

УДК 338.2

DOI: 10.26456/2219-1453/2026.3.229-241

Цифровой инструментарий в системе корпоративного управления: подходы и специфические риски

С.А. Гурдюмов

ФГБОУ ВО «Финансовый университет при Правительстве
Российской Федерации», г. Москва

Статья посвящена применению цифрового инструментария в деятельности органов управления и контроля публичных компаний. Актуальность темы определяется тем, что цифровые решения внедряются в работу советов директоров, комитетов, служб внутреннего контроля и аудита и корпоративного секретаря быстрее, чем складываются упорядоченные представления о соответствии инструментов функциям органов и о порождаемых ими рисках. Цель исследования – обоснование методического подхода, который связывает выбор цифрового инструмента с функцией органа управления или контроля и достигнутым уровнем его цифровой зрелости и классифицирует связанные с применением инструментария специфические риски. В статье разграничены понятия цифровизации, цифровой трансформации и цифрового инструментария; типовые цифровые инструменты соотнесены с функциями органов управления и контроля; обоснован методический подход, в основе которого лежит правило соответствия инструмента функции органа и уровню цифровой зрелости и определение контура контроля; систематизированы специфические риски, не сводимые к техническим рискам информационных технологий. Научная новизна: цифровой инструментарий классифицирован по функциям органов управления и контроля, а эффект от цифровой трансформации связывается с уровнем цифровой зрелости и контуром контрольного воздействия, в то же время несоответствие инструмента функции и уровню зрелости рассматривается как источник специфических рисков цифровизации

Ключевые слова: цифровой инструментарий, цифровая трансформация, цифровая зрелость, совет директоров, внутренний контроль, внутренний аудит, контур контроля, специфические риски.

Введение

Цифровая трансформация меняет условия работы органов управления и контроля публичных компаний. Электронный документооборот, защищенные платформы подготовки и проведения заседаний, аналитические сервисы, автоматизированные средства контроля и системы дистанционного взаимодействия с акционерами входят в повседневную практику советов директоров, комитетов при совете, служб внутреннего контроля и аудита, корпоративного секретаря

© Гурдюмов С.А., 2026

[17; 18]. Указанные решения затрагивают не только техническую организацию корпоративных процедур, но и порядок подготовки, обсуждения и принятия решений, а также распределение контрольных функций между органами. Для публичных компаний значимость таких изменений повышается из-за интенсивного информационного обмена, требований к раскрытию информации и необходимости согласованной работы нескольких органов управления и контроля [2; 5].

Вместе с возможностями цифровые решения формируют новые источники уязвимости. Зависимость от внешней цифровой инфраструктуры и расширение дистанционного формата повышают значимость киберрисков и рисков информационной безопасности на уровне совета директоров [11; 19]. Применение алгоритмических и аналитических инструментов при подготовке решений ставит вопрос о границах их использования и о сохранении ответственности органов управления [12]. Поэтому цифровой инструментарий следует рассматривать не как нейтральное техническое средство, а как фактор, влияющий на качество корпоративного управления и на профиль связанных с ним рисков.

Научная проблема состоит в том, что цифровые решения внедряются в деятельность органов управления и контроля быстрее, чем складываются упорядоченные представления о том, какой инструмент соответствует функции конкретного органа, какому уровню готовности компании он отвечает и какие специфические риски порождает. Результат цифровизации зависит не только от самого инструмента, но и от зрелости процессов, в которые он встраивается: содержательно оцифровать можно лишь отлаженный и описанный процесс, тогда как перенос в цифровую форму неупорядоченной процедуры дает преимущественно ее формальное отображение. Вследствие этого выбор и применение цифровых инструментов нередко происходят без увязки с функцией органа и достигнутым уровнем цифровой зрелости, что снижает отдачу от цифровизации и повышает сопутствующие риски.

