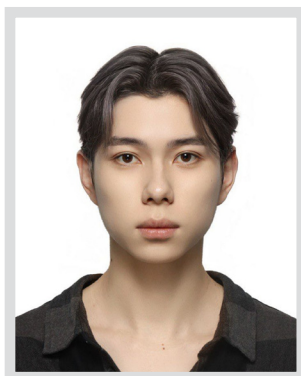


УДК 32.01

DOI: 10.24412/1998-5533-2026-1-243-253

### Способы управления политическими рисками в гибридных режимах цифровой власти



**Хван Данил Андреевич**

Независимый исследователь

*Цифровое развитие современной политики привело к тому, что смешанные формы власти сталкиваются с расширением возможностей контроля и ростом непредсказуемых угроз. Актуальность исследования определяется тем, что цифровая среда меняет механизмы политического управления быстрее, чем традиционные институты способны к адаптации, что приводит к появлению новых типов рисков в деятельности акторов власти. Цель работы заключается в выявлении способов, посредством которых смешанные (гибридные) политические режимы стремятся уменьшить политические риски, возникающие в цифровой среде. Для достижения цели решаются задачи анализа природы цифровых угроз, определения их структурных последствий для политической системы и обоснования подходов, применяемых властью для их нейтрализации. Научная и практическая значимость исследования состоит в том, что работа предлагает целостный взгляд на взаимодействие цифровых технологий и политических институтов, позволяет понять, как технические решения перестраивают процессы управления. Представленные результаты показывают, что власть использует три основных способа: институциональное дублирование, алгоритмическая фильтрация и символическая легитимация рисков. Эти способы обеспечивают временную стабилизацию, однако сопровождаются накоплением скрытых проблем, снижением доверия и возникновением рисков второго порядка. Научная новизна исследования заключается в концептуализации цифрового управления рисками как циклического процесса, в котором техническое подавление угроз сочетается с их дальнейшим воспроизводством. В работе обосновывается, что цифровые методы позволяют сглаживать отдельные проявления нестабильности, однако не устраняют первопричины рисков и со временем формируют зоны, делающие политический режим более чувствительным к новым вызовам. Полученные выводы уточняют представления о природе цифровой устойчивости и расширяют инструментарий анализа современных политических систем.*

**Ключевые слова:** цифровая политическая среда, политические риски, гибридные режимы, алгоритмическое управление, институциональное дублирование, общественное доверие, символическая интерпретация кризисов

**Для цитирования:** Хван Д.А. Способы управления политическими рисками в гибридных режимах цифровой власти // Вестник экономики, права и социологии. 2026. № 1. С. 243–253. DOI: 10.24412/1998-5533-2026-1-243-253.

Масштабная цифровизация кардинально усложняет политику, обеспечивая власти беспрецедентные технические ресурсы и одновременно порождая новые угрозы. В начале 2020-х гг. в он-

лайн-пространство переместилось около двух третей человечества [1]. Государственные структуры получают доступ к массивам *Big Data*, системам наблюдения и аналитическим алгоритмам, которые теоретически позволяют им реализовать своего рода «цифровой Паноптикум» с полным контролем над обществом. Одновременно цифровая среда создаёт бесконтрольные каналы коммуникации, через которые стихийно распространяются политические настроения, протестная мобилизация и дезинформация. Такая двойственность означает, что усиление технической оснащённости власти сопровождается ростом политических рисков.

Противоречие между технологическим всемогуществом и утратой управляемости проявляется в политической практике гибридных режимов. С одной стороны, авторитарно-ориентированные правительства активно используют цифровые платформы для наблюдения и влияния на общество, пытаясь подавлять оппозиционные дискурсы с помощью цензуры и алгоритмов. С другой стороны, сами цифровые технологии становятся источником нестабильности: онлайн-пространство генерирует проблемы, которые невозможно полностью нейтрализовать силовыми методами. В 2023 г. власти разных стран отключали интернет 283 раза в ответ на кризисные ситуации – это рекордное число подобных случаев, на 41 % превышающее показатели предыдущего года [2]. Данный факт свидетельствует о том, что, даже усиливая контроль над цифровой сферой, режимы сталкиваются с новыми вызовами для своей легитимности и общественного порядка.

В этих условиях актуальным становится исследование политических рисков гибридных режимов цифровой эпохи и разработка методов их управления. Цель настоящего исследования – выявить и проанализировать способы, которыми властные элиты гибридных режимов пытаются минимизировать политические риски в цифровой среде. Рассмотрение данных способов с позиций политической социологии позволит оценить их эффективность и побочные эффекты, включая возникновение новых зон уязвимости для самих политических режимов.

Гибридный политический режим традиционно понимается как смешанная система, сочетающая в себе авторитарные и демократические институты. Ещё в начале 2000-х гг. политологи отмечали рост числа таких промежуточных режимов, не укладывающихся в дихотомию «демократия vs диктатура». Классические типологии (Д. Истон, Х. Линц, С. Левицкий и др.) исходили из институциональных критериев (степени политической конкуренции и политического участия) для разграничения демократий, автократий и переходных форм государственного управления. Однако современная цифровая среда требует переосмысления этих категорий. В условиях платформенной коммуникации власть получает

новые источники ресурсов и новые ограничения, что меняет сам характер гибридности. Гибридный режим в цифровом измерении – это качественно иная конфигурация, в которой цифровые платформы интегрированы в структуру государственной власти [3].

