УДК 338
DOI 10.26118/2782-4586.2025.24.13.001

Константинов Михаил Александрович
Московская международная академия

Информационная безопасность как объект управления: теоретический аспект

Аннотация. В условиях глубокой цифровизации экономики и роста киберугроз информационная безопасность (ИБ) трансформируется из узкоспециализированной технической функции в стратегический элемент корпоративного управления и риск-менеджмента. В статье проводится теоретико-методологический анализ ИБ как сложного, многокомпонентного объекта управления, интегрированного в общую систему менеджмента организации. На основе международных стандартов (ISO/IEC 27001), национального законодательства (ФЗ № 149-ФЗ) и работ ведущих исследователей (Б. фон Солмс, Р. Баскервилл) раскрываются ключевые характеристики ИБ: социотехнический характер, риск-ориентированность, нормативная нагруженность и динамичность. Автор систематизирует пять теоретических подходов к пониманию ИБ в управленческой оптике — ресурсно-ориентированный, риск-ориентированный, процессный (PDCA), социотехнический и институциональный — и на их основе предлагает структурно-функциональную модель управления ИБ, включающую три иерархических уровня (стратегический, тактический, операционный) и пять базовых управленческих функций. Особое внимание уделяется эволюции ИБ от «первого поколения» (техническое обеспечение) к «второму поколению» (стратегическая интеграция в corporate governance, ERM, compliance и BCM). Статья подчёркивает, что эффективное управление ИБ в современных условиях невозможно без её осмысления как комплексной подсистемы, в которой технологические меры, организационные процессы, человеческий фактор и регуляторные требования выступают в едином управленческом контуре. Полученные выводы создают теоретическую основу для дальнейших эмпирических исследований в области метрик зрелости СМИБ, влияния корпоративной культуры на безопасность и стратегического позиционирования ИБ в цифровой экономике.

Ключевые слова: информационная безопасность, система менеджмента информационной безопасности (СМИБ), корпоративное управление, риск-ориентированный подход, социотехническая система, информационные активы, PDCA-цикл, киберриски.

Mikhail Alexandrovich Konstantinov
Moscow International Academy

Information security as an object of management: a theoretical aspect

Annotation. In the context of the deep digitalization of the economy and the growth of cyber threats, information security is being transformed from a highly specialized technical function into a strategic element of corporate governance and risk management. The article provides a theoretical and methodological analysis of information security as a complex, multicomponent management object integrated into the overall management system of the organization. Based on international standards (ISO/IEC 27001), national legislation (Federal Law No. 149-FZ) and the work of leading researchers (B. von Solms, R. Baskerville) reveals the key characteristics of information security: sociotechnical nature, risk-orientation, regulatory burden and dynamism. The author systematizes five theoretical approaches to understanding information security in management optics — resource-oriented, risk-oriented, process (PDCA), sociotechnical and institutional — and based on them offers a structural and functional information

security management model that includes three hierarchical levels (strategic, tactical, operational) and five basic management functions. Special attention is paid to the evolution of information security from the "first generation" (technical support) to the "second generation" (strategic integration into corporate governance, ERM, compliance and BCM). The article emphasizes that effective information security management in modern conditions is impossible without its understanding as a complex subsystem in which technological measures, organizational processes, the human factor and regulatory requirements act in a single management contour. The findings provide a theoretical basis for further empirical research in the field of ISMS maturity metrics, the impact of corporate culture on security, and the strategic positioning of information security in the digital economy.

Keywords: information security, information security management system (ISMS), corporate governance, risk-based approach, sociotechnical system, information assets, PDCA cycle, cyber risks.

Информационная безопасность (ИБ) перестала быть преимущественно технической проблемой и в современных условиях рассматривается как ключевое направление корпоративного управления и риск-менеджмента. Международные стандарты серии ISO/IEC 27000 определяют систему менеджмента информационной безопасности (СМИБ) как часть общей системы менеджмента организации, основанную на оценке рисков и предназначенную для установления, реализации, поддержания и постоянного улучшения политики и целей в области ИБ.