Несмотря на рост числа работ по цифровизации корпоративного управления, сохраняется недостаточная систематизация цифрового инструментария органов управления и контроля. Цифровизация чаще рассматривается либо как часть общей информационно-технологической трансформации бизнеса, либо как фактор повышения эффективности корпоративных процедур, тогда как связь конкретных решений с функциями органов, с уровнем цифровой зрелости и с профилем специфических рисков остается слабо проработанной [3; 18]. Ранее автором была предложена классификация цифровых технологий по характеру их влияния на функции и процессы органов управления и контроля [1]; настоящая работа развивает данное направление, перенося анализ с характера влияния технологий на порядок применения

конкретных цифровых инструментов в привязке к функциям органов и уровню их цифровой зрелости.

Цель статьи – обоснование методического подхода, связывающего выбор цифрового инструмента с функцией органа управления или контроля и уровнем его цифровой зрелости и классифицирующего связанные с применением инструментария специфические риски.

Понятийные границы: цифровизация, цифровая трансформация и цифровой инструментарий

В литературе понятия цифровизации и цифровой трансформации нередко используются как взаимозаменяемые, что затрудняет анализ конкретных цифровых решений в корпоративном управлении. Для целей настоящей работы их целесообразно развести и дополнить третьим, более узким понятием – цифровым инструментарием.

Под цифровизацией понимается перевод информации и отдельных процедур в цифровую форму и внедрение цифровых технологий в отдельные процессы без изменения их логики и распределения функций. Цифровизация носит локальный характер: она повышает скорость и точность операций, но оставляет неизменными порядок принятия решений и структуру управления [18].

Цифровая трансформация представляет собой более глубокий процесс, при котором цифровые технологии меняют не отдельные процедуры, а способ организации деятельности, модель управления и характер взаимодействия между ее участниками [17; 18]. В корпоративном управлении трансформация проявляется в изменении порядка подготовки и принятия решений, в перераспределении контрольных функций и в появлении новых форм взаимодействия органов управления с акционерами и иными заинтересованными сторонами [2; 7]. Трансформация есть процесс изменения, а не набор средств, поэтому ее нельзя свести к перечню внедренных технологий.

Цифровой инструментарий занимает в рассматриваемом ряду обособленное место. Под цифровым инструментарием органов управления и контроля понимается совокупность цифровых решений, платформ и сервисов, применяемых для выполнения функций стратегического управления, контроля, корпоративного взаимодействия и раскрытия информации. В отличие от трансформации как процесса, инструментарий есть средства, через которые она реализуется; в отличие от цифровизации отдельной операции, инструментарий рассматривается в привязке к функции конкретного органа управления или контроля. Такое разграничение позволяет перейти от общих рассуждений о цифровизации к анализу того, какие именно решения и для каких функций применяются и какие последствия они порождают.

Применимость цифрового инструментария определяется не только его техническими возможностями, но и готовностью процессов, в которые он встраивается. Готовность процессов отражает понятие цифровой зрелости, использованное ранее при классификации цифровых технологий по характеру их влияния на функции органов управления и контроля [1]. Под цифровой зрелостью в настоящей работе понимается степень, в которой процессы органа управления или контроля описаны, регламентированы, обеспечены качественными данными и интегрированы между собой настолько, что допускают содержательное применение цифровых решений и переход от автоматизации отдельных операций к цифровой поддержке принятия решений и контроля. Цифровая зрелость характеризует не отдельную технологию, а готовность функции к цифровизации, и поэтому может различаться у разных органов одной компании. Низкая зрелость ограничивает отдачу даже от технически совершенного инструмента, а применение сложного решения к неупорядоченному процессу переносит в цифровую форму его недостатки. Поэтому цифровой инструментарий далее рассматривается не сам по себе, а в связке с функцией органа и достигнутым уровнем цифровой зрелости.

Цифровой инструментарий органов управления и контроля

Распределение цифрового инструментария по функциям органов управления и контроля опирается на ранее предложенную классификацию цифровых технологий по характеру их влияния на функции и процессы этих органов [1]. Если в указанной работе технологии группировались по типу воздействия на управленческие функции, то в данной работе рассматривается обратная сторона вопроса: какие конкретные цифровые инструменты закреплены за отдельными функциями и органами.