Цифровое измерение гибридности проявляется во «вложенности» власти в глобальные сети и алгоритмы. В настоящее время наблюдается глубокая гибридизация функций государства и цифровых корпораций, которая приводит к трансформации политических режимов [4]. Государственные институты передают часть своих функций частным платформам – от сбора данных до модерации политической коммуникации, в результате чего, размываются границы между публичной властью и технологиями, когда корпорации приобретают черты новых политических акторов, способных влиять на повестку дня и поведение граждан (например, И. Маск и его компания в США). Вместе с тем происходит институциональное дублирование, когда цифровые платформы начинают выполнять роль каналов обратной связи, ранее свойственную только государственным структурам. Таким образом, цифровая гибридность выражается в одновременном сосуществовании традиционных институтов и сетевых механизмов управления, образующих единую систему.

Признаками гибридного режима цифровой эпохи становятся платформенная модификация власти и сетевое опосредование политических процессов. Во-первых, алгоритмизация власти позволяет режимам применять корпоративные технологии предиктивной аналитики, фильтрации информации и ранжирования контента для управления общественным мнением [5]. Во-вторых, появляются гибридные акторы (например, владельцы крупных социальных сетей или разработчики популярных приложений, обладающие властным ресурсом, сопоставимым с государственным). В-третьих, политические практики все более переносятся в «фиджитал»-пространство (*phygital*), т.е. в такое пространство, в котором границы между онлайн- и офлайн-активностью размыты [6]. Граждане вовлечены в политические взаимодействия посредством цифровых интерфейсов, тогда как власть стремится контролировать эти цифровые интерфейсы. В совокупности эти черты указывают на то, что гибридный режим в цифровом измерении – это система власти, которая опирается и на институты государства, и встраивается в цифровую инфраструктуру, что радикально меняет механизмы легитимации и управления.

Цифровая среда порождает целый спектр политических рисков, с которыми сталкиваются гибридные режимы. Эти риски можно условно разделить на институциональные, репутационные, управленческие, правовые и поведенческие.

Институциональные риски связаны с размыванием роли традиционных институтов и возможной

утратой ими функциональной состоятельности. Передача государством части своего функционала цифровым корпорациям чревата тем, что государственные служащие теряют компетенции в важных сферах. Возникает опасность паралича классических механизмов принятия решений, если фактическая власть смещается к алгоритмам и платформам.

Репутационные риски проявляются в подрыве доверия к политическому режиму вследствие цифровой прозрачности и быстрых информационных кампаний. Падение доверия к выборам и обвинения власти в фальсификациях распространяются мгновенно через социальные сети, ведя к делегитимации режимов. Любой скандал или ошибка власти моментально выходит в публичное пространство, что формирует постоянную угрозу репутационным потерям.

Управленческие риски цифровой эпохи заключаются в потере контролируемости и эффективности государственного управления. Традиционные бюрократические модели оказываются слишком медленными и «реактивными» для того, чтобы адекватно реагировать на стремительные цифровые изменения. Сложные алгоритмы, внедряемые для принятия решений, могут давать сбои или приводить к непредвиденным эффектам. Например, внедрение систем автоматизированной аналитики способно избавить от части нагрузки, но одновременно рискует навязать предвзятые решения, если алгоритмы обучены на искажённых данных. В совокупности это создаёт риск управленческих просчётов, которые труднее предвидеть и исправить.

Правовые риски обусловлены отставанием нормативно-правовой базы от технологической практики. Законодательство зачастую не успевает охватывать новые явления (от дипфейков до утечек данных), что создаёт зоны правовой неопределённости [7]. Государство само иногда прибегает к неправовым действиям для контроля цифровой сферы, чем подрывается принцип верховенства закона и порождаются риски для собственной легитимности [8].

Наконец, поведенческие риски связаны с трансформацией массового политического поведения под влиянием цифровых технологий. С одной стороны, возникают феномены «слактивизма» (диванного активизма) и поверхностной онлайн-активности, которые снижают реальное участие граждан в политике. С другой стороны, цифровая среда облегчает радикализацию и экстремизм, что позволяет экстремистским группам распространять призывы и координировать действия анонимно. Власть сталкивается с непредсказуемыми всплесками протестов, спровоцированных вирусным контентом или с массовым уклонением граждан от участия в институтах (например, бойкот выборов), что угрожает стабильности политики [9]. Как отмечал ещё В.Я. Гельман, «политические институты (как вновь соз-

данные, так и унаследованные от прежнего режима) играют двоякую роль в процессе смены режимов. Во-первых, они меняют характер распределения ресурсов между элитами, способствуя равенству сил либо одностороннему преобладанию. Во-вторых, от их эффективности зависит уровень неопределённости, а тем самым – и представления акторов об относительной цене стратегий» [10, с. 104].

Каждый из указанных типов рисков способен проявиться отдельно, однако чаще они взаимосвязаны. Например, управленческий просчёт при внедрении цифровой системы может перерасти в репутационный скандал и подорвать доверие (репутационный риск), а попытка закрыть проблему кулуарно создаст правовые коллизии. Поэтому классификация рисков носит аналитический характер – в реальности гибридные режимы сталкиваются с комбинированными вызовами. В то же время осознание многообразия и взаимосвязи политических рисков есть необходимое условие для поиска способов их эффективного управления в цифровой среде.

Основываясь на этом, далее можно выделить три основных способа управления политическими рисками в гибридных режимах цифровой власти: институциональное дублирование, алгоритмическая фильтрация и символическая легитимация рисков.