В российской практике это понимание закреплено через адаптацию ISO/IEC 27001 в национальный стандарт ГОСТ Р ИСО/МЭК 27001-2021, определяющий требования к СМИБ в организациях различных отраслей.

Рост значимости ИБ как объекта управления обусловлен не только технологической зависимостью бизнеса от цифровой инфраструктуры, но и масштабом экономических последствий инцидентов. По данным отчёта IBM «Cost of a Data Breach 2024», средняя стоимость утечки данных в мире достигла 4,88 млн долл. США, причём в финансовом секторе этот показатель традиционно выше среднерыночного [1].

Это приводит к тому, что ИБ встраивается в контуры корпоративного управления, управления рисками, непрерывности бизнеса, комплаенса и стратегического планирования.

В теоретическом плане управление ИБ постепенно эволюционирует от «первого поколения» — преимущественно технического и регламентно-ориентированного подхода — к «второму поколению» менеджмента ИБ, основанному на принципах корпоративного управления, риск-ориентированности и интеграции в общую систему менеджмента организации, на что указывал Б. фон Солмс, анализируя эволюцию концепции «information security management: the second generation» [2].

Цель данной статьи — раскрыть теоретический аспект информационной безопасности компании как объекта управления, описать её специфику как управляемой подсистемы, определить ключевые элементы, функции, уровни и механизмы управления, а также систематизировать базовые теоретико-методологические подходы к анализу ИБ в управленческой оптике.

В международных стандартах ISO/IEC 27000 информационная безопасность определяется как сохранение конфиденциальности, целостности и доступности информации, а также, при необходимости, иных свойств, таких как подлинность, подотчётность, неотказуемость и надежность.

В корпоративном контексте ИБ выступает:

- как состояние защищённости информационных активов компании от угроз;
- как совокупность процессов, политик, процедур и технических средств;
- как часть корпоративной системы управления рисками и соответствия требованиям (compliance).

Как управляемый объект ИБ обладает рядом специфических характеристик:

Социотехнический характер. Объект управления включает не только техническую инфраструктуру (сети, серверы, приложения), но и людей, организационные структуры, процессы и внешние регуляторные требования. Это соответствует социотехническому подходу к ИБ, сформированному в работах Р. Баскервилла и последующих авторов, рассматривающих безопасность как свойство комплексной системы «человек – технология – организация» [3].

Риск-ориентированность. ИБ как объект управления проявляется через совокупность рисков, связанных с угрозами, уязвимостями и последствиями их реализации. ISO/IEC 27001 закрепляет риск-ориентированный подход как основу для построения СМИБ: управление ИБ фактически сводится к циклу идентификации, анализа, оценки и обработки рисков.

Нормативная нагруженность. Современная ИБ существует в плотном регуляторном поле (законодательство об информации и персональных данных, отраслевые требования, стандарты), что делает объект управления одновременно техническим и правовым. В России это, в частности, Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и подзаконные акты к нему [4].

Динамичность и неопределённость. Конфигурация угроз и уязвимостей постоянно изменяется. Это придаёт объекту управления черты «движущейся цели», что требует непрерывного мониторинга и цикличного пересмотра управленческих решений.

Таким образом, информационная безопасность компании как объект управления может быть описана как интегрированная подсистема корпоративного управления, объединяющая ресурсы (активы), процессы (политики, процедуры), людей (пользователи, специалисты, руководители) и инфраструктуру (технологии) в целях управления рисками, связанными с информацией.

Теоретическая рефлексия над управлением ИБ опирается на несколько исследовательских традиций. Условно можно выделить следующие подходы.

1. Ресурсно-ориентированный подход. В логике ресурсно-ориентированного подхода информационная безопасность рассматривается как специфический стратегический ресурс и элемент нематериального капитала компании, который обладает ценностью, редкостью, трудностью имитации и незаменимостью. Комплексно выстроенная система ИБ формирует «организационный капитал» в виде процедур, рутин, доверительных отношений и репутации, обеспечивающей устойчивость бизнеса в условиях цифровых угроз.