Деятельность совета директоров и комитетов при совете обеспечивается прежде всего платформами подготовки и проведения заседаний (board portal systems), которые предоставляют защищенный доступ к материалам, ведение повестки, электронное согласование и хранение документов, фиксацию решений и голосований. Указанные инструменты поддерживают функцию стратегического управления и коллегиального контроля, для которой характерны работа с большими объемами документации и требования к конфиденциальности [5; 16]. Их дополняют аналитические панели мониторинга, агрегирующие показатели деятельности компании для совета, а также сервисы, поддерживающие подготовку решений на основе анализа данных; применение таких сервисов в подготовке решений ставит отдельный вопрос о границах их использования [12].

Комитет по аудиту и комитет по рискам используют аналитические платформы и средства автоматизированного

мониторинга, позволяющие отслеживать ключевые риски и контрольные показатели в режиме, близком к непрерывному. Для функции контроля цифровой инструментариий смещает акцент с выборочных проверок по итогам периода на постоянное наблюдение за процессами.

В системе внутреннего контроля и внутреннего аудита применяются автоматизация контрольных процедур, средства анализа данных и непрерывный мониторинг. Концепция непрерывного аудита предполагает регулярную автоматизированную проверку операций и контрольных процедур вместо периодических обследований [8]. Данные инструменты расширяют охват контроля и сокращают разрыв между событием и его выявлением, однако предъявляют повышенные требования к качеству данных и регламентации процессов.

Корпоративный секретарь использует системы электронного документооборота, цифровые средства организации заседаний и дистанционного взаимодействия с акционерами, а также сервисы раскрытия информации. Перечисленные инструменты обслуживают функцию корпоративного взаимодействия и информационной открытости, обеспечивая своевременность и полноту раскрытия [2; 4; 14].

Функция взаимодействия с акционерами на общем собрании поддерживается системами электронного голосования и проведения собраний в дистанционном и гибридном форматах. Распространение данных систем расширяет участие акционеров, но одновременно затрагивает вопросы легитимности процедур, идентификации участников и фиксации волеизъявления [6; 15].

Проведенный анализ показывает, что один и тот же класс решений (например, средства аналитики или дистанционного взаимодействия) применяется разными органами и для разных функций, а значит, и последствия его применения, и необходимый контур контроля будут различаться.

Методический подход к применению цифрового инструментария

Предлагаемый методический подход определяет порядок выбора цифрового инструмента исходя из функции органа управления или контроля и достигнутого уровня его цифровой зрелости. Суть подхода заключается в решающем правиле, которое связывает функцию органа и уровень зрелости с допустимым классом инструмента и необходимым контуром контроля. В основе подхода лежит положение о том, что эффект цифрового инструмента не является автоматическим: один и тот же инструмент дает разный результат в зависимости от того, какую функцию он обслуживает и уровень зрелости процесса, в который он встраивается.

Данное положение подтверждается эмпирически – по данным Deloitte, компании с высоким уровнем цифровой зрелости примерно в 3 раза чаще компаний с низкой зрелостью сообщают о темпах роста выручки и рентабельности, заметно превышающих среднеотраслевые: о превышении среднеотраслевой рентабельности заявляют около 50 %

зрелых компаний против 17 % компаний с низкой зрелостью [9]. Отдача от цифровых решений определяется не самим фактом их внедрения, а зрелостью процессов. Одновременно сохраняется разрыв между внедрением и готовностью к контролю: 66% организаций ожидают наибольшего влияния искусственного интеллекта на кибербезопасность, однако лишь 37 % имеют процедуры оценки безопасности таких инструментов до их применения [19]. Этот разрыв и составляет область, которой адресован предлагаемый подход.

Основанием подхода служит функция органа, а не технический тип решения. Выбор такого основания определяется тем, что ответственность за результат и контур контроля закрепляются не за технологией, а за функцией конкретного органа: как показано выше, один класс решений в разных функциях порождает разные риски и требует разного контроля. Поэтому функциональная классификация цифрового инструментария (табл. 1) выступает рабочим инструментом подхода: она задает соответствие между функцией органа, типовым инструментом, специфическим риском и контуром контроля и используется как основа для решения о допустимости инструмента.