Институциональное дублирование. Одной из стратегий управления рисками в условиях цифровой неопределённости становится институциональное дублирование, то есть создание параллельных цифровых структур для контроля проблемных ситуаций и каналов обратной связи. Гибридные режимы пытаются встроить гражданскую активность в управляемое русло, открывая электронные приемные, платформы для жалоб и имитируя общественные советы в онлайн-формате. Считается, что если предоставить населению официальный цифровой канал выражения недовольства, то можно заранее выявить и нейтрализовать назревающие конфликты [11]. Например, в Турции создан президентский коммуникационный центр *CİMER*, через который граждане могут подавать жалобы и запросы онлайн; он принимает миллионы обращений в год и позиционируется как механизм участия общества в управлении [12]. Подобные платформы институционально дублируют функции традиционных органов (приемных, общественных приемов, консультативных советов), однако действуют в цифровой среде с высокой скоростью обработки обращений.

*Институциональное дублирование* призвано повысить оперативность реакции власти и снизить накал протестной активности. Так, электронные порталы обращений позволяют властям отслеживать наиболее острые проблемы в режиме реального времени и точно реагировать до возникновения каких-либо проблем. Более того, публичная демонстрация таких цифровых инициатив создает

эффект присутствия государства «рядом» с гражданами, что, безусловно, повышает степень заботы о гражданах [13]. Например, вместо несанкционированных митингов граждане направляют петиции через официальный сайт и спокойно ожидают ответа в установленном порядке. Таким образом достигается стабилизация за счёт перенаправления недовольства из офлайн в онлайн-бюрократию.

Однако описываемый способ несёт и риски ритуализации обратной связи. Когда цифровые каналы существуют формально, а решения по обращениям принимаются все равно по усмотрению власти, доверие граждан может постепенно подрываться. Институциональное дублирование может превратиться в имитацию диалога, когда обращения принимаются и даже публикуются статистические отчёты об их количестве, однако существенные проблемы остаются нерешёнными [14]. В конечном итоге цифровые приемные начинают выполнять функцию «парового клапана» – выпускают пар общественного недовольства, не влияя на политику. Данный подход чреват консервацией скрытых конфликтов. Население привыкает к тому, что можно пожаловаться в интернете, но реальные изменения не происходят, отчего цинизм и отчуждение только усиливаются. Следовательно, институциональное дублирование эффективно снижает остроту рисков в краткосрочной перспективе, но без подкрепления реальными реформами со временем утрачивает легитимность и может привести к ещё большей фрустрации общества.

Алгоритмическая фильтрация. Другой ключевой стратегией является алгоритмическая фильтрация политически значимой информации и активности. Так, политические режимы западных стран всё чаще внедряют автоматизированные системы мониторинга социальных сетей, анализ больших данных и машинное обучение для прогнозирования и предварительной нейтрализации угроз. Алгоритмы позволяют выявлять «тревожные сигналы» (экстремистские призывы, координацию протестов, всплески недовольства) ещё на ранней стадии и принимать упреждающие меры. Например, внедрение технологий ранжирования контента и модерации комментариев предоставляет возможность «сглаживать» острые дискуссии и ограничивать охват радикальных призывов. По сути, традиционная репрессивная логика заменяется цифровыми алгоритмами – вместо прямой цензуры и силового подавления власть предпочитает невидимым образом управлять информационными потоками.

*Алгоритмическая фильтрация* выражается в разнообразных практиках. Во-первых, это автоматическое удаление или сокрытие нежелательного контента на цифровых платформах. Государство через давление на технологические компании или посредством собственных ботов и технических средств добивается того, чтобы оппозиционные по-

сты, призывы к протестам или разоблачительные материалы либо не попадали в тренды, либо оперативно блокировались. Во-вторых, на практике, особенно в США, применяется предиктивное программирование, когда алгоритмы анализируют поведение пользователей и прогнозируют, кто может стать источником «рискованной» активности [11]. Таких пользователей берут под особое наблюдение, их сообщения помечаются и при необходимости блокируются ещё до того, как приобретут вирусную популярность. В-третьих, ограничивается глубина критики – рекомендательные системы намеренно не рекомендуют пользователям контент, чрезмерно критикующий власть, что создаёт эффект «тихого редактирования» общественной повестки. Как отмечают эксперты, алгоритмизация власти приводит к существенной гибридации функций государства и IT-корпораций, когда технические системы фактически исполняют задачи цензуры и пропаганды [11].

Главное преимущество данного способа – невидимость и повсеместность. Большая часть населения может не осознавать, что информационная среда уже отфильтрована – новости выглядят обыденно, радикальные призывы не встречаются, негативные комментарии тонут среди положительных. Таким образом, потенциальный конфликт смягчается до того, как оформится в явном виде.

Однако и здесь есть побочные эффекты. Алгоритмическая фильтрация приводит к имитации стабильности, а не к решению глубинных проблем, что характерно, скажем, для стран ЕС [6]. Она ограничивает общественную дискуссию, подавляет как деструктивные, так и конструктивные критические сигналы. Кроме того, алгоритмы не лишены предубеждений и сбоев. Если автоматизированная система обучена на данных с существующей дискриминацией, она может начать блокировать контент определённых социальных групп, усиливая раскол в обществе. Бывают случаи и ошибочных действий алгоритмов, когда под ограничения попадают случайные или нейтральные высказывания [4]. Всё это способно порождать новые риски: скрытая цензура стимулирует развитие альтернативных каналов (например, ухода оппозиции в зашифрованные мессенджеры или даркнет), тогда как ошибки алгоритмов – возмущение уже лояльных граждан. Следовательно, хотя алгоритмическая фильтрация представляет собой мощный инструмент упреждающего управления рисками, её чрезмерное применение чревато снижением качества обратной связи и злоупотреблениями технологиями.