2. Риск-ориентированный подход. С позиций риск-менеджмента ИБ трактуется как подсистема управления рисками, направленная на идентификацию, оценку и обработку рисков, связанных с нарушением конфиденциальности, целостности и доступности информации. Международные стандарты ISO/IEC 27005 (risk management) и практики NIST Cybersecurity Framework институционализируют риск-ориентированный подход, связывая управление ИБ с финансовыми и операционными показателями компании [5].

3. Процессный подход и PDCA-модель. ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001-2021 основываются на цикле PDCA (Plan–Do–Check–Act), рассматривая ИБ как совокупность управляемых процессов, подлежащих постоянному улучшению.

В этом контексте объектом управления выступает не только состояние защищённости, но и сами процессы — планирование, внедрение, контроль и совершенствование мер безопасности.

4. Социотехнический и организационный подход. Работы Р. Баскервилла, Б. фон Солмса и других исследователей подчёркивают, что безопасность информационных систем – это в первую очередь организационно-социальная проблема, а не только техническая [6].

Социотехнический подход фокусируется на взаимосвязи технологических решений с культурой, структурой и практиками организации: уровень ИБ определяется не только качеством шифрования или настройки межсетевых экранов, но и поведением

пользователей, управленческими стилями, системой мотивации и корпоративной культурой.

5. Институциональный и нормативный подход. ИБ рассматривается как институт, встроенный в систему формальных норм (законодательство, стандарты, внутренние регламенты) и неформальных правил (практики использования ИТ, этика, «невидимые» организационные соглашения). Теоретическая рамка здесь включает концепции институциональной экономики и теории регуляции, акцентируя влияние внешних регуляторов (государства, отраслевых регуляторов, профессиональных ассоциаций) на формирование корпоративной политики ИБ.

С учётом изложенных подходов ИБ компании как объект управления может быть представлена в виде структурно-функциональной модели, включающей следующие блоки (рисунок 1):

Функционально управление ИБ включает классические управленческие функции, адаптированные к специфике объекта:

- Планирование: формирование политики, целей, риск-аппетита, планов обработки рисков;
- Организация: определение структуры, ролей, распределение ресурсов, интеграция ИБ в бизнес-процессы;
- Мотивация: создание стимулов соблюдения требований ИБ, формирование культуры «security awareness»;
- Контроль: мониторинг инцидентов, аудиты, KPI, пересмотр эффективности мер контроля;
- Улучшение: корректирующие и предупреждающие действия, пересмотр политики и процедур в рамках PDCA-цикла.

Рисунок 1. ИБ компании как объект управления: структурно-функциональная модель.

Стратегический уровень (совет директоров, высшее руководство) — определение принципов, риск-аппетита, приоритизация инвестиций, включение ИБ в стратегию. Б. фон Солмс подчёркивает, что на этом уровне ИБ становится частью корпоративного управления (information security governance).

Тактический уровень (CISO, руководители направлений) — разработка политик, планов, программ безопасности, управление проектами по внедрению средств и процессов ИБ.

Операционный уровень (администраторы, специалисты ИБ, пользователи) — реализация процедур, реагирование на инциденты, соблюдение регламентов, эксплуатация средств защиты.

Взаимосвязь уровней носит двусторонний характер: стратегические решения определяют рамки и ресурсы, а операционные данные (инциденты, результаты аудитов, показатели KPI) служат основой для корректировки стратегии. Это подчёркивает цикличность управления ИБ как объекта, характеризующегося динамичной обратной связью.

В современных моделях корпоративного управления ИБ рассматривается как ключевой элемент обеспечения устойчивости бизнеса и доверия заинтересованных сторон (stakeholders). Отчёты международных консалтинговых и аудиторских компаний фиксируют рост внимания советов директоров к вопросам киберрисков и ИБ; в ряде стран регуляторы прямо возлагают ответственность за киберустойчивость на высшее руководство.