Таблица 1

Функциональная классификация цифрового инструментария
как основа методического подхода

Функция органа управления и контроля	Типовой цифровой инструмент	Специфический риск	Контур контроля
Стратегическое управление (совет директоров)	Платформы заседаний, аналитические панели мониторинга	Снижение качества коллективного обсуждения, чрезмерная опора на агрегированные данные	Совет директоров, комитет по стратегии
Подготовка решений на основе аналитики (совет, менеджмент)	Аналитические и алгоритмические сервисы поддержки решений	Алгоритмические ошибки, ослабление профессионального суждения, размывание ответственности	Совет директоров, комитет по аудиту
Контроль и аудит (комитет по аудиту, внутренний аудит и контроль)	Непрерывный мониторинг, автоматизация контрольных процедур	Формализация контроля, пропуск нетипичных рисков, зависимость от качества данных	Комитет по аудиту, служба внутреннего аудита
Управление рисками (комитет по рискам, риск-менеджмент)	Платформы анализа и мониторинга рисков	Неполнота моделей риска, ложная уверенность в оценках	Комитет по рискам, служба риск-менеджмента

Функция органа управления и контроля	Типовой цифровой инструмент	Специфический риск	Контур контроля
Корпоративное взаимодействие и раскрытие (корпоративный секретарь)	Электронный документооборот, сервисы раскрытия информации	Утечки информации, нарушение полноты и сроков раскрытия	Корпоративный секретарь, служба внутреннего контроля
Взаимодействие с акционерами (общее собрание)	Электронное голосование, дистанционные и гибридные собрания	Риски легитимности решений, идентификации участников, кибератак на процедуру	Совет директоров, корпоративный секретарь, ревизионная комиссия

Уровень цифровой зрелости оценивается по отдельной функции, а не по компании в целом, и определяется по наблюдаемым признакам: степени регламентации процесса, наличию и качеству данных, связанности решений между собой и влиянию цифрового инструмента на содержание решений. Базовому уровню отвечает перевод документооборота в цифровую форму при сохранении прежней логики процесса. Интегрированному уровню – связанность решений и использование аналитики при подготовке решений. Стратегическому уровню – встроенность инструментария в процессы управления и контроля и его влияние на содержание принимаемых решений. Уровень зрелости задает верхнюю границу сложности инструмента: решение, опережающее зрелость процесса, дает формальный результат, а не управленческий эффект.

Решающим элементом подхода выступает правило соответствия. Цифровой инструмент признается допустимым для функции при одновременном выполнении двух условий: его сложность не превышает достигнутого уровня цифровой зрелости этой функции, и за результаты его применения ответственен определенный контур контроля, то есть орган или подразделение, отвечающее за работу инструмента и за проверку его выводов. Если хотя бы одно условие не выполнено, инструмент переходит из источника пользы в источник специфического риска: при превышении зрелости – риск формализации, при отсутствии контура – риск утраты ответственности. Правило соответствия переводит выбор цифрового инструмента из технического решения в управленческое, обусловленное функцией и зрелостью.

Допустимый по этому правилу инструмент оценивается по двум группам критериев, которые операционализируют сопоставление эффекта и риска. Эффективность оценивается по охвату функции (доля операций или решений, поддержанных инструментом), своевременности (сокращение разрыва между событием и его выявлением или

отражением) и интегрированности (связанность с другими инструментами органа). Риск оценивается по чувствительности к киберугрозам, степени алгоритмизации и ее влиянию на профессиональное суждение, зависимости от внешнего поставщика и влиянию на качество коллективного обсуждения. Решение о применении инструмента принимается в пользу варианта, при котором прирост эффективности на данном уровне зрелости не сопровождается непропорциональным ростом риска.