*Символическая легитимация рисков.* Третий заметный подход гибридных режимов к управлению угрозами – символическая легитимация рисков, то есть особая стратегия публичной риторики, оформляющая появляющиеся проблемы в выгодном для власти свете. В данном случае политический ре-

жим не столько устраняет риск, сколько меняет его восприятие обществом с помощью пропаганды. Политически опасные ситуации интерпретируются официальными лицами как результат внешнего вмешательства, технического сбоя или отклонения работы платформ, что тем самым как бы снимает ответственность с внутренних институтов власти [15]. Например, массовые протесты могут объявляться следствием «внешнего давления» – инцидентов иностранных государств или глобальных ИТ-корпораций, которые манипулируют сознанием граждан. Широко используется нарратив о «цветных революциях», инспирируемых из-за рубежа, что перекладывает фокус с внутренних проблем на внешних врагов [16]. Подобные нарративы не только смещают фокус с внутренних проблем, но и часто игнорируют или искажают экономические причины социального недовольства [17].

Когда имеет место утечка данных или сбой в государственной информационной системе, официальный дискурс представляет это как «техническую ошибку», т.е. умаляет политическое значение инцидента и внушает, что намеренного провала в работе институтов нет, что, в частности, характерно для политики недружественных стран. Когда же в публичном поле выявляются искажения информации (например, распространение фейковых новостей), их нередко называют «платформенным искажением», обвиняются алгоритмы социальных сетей или анонимных злоумышленников, тогда как недоработки власти «остаются за кадром».

Символическая легитимация рисков выполняет сразу несколько задач:

– формирует объяснения, удобные для лояльной аудитории. Гражданам предлагается понятная картина (виновники всех неприятностей – внешние силы или неконтролируемые технологии, государство остается защитником правопорядка), что позволяет сохранить базовый уровень доверия;

– ритуализирует реагирование на риски. Каждый новый кризис сопровождается повторяющимся риторическим обрядом (поиском внешнего врага, заявлением о расследовании «сбоя» и заверением, что выводы будут сделаны). В итоге складывается иллюзия контроля, когда риски вроде бы признаны и помещены в рамку понятного нарратива, хотя реально их причины могут оставаться нетронутыми;

– позволяет перераспределить ответственность за негативные события. Вместо признания ошибок правительства вина возлагается на «технологии» или «агентов влияния», тогда как сама власть выступает в роли пострадавшей стороны, вынужденной устранять чужие козни, что укрепляет внутреннюю солидарность элит и части общества против «нарисованного» общего противника.

Хотя обозначенный способ часто эффективен в краткосрочной перспективе (особенно при кон-

троле над СМИ), у него есть явное ограничение. Так, постоянное «списывание» проблем на внешние силы и технические факторы со временем начинает выглядеть неправдоподобно и снижает общий уровень доверия к официальному дискурсу. Если каждое чрезвычайное положение или острая ситуация объявляется случайностью или происками врагов, граждане могут сделать вывод о некомпетентности властей, которые якобы не способны ни предотвратить вмешательство, ни наладить надежную работу систем [7].

Кроме того, борьба с «внешними угрозами» нередко сопровождается усилением репрессий и изоляции (цензура под предлогом суверенитета, давление на неправительственные организации и независимые медиа как «агентов иностранного влияния»), что в долгосрочном плане ослабляет общественные институты. Следовательно, символическая легитимация – это паллиативный метод, маскирующий риски под удобными ярлыками. Он помогает выиграть время и сохранить лицо политическому режиму, однако не устраняет ни самих угроз, ни причин их возникновения. В целом это наблюдается в настоящее время во многих странах мира, особенно тех, которые стремятся сохранить власть «коллективного Запада».

Таким образом, учитывая рассмотренные способы, их можно соотнести с типами рисков и эффектами, что показано в таблице 1.

Анализ указанных способов показывает, что цифровое управление рисками приносит неоднозначные результаты. С одной стороны, каждый из методов предоставляет политическому режиму определённую «передышку» и снижает остроту непосредственной угрозы. Институциональное дублирование позволяет выпустить пар недовольства контролируемым образом, алгоритмическая фильтрация – уменьшить вероятность стихийной мобилизации, символическая легитимация – сохранить «лицо власти» в глазах лоялистов во время кризиса. В краткосрочной перспективе эти меры действительно стабилизируют политическую ситуацию, но эта стабильность носит во многом симуляционный характер. По сути, создаётся модель технологически стабилизированной нестабильности, когда видимое спокойствие поддерживается постоянными техническими и пропагандистскими интервенциями, не дающими конфликтам открыто проявиться. Однако причины конфликтов при этом не устраняются, а лишь маскируются под совокупностью цифровых решений.

Некоторые риски в рамках такой модели управления превращаются в «поглощённые», то есть временно нейтрализованные. Например, риск массового уличного протеста частично поглощается активностью на правительственных онлайн-платформах, когда недовольные пишут петиции вместо того, чтобы выходить на площадь.