С теоретической точки зрения это означает, что ИБ не может оставаться только задачей ИТ-подразделения. Она интегрируется:

- в систему ERM (Enterprise Risk Management) — риски ИБ рассматриваются наряду с финансовыми, операционными, правовыми и репутационными;
- в систему compliance — соблюдение требований по персональным данным, критической инфраструктуре, отраслевым стандартам;
- в систему управления непрерывностью бизнеса (BCM) — ИБ выступает предпосылкой способности компании функционировать при инцидентах.

Таким образом, объект управления «информационная безопасность» оказывается вписанным в более широкий контекст корпоративного управления. Это требует согласованности целей и показателей: KPI ИБ должны соотноситься с бизнес-целями (снижением потерь, увеличением доверия клиентов, обеспечением соответствия).

Теоретический анализ информационной безопасности компании как объекта управления позволяет выделить несколько ключевых положений.

Во-первых, ИБ представляет собой социотехнический и институционально нагруженный объект, сочетающий в себе технологические, организационные, правовые и культурные компоненты. Её нельзя свести к набору технических средств; она должна рассматриваться как интегрированная управляемая подсистема корпоративной системы.

Во-вторых, доминирующим теоретическим основанием управления ИБ является риск-ориентированный подход, институционализированный в международных и национальных стандартах (ISO/IEC 27001, ГОСТ Р ИСО/МЭК 27001-2021). Он предполагает, что объект управления описывается через конфигурацию рисков, а управленческие решения строятся на их идентификации, оценке и обработке.

В-третьих, развитие менеджмента ИБ демонстрирует движение от «первого поколения» — технического и регламентного — к «второму поколению», основанному на принципах corporate governance, стратегической интеграции и непрерывного улучшения, о чём свидетельствуют работы Б. фон Солмса и других исследователей.

В-четвёртых, структурно-функциональная модель ИБ как объекта управления включает совокупность элементов (активы, угрозы, уязвимости, меры защиты, процессы и результаты), связанных управленческим циклом PDCA и распределённых по стратегическому, тактическому и операционному уровням.

Наконец, встраивание ИБ в систему корпоративного управления и риск-менеджмента делает её управляемость критическим фактором устойчивости и конкурентоспособности компании в цифровой экономике. Теоретическое осмысление ИБ как объекта управления создаёт основу для дальнейших эмпирических исследований — разработки метрик эффективности управления ИБ, моделей зрелости СМИБ, анализа влияния организационной культуры на уровень защищённости и др.

Такое понимание позволяет перейти от фрагментарного, «технического» взгляда на безопасность к целостной управленческой концепции, в которой информационная безопасность становится не только средством защиты, но и важной составляющей стратегического развития организации.

Список источников

1. IBM reports average breach costs hit record $4.88M in 2024, up 10% from last year. URL:https://siliconangle.com/2024/07/30/ibm-reports-average-breach-costs-hit-record-4-88m-2024-10-last-year/ (дата обращения: 12.10.2025 г.)
2. Васильева И.Н., Стельмашонок Е.В. Современный взгляд на управление информационной безопасностью предприятия. Вестник ИНЖЭКОНа. Серия: Экономика. 2014. № 1 (68). С. 166-171.
3. Руднева Н.И. Менеджмент экономической безопасности в социотехнических системах: сущность и специфика. Наука и Образование. 2025. Т. 8. № 1.
4. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL:http://www.kremlin.ru/acts/bank/24157 (дата обращения: 12.10.2025 г.)
5. Управление рисками информационной безопасности. Стандарт ISO/IEC 27005:2018. URL:https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-6-standart-iso-iec-27005-2018/ (дата обращения: 12.10.2025 г.)
6. Козачок В.И. Информационная безопасность корпорации как объект социального управления. Власть. 2017. Т. 25. № 5. С. 74-82.

Сведения об авторе

Константинов Михаил Александрович, аспирант Московской международной академии, г. Москва, Россия

Information about the author

Konstantinov Mikhail Alexandrovich, PhD student at the Moscow International Academy, Moscow, Russia