Применение правила можно показать на двух функциях. В функции внутреннего аудита непрерывный мониторинг анализирует операции и контрольные процедуры в режиме, близком к сплошному, вместо выборочных проверок по итогам периода [8], что повышает охват и своевременность. Такой эффект достигается лишь при интегрированном или стратегическом уровне зрелости, когда процедуры регламентированы, а данные пригодны для анализа; при базовом уровне тот же инструмент дает формальный охват без содержательного контроля. Контур контроля здесь образуют комитет по аудиту и служба внутреннего аудита. В функции взаимодействия с акционерами электронное голосование и дистанционные собрания допускаются уже в большинстве правопорядков: на конец 2024 г. виртуальные собрания разрешены в 85 %, гибридные – в 94 % юрисдикций [15]. При этом в 42 % юрисдикций отсутствует порядок управления цифровыми рисками собраний, а в 48 % – защита акционеров при сбоях [15]. Без закреплённого контура контроля (совет директоров, корпоративный секретарь, ревизионная комиссия) преобладает не польза от цифровизации, а риск легитимности решений.

Результатом применения подхода становится обоснованное соответствие цифровых инструментов функциям органов с закреплённым контуром контроля и оценкой допустимости по критериям эффективности и риска. Подход задает правило, по которому состав инструментария определяется функцией органа и достигнутым уровнем его цифровой зрелости.

Специфические риски применения цифрового инструментария

Внедрение цифрового инструментария порождает риски, которые не сводятся к техническим рискам информационных технологий. Технические риски (сбои, уязвимости, недоступность систем) относятся к сфере информационной безопасности и управляются профильными подразделениями. Специфические риски корпоративного управления возникают на уровне функций органов управления и контроля и затрагивают качество решений, легитимность процедур и распределение ответственности. Источником таких рисков часто выступает не сама технология, а несоответствие между уровнем цифровой зрелости

процесса и сложностью внедряемого инструмента. Целесообразно выделить несколько групп специфических рисков.

Первая группа – риски легитимности решений. Перевод заседаний и голосования в дистанционный и гибридный формат расширяет участие, но ставит вопросы кворума, идентификации участников, корректной фиксации волеизъявления и защиты процедуры от вмешательства. Недостаточная проработка указанных вопросов может ставить под сомнение действительность принятых решений [6; 15].

Вторая группа – риски алгоритмизации и ослабления профессионального суждения. Использование аналитических и алгоритмических сервисов при подготовке решений способно повышать их обоснованность, но при чрезмерной опоре на алгоритм возникает риск переноса ответственности на инструмент, снижения критического анализа со стороны членов органов управления и тиражирования заложенных в модель ошибок. Особую сложность представляет распределение ответственности за решение, поддержанное алгоритмом [12].

Третья группа – риски формализации контроля. Автоматизация контрольных процедур и непрерывный мониторинг расширяют охват контроля, однако создают риск подмены содержательного контроля формальным: наличие цифровой процедуры может восприниматься как доказательство ее результативности. Риск усиливается, когда инструмент внедряется в недостаточно зрелый процесс, и сопровождается снижением качества коллективного обсуждения, если цифровой формат вытесняет содержательную дискуссию [8].

Четвертая группа – риски зависимости от поставщиков цифровых решений. Использование внешних платформ и сервисов формирует зависимость от их поставщиков, включая риск ограниченной заменяемости решений, концентрации критичных функций у одного провайдера и утраты контроля над данными. Значимость такой зависимости подтверждается тем, что 54 % крупных организаций называют цепочку поставок главным барьером для киберустойчивости, а 72 % отмечают рост киберрисков [19]. Зависимость от внешней цифровой инфраструктуры повышает значимость киберрисков и рисков утечки информации на уровне органов управления, что требует их рассмотрения как вопроса корпоративного управления, а не только информационной безопасности [10; 11; 13; 19].

Перечисленные группы рисков связаны между собой и с уровнем цифровой зрелости: чем больше разрыв между сложностью инструмента и отлаженностью процесса, тем выше вероятность того, что ожидаемая польза обернется формализацией, утратой контроля или сомнительной легитимностью решений. Управление специфическими рисками нельзя отделять от выбора инструмента. Поскольку и эффект, и риск цифрового решения определяются сочетанием функции органа, уровня зрелости и

закрепленного контура контроля, риск формируется уже в момент выбора инструмента, а не после его внедрения. Оценка риска, выполняемая обособленно и после того, как инструмент зафиксирован, лишает организацию наиболее действенных мер – подбора инструмента под уровень зрелости функции и закрепления контура контроля до начала эксплуатации. Распространенность разрыва между темпами внедрения цифровых решений и готовностью процедур их контроля, отмеченная выше, подтверждает, что вынесение оценки риска за пределы выбора инструмента ведет к накоплению уязвимости. Поэтому управление специфическими рисками целесообразно встраивать в методический подход, определяя для каждого инструмента допустимость по уровню зрелости, контур контроля и критерии оценки.