**Соотнесение методов управления рисками с типами рисков и эффектами**

Способ управления риском	На какие риски нацелен	Механизм действия	Ожидаемые эффекты
Институциональное дублирование	Институциональные, поведенческие риски	Создание цифровых каналов обращений и контроля (электронные приёмные, онлайн-советы) для интеграции протестной активности в управляемое русло	Временная стабилизация за счёт снижения открытой конфронтации; ритуализация обратной связи, имитация участия
Алгоритмическая фильтрация	Поведенческие, репутационные риски	Превентивный контроль контента и коммуникаций посредством ИИ и алгоритмов (автоцензура, скрытие радикальных сообщений)	Сглаживание конфликтов, снижение публичной критики; имитация контроля над повесткой, скрытое подавление недовольства
Символическая легитимация	Репутационные, правовые риски	Публичное реоформление рисков как внешних либо случайных: пропагандистское объяснение кризисов без признания вины власти	Временное сохранение доверия через перевод стрелок на «врагов» и фактор случая; перераспределение ответственности, оправдание репрессивных мер

Источник: авторская разработка.

Риск репутационных потерь сглаживается информационными кампаниями, которые меняют тему обсуждения или находят оправдание случившемуся. Тем не менее другие риски сохраняются и, более того, способны усилиться внутри закрытой системы. Если власть перестаёт получать честные сигналы обратной связи из-за тотальной фильтрации информации, управленческие решения становятся менее адекватными, что накапливает институциональные проблемы. Подавленное и загнанное вглубь недовольство может привести к более мощному всплеску кризиса, когда внешние обстоятельства нейтрализуют цифровые барьеры (например, когда экономический шок выведет людей на улицы, и ни цензура, ни приемные уже не помогут).

Внимание здесь также следует обратить на контрпродуктивные эффекты цифрового управления рисками. Одним из них является рефлексивный риск, когда сами усилия по предотвращению угроз формируют новые угрозы. Применение сложных автоматизированных систем порождает зависимость государства от этих систем и тех, кто ими управляет. Появляется «теневая цифровая элита» – круг технических специалистов и администраторов платформ, которые концентрируют реальную власть и остаются вне публичной ответственности. Делегируя алгоритмам контроль над коммуникацией, власть потенциально теряет часть суверенитета. Другой пример рефлексивного риска – эффект деполитизации общества. Чрез-

**Таблица 1** мерный акцент на технологическом контроле отчуждает граждан от политики, и они перестают верить в возможность влиять на решения и уходят в частную жизнь, что снижает открытое давление на власть, хотя также лишает режим важнейшего ресурса – общественной поддержки и легитимации «снизу». Как следствие, система становится хрупкой – при минимальном стресс-факторе, когда технологии дадут сбой или появится новая непредвиденная угроза, пассивное и отчужденное общество или взорвётся протестом, или не поддержит власть в критический момент.

В целях обобщения можно описать цикл управления цифровыми политическими рисками в гибридном режиме, который визуализирован на рисунке 1.

На первом этапе власть фиксирует возникающую угрозу (например, всплеск недовольства, скандал



**Рис. 1. Цикл управления цифровыми политическими рисками (авторская разработка)**

в сети, утечку данных) с помощью систем мониторинга. Затем следует этап интерпретации риска – решается, считать ли проблему технической, политической или внешней.

В зависимости от этого запускается один из рассмотренных способов – или перевод проблемы во внутренний управляемый канал (институциональное дублирование), или её технократическая нейтрализация (алгоритмическая фильтрация), или пропагандистская кампания по объяснению (символическая легитимация). Каждый из способов приводит к временной стабилизации ситуации, после чего наступает фаза перераспределения ответственности и последствий. Например, если риск обставлен как внешняя угроза, ответственность смещается на врага; если снят алгоритмом – на случайный сбой.

Власть на короткое время извлекает выгоду, однако цикл завершается возвращением латентного риска: нерешённая проблема остаётся в системе, и при новом проявлении запускается следующий цикл. Данная модель наглядно показывает, что без качественно новых, институциональных решений управление рисками превращается в бесконечное повторение одних и тех же мер, постепенно уменьшающих свою эффективность.

Однако в целом попытки гибридных режимов управлять рисками с опорой на цифровые технологии неизбежно порождают рефлексивные риски. Данный концепт, восходящий к теории У. Бека о рефлексивной модернизации, означает, что чем более развитой становится система управления рисками, тем больше она сама производит новых, побочных рисков. В политико-управленческом контексте это проявляется особенно остро. Когда государство вводит сложные системы контроля (массовую слежку, автоматизированное принятие решений, блокировки интернета), оно должно учитывать, что эти же меры могут дать обратный ожидаемому эффект. Например, стремясь обезопасить себя от массовых протестов путем тотального мониторинга, режим достигает только временного подавления активности, зато формирует у населения накопленное чувство фрустрации. Люди осознают наличие невидимой цензуры и надзора, что переводит недовольство на новый уровень – недоверие к самой системе управления рисками.

Парадокс здесь состоит в том, что чем более активно власть старается исключить любые случайности и угрозы, тем более хрупкой она становится перед лицом неизбежной неопределённости. Реализация цифровых мегапроектов управления нередко приводит к избыточной уверенности элит в своей защищённости. По сути, это проявление «парадокса симуляционного контроля», когда власти убеждены, что раз у них есть данные и алгоритмы, они контролируют ситуацию, однако фактически они видят только то, что позволяют видеть настроенные ими

фильтры. В долгосрочной перспективе попытка свести управление политическими рисками к технической задаче оборачивается потерей чувствительности к реальным социальным процессам. Более того, жестко заданные алгоритмы начинают распространять системные ошибки. Если, допустим, правоохранительные органы ориентируются на автоматизированные аналитические отчеты о «зонах риска» в обществе, они могут игнорировать проблемы, не попавшие в метрики, или преследовать невиновных, ошибочно отмеченных системой. Таким образом, рефлексивный риск проявляется и в виде новых уязвимостей (зависимость от техники, утечки данных, саботаж со стороны администраторов систем), и в виде самоусиления старых проблем под другим видом (например, рост коррупции через цифровые инструменты, когда данные используются для избирательного давления).

