сфере информационной безопасности критически важно привлекать высококвалифицированных специалистов, обладающих глубоким пониманием как технических аспектов информационной безопасности, так и бизнес-процессов организации. Кроме того, для повышения объективности результатов рекомендуется комбинировать МАИ с другими методами анализа и моделирования, такими как методы имитационного моделирования или анализа рисков.

Подводя итоги настоящего исследования отме-

тим, что СМИБ представляет собой комплексную модель, охватывающую все аспекты защиты информационных ресурсов предприятия. Эта модель включает в себя процессы создания, внедрения, функционирования, мониторинга, анализа, поддержки и непрерывного совершенствования механизмов защиты информации. Фундаментальной основой СМИБ является систематическая оценка и обработка информационных рисков, что позволяет обеспечить эффективную поддержку бизнес-процессов организации в условиях динамично меняющегося ландшафта киберугроз.

При формировании СМИБ целесообразно опираться на основополагающие принципы управленческой деятельности, адаптируя их к специфике информационной безопасности. Эти принципы, переосмысленные в контексте управления информационной безопасностью, формируют концептуальную основу для построения эффективной СМИБ. Ключевыми аспектами этого подхода являются:

1. Осознание критической важности информационной безопасности на всех уровнях организации. Это подразумевает формирование культуры информационной безопасности, где каждый сотрудник понимает свою роль в защите информационных активов.
2. Четкое распределение ответственности за различные аспекты информационной безопасности. Это включает назначение ответственных лиц, определение их полномочий и обязанностей, а также создание системы подотчетности.
3. Интеграция административных функций с интересами всех заинтересованных сторон. Это предполагает балансирование между требованиями безопасности и потребностями бизнеса, учитывая интересы клиентов, партнеров, регуляторов и других стейкхолдеров.
4. Признание возрастающей роли социальных ценностей в контексте информационной безопасности. Это включает этические аспекты обработки данных, защиту приватности и соблюдение прав человека в цифровой среде.
5. Систематическая оценка рисков как основа для выбора и внедрения адекватных мер контроля и управления. Этот принцип подразумевает регулярное проведение анализа рисков и определение приемлемых уровней риска для организации.
6. Интеграция безопасности как неотъемлемого компонента во все информационные системы и сети организации. Это означает, что безопасность должна рассматриваться не как дополнительная функция, а как базовое свойство всей ИТ-инфраструктуры.
7. Проактивный подход к предупреждению и выявлению инцидентов информационной безопасности. Это включает внедрение систем раннего предупреждения, проведение регулярных аудитов и тестов на проникновение.
8. Реализация комплексного подхода к менеджменту информационной безопасности. Это предполагает охват всех аспектов безопасности: технических, организационных, правовых и человеческих факторов.
9. Непрерывная переоценка и адаптация системы информационной безопасности. Этот принцип отражает необходимость постоянного совершенствования СМИБ в ответ на изменения внешней и внутренней среды организации.

Важно отметить, что применение процессного подхода к управлению информационной безопасностью не противоречит принципу комплексности в рассмотрении вопросов защиты информации. Напротив, процессный подход позволяет структурировать и систематизировать деятельность по обеспечению информационной безопасности, интегрируя ее в общую систему управления организацией. Это способствует более эффективному выявлению взаимосвязей между различными аспектами безопасности и обеспечивает целостный взгляд на защиту информационных активов.

Таким образом, СМИБ, построенная на основе описанных принципов, представляет собой динамичную и адаптивную систему, способную эффективно реагировать на постоянно эволюци-

онирующие угрозы информационной безопасности. Она обеспечивает не только защиту информационных ресурсов, но и поддерживает стратегические цели организации, способствуя устойчивому развитию бизнеса в условиях цифровой трансформации.

Библиографический список

1. *Бадоян М. Д., Алиева А. М., Цукахина М. А.* Надежность информационных систем. Защита. Безопасность // Цифровизация экономики: направления, методы, инструменты : сборник материалов V Всероссийской научно-практической конференции, Краснодар, 16–21 января 2023 года. – Краснодар : Кубанский государственный аграрный университет имени И. Т. Трубилина, 2023. – С. 44–46.
2. *Булей Н. В., Поворина Е. В., Чижанькова И. В.* Обеспечение информационной безопасности со стороны персонала организации: угрозы, мотивы, методы и процедуры противодействия // Экономика и предпринимательство. – 2019. – 3(104). – С. 923–926.
3. *Ветрова Н. М., Гайсарова А. А.* Особенности менеджмента информационной безопасности на современном этапе // Экономика строительства и природопользования. – 2017. – 1(62). – С. 64–69.
4. ГОСТ Р ИСО/МЭК 27000-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология / Консультант Плюс Проф.
5. Информационный менеджмент в организации: оценка и стратегия развития / Е. И. Алехин [и др.] // Вестник Академии знаний. – 2023. – 4(57). – С. 470–473.
6. *Козырь Н. С.* Методические подходы риск-менеджмента информационной безопасности // Научные труды КубГТУ. – 2023. – № 4. – С. 99–109.
7. *Осташева Ю. Н.* Информационная безопасность предприятия // Актуальные вопросы развития национальной экономики : Материалы I Всероссийской с международным участием научно-практической конференции, Пермь, 28 февраля 2022 года. – Пермь : Пермский государственный национальный исследовательский университет, 2022. – С. 132–140.
8. *Симагина С. Г., Матвеева Е. А.* Особенности правовой охраны ранее созданных результатов инновационной деятельности // Вестник Оренбургского государственного университета. – 2004. – 9(34). – С. 25–33.
9. *Смирнов Е. Н.* Теоретические аспекты управления современными предприятиями // Педагогика, психология и экономика: вызовы современности и тенденции развития : Материалы Первой международной научно-практической конференции, Москва, 08 февраля 2024 года. – М. : Московская международная академия, 2024. – С. 155–159.
10. *Собакин И. Б.* Процессная модель управления рисками информационной безопасности // Вопросы экономических наук. – 2013. – 3(61). – С. 116–117.
11. *Сорокин А. И., Сорокин А. Д.* Метод анализа иерархий и его применение в управлении информационной безопасностью // Вестник Международной академии системных исследований. Информатика, экология, экономика. – 2014. – Т. 16, № 1. – С. 80–84.
12. *Сыкеев Д. В., Сыкеева И. Н.* Проблемы обеспечения информационной безопасности // Актуальные проблемы гуманитарных и социально-экономических наук. – 2023. – 4(100). – С. 45–48.
13. *Тетерина А. В.* Процесс управления рисками информационной безопасности // Научный аспект. – 2024. – Т. 47, № 4. – С. 6281–6295.
14. *Хестанова Л. А., Марков М. А.* Информационная безопасность. Технологии защиты персональных данных // Актуальные проблемы науковедения, культуры, образования, экономики, информатики и социальные трансформации – 2017 : Международная научно-практическая конференция, Москва, 12 апреля 2017 года. – М. : Полиграф сервис, 2017. – С. 287–292.
15. Цикл Деминга, или PDCA: улучшение процессов разработки и управление качеством продукта. – URL: https : / / skillbox . ru / media/management/tsikl_deminga (дата обр. 23.09.2024).