Заключение

Проведенное исследование показало, что цифровой инструментарий становится самостоятельным элементом системы корпоративного управления, а его применение затрагивает не только техническую организацию процедур, но и порядок принятия решений, контроль и распределение ответственности между органами управления и контроля.

Разграничены понятия цифровизации, цифровой трансформации и цифрового инструментария, что позволило рассматривать цифровые решения в привязке к функциям конкретных органов, а не как часть общей информационно-технологической трансформации. Типовые цифровые инструменты соотнесены с функциями совета директоров, комитетов при совете, служб внутреннего контроля и аудита, корпоративного секретаря и общего собрания акционеров.

Научная новизна работы состоит в обосновании методического подхода к применению цифрового инструментария, в котором состав и допустимость инструмента определяются функцией органа и достигнутым уровнем его цифровой зрелости, а не техническим типом решения. Ядро подхода составляет правило соответствия инструмента функции и уровню зрелости с закреплением контура контроля, а функциональная классификация инструментария связывает инструмент, специфический риск и контур контроля. Показано, что источником специфических рисков выступает несоответствие между уровнем цифровой зрелости процесса и сложностью внедряемого инструмента.

Практическая значимость результатов состоит в том, что предложенный подход применим советом директоров, комитетами при совете, службами внутреннего контроля и аудита, риск-менеджментом и корпоративным секретарем при выборе и разграничении цифровых инструментов с учетом функции органа и уровня цифровой зрелости, при разработке регламентов цифрового взаимодействия и электронного документооборота, а также при оценке рисков цифровизации.

Полученные результаты показывают, что эффективность цифрового инструментария в корпоративном управлении определяется не самим фактом внедрения, а соответствием инструмента функции органа и достигнутому уровню цифровой зрелости.

Список литературы

1. Гурдюмов С.А. Систематизация и классификация цифровых технологий по характеру их влияния на функции и процессы органов управления и контроля публичных компаний // Экономика строительства. 2026. № 3. С. 170–172. EDN: RQEKEA;
2. Данилова О.В. Цифровизация экономики и современные тенденции изменения модели управления корпоративной собственностью // Вестник Тверского государственного университета. Серия: Экономика и управление. 2021. № 1 (53). С. 50–58. DOI: 10.26456/2219-1453/2021.1.050-058;
3. Ильина И.Ю., Ильин А.Б., Зенкина Е.В. Разработка теории и методов принятия решений в корпоративном управлении в условиях цифровизации // Вестник Сыктывкарского государственного университета. 2023. Т. 3, вып. 4. С. 497–508;
4. Кодекс корпоративного управления: письмо Банка России от 10 апреля 2014 г. № 06-52/2463;
5. Юхно А.С. Совет директоров организации и корпоративное управление ИКТ // Управленческие науки. 2022. Т. 12, № 1. С. 17–31. DOI: 10.26794/2304-022X-2022-12-1-17-31;
6. Brochet F., Chychyla R., Ferri F. Virtual Shareholder Meetings // Management Science. 2024. Vol. 70, No. 9. P. 5896–5930. DOI: 10.1287/mnsc.2023.4946;
7. Brynjolfsson E., McAfee A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York: W.W. Norton & Company, 2014. 306 p;
8. Chan D.Y., Vasarhelyi M.A. Innovation and practice of continuous auditing // International Journal of Accounting Information Systems. 2011. Vol. 12, No. 2. P. 152–160. DOI: 10.1016/j.accinf.2011.01.001;
9. Deloitte. Uncovering the connection between digital maturity and financial performance. Deloitte Insights, 2020;
10. ENISA Threat Landscape 2023. Heraklion: European Union Agency for Cybersecurity, 2023;
11. Gale M., Bongiovanni I., Slapnicar S. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead // Computers & Security. 2022. Vol. 121. Art. 102840. DOI: 10.1016/j.cose.2022.102840;
12. Mertens F. The Use of Artificial Intelligence in Corporate Decision-Making at Board Level: A Preliminary Legal Analysis: SSRN Working Paper. 2023. SSRN ID: 4339413;
13. OECD. Digital Security Risk Management for Economic and Social Prosperity. Paris: OECD Publishing, 2015. DOI: 10.1787/9789264245471-en;
14. OECD. G20/OECD Principles of Corporate Governance 2023. Paris: OECD Publishing, 2023. DOI: 10.1787/ed750b30-en;