Показательным является и то, что рефлексивный риск наиболее силён в условиях симуляционного контроля, когда власть имитирует решение проблем. Техническое вытеснение человеческого фактора и общественной дискуссии из процессов принятия решений означает, что рано или поздно реальность вырывается наружу. Проблемы, считавшиеся устранёнными благодаря отчётам и фильтрам, могут внезапно «заявить о себе» и принять лавинообразный характер. Классический пример – неожиданный массовый взрыв недовольства по «незначительному» поводу в обществе, в котором долгие годы господствовала видимая стабильность. Такого рода события (например, «арабская весна» 2011 г., начавшаяся с единичного акта отчаяния, или протесты в Казахстане 2022 г., вызванные резким повышением цен) показывают, что полное подавление симптомов не равно излечению болезни. Следовательно, проблема рефлексивного риска ставит под сомнение устойчивость чисто технологических стратегий, которые могут краткосрочно укреплять контроль, однако стратегически повышают неопределённость, с которой режиму рано или поздно придётся столкнуться, поскольку вся история, по сути, циклична.

В этом смысле важно проследить соотношение цифрового управления рисками с доверием. Так, цифровые методы политического контроля оказывают сложное воздействие на уровень доверия в обществе. С одной стороны, применяя высокотехнологические решения, власть стремится укрепить доверие граждан к своей эффективности и современности. Формально запускаются электронные сервисы, демонстрируется открытость данных, утверждается имидж «цифрового прогресса». Однако парадоксально, что техническое управление без полноценной обратной связи снижает подлинное доверие, на котором зиждется легитимность режима [11]. Причина этого заключается в отчуждении граждан от политического процесса. Когда люди

видят, что власть предпочитает алгоритмы вместо живого диалога и что их активность направляется в имитационные структуры, возникает недоверие к мотивам власти. Фактически симулякры гражданской активности, создаваемые властями из-за боязни собственного народа, консервируют проблемы и выводят их из повестки дня [6]. Граждане быстро улавливают инсценировку – если электронные голосования или обсуждения имеют predetermined исход, следующая их итерация уже не вызовет энтузиазма.

Кроме того, чрезмерно высокая ставка на технологии подрывает межличностное и институциональное доверие. В условиях «тотальной слежки» люди меньше доверяют друг другу, поскольку опасаются, что любое высказывание может быть зафиксировано и использовано против них. Парадоксально, однако и сам режим рискует потерять доверие к населению, так как власть начинает видеть в каждом гражданине потенциальный источник рисков, которого нужно мониторить и фильтровать. Взаимная подозрительность в отношениях «власть – граждане» несовместима с устойчивой легитимностью. Для легитимности требуется, чтобы граждане хотя бы минимально верили в добросовестность и компетентность власти, а власть – в лояльность основной массы населения. Цифровой контроль без подотчётности разрушает оба этих элемента. Недоверие властей к народу порождает репрессивные симулякры участия (как выше отмечалось, имитацию консультаций из страха перед реальным мнением граждан), тогда как недоверие граждан к власти приводит к тому, что даже полезные инициативы (например, цифровой сервис или приложение) воспринимаются скептически, как потенциальный инструмент слежки или манипуляции.

Эмпирические данные подтверждают, что падение доверия сопровождается процессом цифровой авторитарной эволюции режимов. Зачастую наблюдается феномен, когда население начинает больше доверять нейтральным техническим системам, чем официальным учреждениям [14]. Например, в литературе отмечается, что избиратели могут оказаться склонны верить результатам, выданным компьютером, больше, чем протоколам, подписанным членами избиркома [4], что говорит о серьёзном кризисе политического доверия; граждане предполагают, что машина менее пристрастна, чем человек, ассоциированный с властью. В краткосрочной перспективе власть может радоваться такому переносу в том смысле, что главные выборы признаны честными благодаря технике. Однако стратегически это свидетельствует о разрыве символической связи между народом и институтами. Восстановить её одними цифровыми средствами фактически невозможно.

Таким образом, без доверия цифровое управление рисками превращается в самоцель, которая

требует всё большего принуждения. Режим, потерявший кредит доверия, вынужден опираться только на контроль и страх, т.е., по сути, прямой путь к росту нестабильности при первом же ослаблении контроля. Следовательно, поддержание доверия – главный вызов, с которым нельзя справиться только техническими ухищрениями. Не случайно в успешных моделях управления рисками (например, в ряде демократий) делается упор на вовлечение общества и прозрачность [3].

Поэтому целесообразно сравнить цифровые и аналоговые подходы к управлению политическими рисками (табл. 2). Сравнение аналоговых и цифровых подходов показывает, что цифровизация приносит как новые инструменты, так и изменяет природу самой стабильности режима. Возникает феномен технологически стабилизированной нестабильности, который означает, что режим сохраняет видимость устойчивости лишь при постоянной работе цифрового механизма контроля. Стоит этому механизму дать сбой или на горизонте появится не учтенный алгоритмами риск, как стабильность тут же оказывается под угрозой. Власть как бы «едет на велосипеде», который не может остановиться – требуются всё новые и новые технические ухищрения для балансирования, иначе система потеряет равновесие. Как следствие, формируется модель, противоположная классической легитимной стабильности.

Долгосрочные последствия такого положения включают институциональное вырождение и ухудшение способности системы к развитию. Режим, полагающийся лишь на цифровизацию, утрачивает навыки политической гибкости. Решения принимаются на основе удобных данных, обратная связь фильтруется, и в итоге стратегические ошибки накапливаются. Общество привыкает к тому, что инициативы «сверху» являются манипулятивными, и отвечает апатией или латентным сопротивлением.

При этом деградирует и политическая культура, поскольку граждане избегают открытой дискуссии, чиновники боятся брать ответственность без оглядки на «данные», что приводит к тому, что политический режим становится малочувствительным к слабым сигналам, пока те не превратятся в громкий кризис.

Можно говорить и о своеобразном провале адаптации. Цифровые технологии развиваются быстро, и общества в других странах учатся их использовать, в том числе для самоорганизации и давления на власть. Гибридный режим, закрепившись в своей имитационной практике, оказывается не готов к новому витку технологических изменений. Например, появление децентрализованных зашифрованных платформ, неподдающихся цензуре, или широкое распространение продвинутого ИИ среди населения может резко снизить эффективность прежних методов контроля [11]. Если режим не выстроил к этому

Таблица 2

## Цифровые и аналоговые подходы к управлению политическими рисками

Критерий	Аналоговый подход	Цифровой подход
Источник угрозы	Индивидуальные или групповые акторы, локальные события. Риски воспринимаются как обусловленные действиями конкретных людей (оппозиционных лидеров, протестных групп)	Структурные данные и сетевые процессы. Угроза фиксируется как абстрактный паттерн (тренд в социальных сетях, аномалия в больших данных) без явного личностного носителя
Реакция власти	Реактивные меры (силовое подавление протестов, точечные репрессии, цензура СМИ и прямые запреты). Вмешательство происходит после проявления риска, часто публично и ощутимо	Активные технические меры (упреждающая фильтрация контента, превентивное блокирование коммуникаций, алгоритмическое снижение охвата «опасных» тем). Вмешательство происходит до широкой огласки риска, незримо для общества
Обратная связь	Неформальные сигналы (слухи, уличные настроения, обращения посредством традиционных каналов (петиций, встреч с депутатами)). Возможна открытая критика, на которую власти реагируют интуитивно	Метрики и мониторинг (анализ социальных медиа, онлайн-опросы, показатели «социального режима»). Обратная связь сводится к числовым индикаторам (рейтинги одобрения, частота негативных упоминаний), часто без учёта качественного диалога
Нормативный статус	Действия власти опираются на явные законные полномочия или чрезвычайное положение. Ограничения вводятся указами, видимыми для общества (цензура по закону, комендантский час)	Используются серые зоны права и новые регуляции. Формально вводятся технические стандарты (например, обязательство локализации данных), которые де-факто дают широчайшие возможности контроля. Меры часто не прозрачны и трудно оспоримы юридически

Источник: авторская разработка.

времени институциональных каналов участия и не завоевал хотя бы частичного доверия, он столкнется с волной нестабильности, против которой его прежние цифровые инструменты окажутся, по сути, бесполезны. Таким образом, технологически стабилизированная нестабильность чревата тем, что любая внезапная инновация или экзогенный шок (будь то новый гаджет, кризис или вирусный контент) может спровоцировать дестабилизацию. Итоговый вывод здесь состоит в том, что цифровые способы управления политическими рисками усиливают контроль, однако не устраняют фундаментальных причин рисков и со временем даже усугубляют их. Режим, полагающийся лишь на технократическое подавление и симуляцию, рискует потерять «связь с реальностью», растратить ресурс доверия и оказаться незащищённым перед новым поколением вызовов. Иными словами, модель устойчивости, основанная на цифровых технологиях вне должной институциональной рефлексии, сама оказывается неустойчивой.

Таким образом, проведённый анализ показал, что в гибридных режимах цифровые способы управления рисками одновременно укрепляют контроль власти и ослабляют её чувствительность к политическим сигналам общества. Институциональное дублирование, алгоритмическая фильтрация и символическая легитимация позволяют быстро и относительно малозатратно гасить проявления нестабильности. Однако эти меры носят поверхностный характер – они откладывают или скрывают проблемы и создают только видимость безопасности режима. Более того, со временем назревают новые риски второго порядка (снижение доверия, технологические уязвимости, деградация институтов), которые

могут проявиться в ещё более острой форме. Другими словами, цифровой контроль – это паллиатив, который без учёта коррекции способен превратиться в источник долгосрочной нестабильности власти. Для обеспечения подлинной устойчивости стратегии технического управления рисками должны быть дополнены институциональной рефлексией и политическими реформами. Властям гибридных режимов необходимо как мониторить и подавлять, так и прислушиваться и адаптироваться. Реальное вовлечение граждан в выработку решений, восстановление механизма доверия, обновление легитимных каналов выражения интересов – всё это важно в цифровую эпоху. Без таких шагов режимы рискуют попасть в ловушку собственных технологий, когда контроль тотален, однако управление остаётся иллюзорным. Поэтому главной рекомендацией из проведённого исследования является необходимость сбалансировать цифровые и традиционные механизмы управления на основе укрепления как цифровой безопасности, так и общественного фундамента политической системы. Только при этом условии гибридные режимы смогут уменьшить политические риски при отсутствии новых угроз для собственного будущего.