15. OECD. OECD Corporate Governance Factbook 2025. Paris: OECD Publishing, 2025. DOI: 10.1787/f4f43735-en;
16. Schwartz-Ziv M., Weisbach M.S. What do boards really do? Evidence from minutes of board meetings // *Journal of Financial Economics*. 2013. Vol. 108, No. 2. P. 349–366. DOI: 10.1016/j.jfineco.2012.04.011;
17. Verhoef P.C., Broekhuizen T., Bart Y. et al. Digital transformation: a multidisciplinary reflection and research agenda // *Journal of Business Research*. 2021. Vol. 122. P. 889–901. DOI: 10.1016/j.jbusres.2019.09.022;
18. Vial G. Understanding digital transformation: a review and a research agenda // *The Journal of Strategic Information Systems*. 2019. Vol. 28, No. 2. P. 118–144. DOI: 10.1016/j.jsis.2019.01.003;
19. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: WEF, 2025.

Об авторе:

ГУРДЮМОВ Сергей Александрович – аспирант кафедры Корпоративных финансов и корпоративного управления, факультета Экономики и бизнеса, направления подготовки “Менеджмент”, ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», г. Москва (125167, г. Москва Ленинградский пр-т, д. 49/2), e-mail: sgurd007@gmail.com; ORCID: 0009-0006-5512-0079, Spin-код: 7026-2853

Digital tools in the corporate governance system: approaches and specific risks

S.A. Gurdyumov

Financial University under the Government of the Russian Federation, Moscow

The article addresses the application of digital tools in the activities of the governing and control bodies of public companies. The relevance of the topic stems from the fact that digital solutions are being introduced into the work of boards of directors, board committees, internal control and audit services and the corporate secretary faster than ordered notions take shape about the correspondence of tools to the functions of these bodies and about the risks they generate. The aim of the article is to substantiate a methodological approach that links the choice of a digital tool to the function of a governing or control body and to the achieved level of its digital maturity, and that classifies the specific risks associated with the use of such tools. The study was carried out using methods of analysis of academic literature and regulatory sources, comparison, systematization and classification. The article distinguishes the concepts of digitalization, digital transformation and digital tools; typical digital tools are matched to the functions of governing and control bodies; a methodological approach is substantiated, based on the rule of correspondence of a tool to the function of a body and to the level of digital maturity and on the definition of a control contour; specific risks that cannot be reduced to technical

risks of information technology are systematized. The scientific novelty lies in the fact that digital tools are classified by the functions of governing and control bodies and linked to the level of digital maturity and the control contour, while a mismatch of a tool to the function and the maturity level is considered a source of specific risks of digitalization.

Keywords: *digital tools, digital transformation, digital maturity, board of directors, internal control, internal audit, control contour, specific risks.*

About author:

GURDYUMOV Sergey Aleksandrovich – graduate student of the Department of Corporate Finance and Corporate Governance, Faculty of Economics and Business, direction of training “Management”, FGOBU VO “Financial University under the Government of the Russian Federation”, Moscow (125167, Moscow, Leningradsky Prospekt, 49/2), e-mail: sgurd007@gmail.com; ORCID: 0009-0006-5512-0079, Spin code: 7026-2853

Статья поступила в редакцию 01.01.2026

Статья подписана в печать 15.09.2026