## Литература:

1. Global Internet use continues to rise but disparities remain. UN Department of Economic and Social Affairs Social Inclusion. URL: <https://social.desa.un.org/sdn/global-internet-use-continues-to-rise-but-disparities-remain#:~:text=An%20estimated%205,ITU> (дата обращения: 30.11.2025).
2. Analysis. Digital Authoritarianism vs. Digital Democracy: Defending the Open Internet in an Era of Tech Fragmentation. Medium. The Diplomatic Pouch. URL: <https://medium.com/the-diplomatic-pouch/analysis-digital-authoritarianism-vs-f6ab4deb0910#:~:text=At%20midnight%20on%20the%20eve,From%20targeted%20surveillance%20of> (дата обращения: 30.11.2025).
3. Никифоров А.А. Особенности формирования гибридных рисков в российской публичной сфере // Социология власти. 2023. Т. 35. № 1. С. 219–241.
4. Поярков С.Ю. Модификация конституционных механизмов обеспечения стабильности в государстве в контексте трансформации современного конституционализма // Политика и общество. 2025. № 2. С. 242–261.
5. Куровский С.В., Зинчук М.Г., Мишин Д.А. Детерминанты российской политики в прибрежных странах Персидского залива // Казачество. 2025. № 82 (1). С. 156–165.
6. Володенков С.В., Федорченко С.Н., Артамонова Ю.Д. Социотехническая реальность цифрового пространства современной политики: структура и особенности // Политическая экспертиза: ПОЛИТЭК. 2022. Т. 18. № 3. С. 230–253.
7. Холоденко Ю.А. Цифровая трансформация государственного управления: возможности и риски // Вестник Московского университета. Серия 18. Социология и политология. 2022. Т. 28. № 3. С. 28–53.
8. Мишин Д.А., Куровский С.В., Сижажев А.Х. Понятие юрисдикции в национальном и международно-правовом аспектах // Юридическая наука. 2024. № 2. С. 247–251.
9. Мишин Д.А., Куровский С.В., Смолин П.В. Проблемы и перспективы развития отечественного конституционализма // Современное общество и право. 2024. № 4 (71). С. 45–50.
10. Гельман В.Я. Из огня да в полымя (динамика постсоветских режимов в сравнительной перспективе) // Полис. Политические исследования. 2007. № 2. С. 81–108.
11. Победин П.К. Формирование политических институтов и процессов с помощью цифровых технологий и искусственного интеллекта // Постсоветский материк. 2024. № 2 (42). С. 51–61.
12. Discipline and punish: how Turkey controls the internet. OSW (24.06.2025). URL: <https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-06-24/discipline-and-punish-how-turkey-controls-internet#:~:text=The%20Presidential%20Communication%20Centre%20his%20arrest%2C%20stemmed%20from%20an> (дата обращения: 30.11.2025).
13. Хорошкевич Н.Г. Классификация политических рисков государственных гражданских служащих // Гуманитарные, социально-экономические и общественные науки. 2021. № 5. С. 73–78.
14. Бордовских А.Н. Политические риски в условиях глобальных вызовов традиционным системам госуправления // Анализ и прогноз. Журнал ИМЭМО РАН. 2020. № 1. С. 63–73.
15. Володенков С.В., Федорченко С.Н. Традиционные политические институты в условиях цифровизации: риски и перспективы трансформации // Дискурс-Пи. 2022. Т. 19. № 1. С. 84–103.
16. Володенков С.В. Digital-технологии в системе традиционных институтов власти: политический потенциал и современные вызовы // Вестник Московского государственного областного университета. 2018. № 2. С. 39–48.
17. Манаширов Э.С. Математическое доказательство экономического иррационализма политики «социальной справедливости» // Экономическое развитие России. 2025. №10. С. 308–313.

## Ways to Manage Political Risks in Hybrid Regimes of Digital Power

*Khvan D.A.*

*The digital development of modern politics has led to the fact that mixed forms of government are faced with an expansion of control capabilities and an increase in unpredictable threats. The relevance of the study is determined by the fact that the digital environment is changing the mechanisms of political governance faster than traditional institutions are able to adapt, which leads to the emergence of new types of risks in the activities of government actors. The aim of the work is to identify ways in which mixed (hybrid) political regimes seek to reduce political risks arising in the digital environment. To achieve this goal, the tasks of analyzing the nature of digital threats, determining their structural consequences*

*for the political system and substantiating the approaches used by the authorities to neutralize them are being solved. The scientific and practical significance of the research lies in the fact that the work offers a holistic view of the interaction of digital technologies and political institutions, allows us to understand how technical solutions restructure management processes. The presented results show that the government uses three main methods: institutional duplication, algorithmic filtering and symbolic legitimization of risks. These methods provide temporary stabilization, but they are accompanied by the accumulation of hidden problems, a decrease in trust, and the emergence of second-order risks. The scientific novelty of the research lies in the conceptualization of digital risk management as a cyclical process in which the technical suppression of threats is combined with their further reproduction. The paper substantiates that digital methods make it possible to smooth out individual manifestations of instability, but they do not eliminate the root causes of risks and over time form zones that make the political regime more sensitive to new challenges. The findings clarify the understanding of the nature of digital sustainability and expand the tools for analyzing modern political systems.*

*Keywords: digital political environment, political risks, hybrid regimes, algorithmic management, institutional duplication, public trust, symbolic interpretation of crises*

