DOI 10.37882/2223-2974.2024.05.36

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЧАСТЬ КОРПОРАТИВНОЙ КУЛЬТУРЫ

## INFORMATION SECURITY AS PART OF CORPORATE CULTURE

***A. Trubin***
***E. Timofeev***

*Summary*. The article discusses the integration of information security into the corporate culture of modern enterprises as a critical element of sustainable development and competitiveness in the market. The aspects of developing strategic documents, including information security policies, and implementing a control system to minimize risks and prevent violations are highlighted. The legal framework for managing information flows and the need for a systematic approach to ensuring information security in organizations of various scales are analyzed. The importance of corporate culture in ensuring information security and the need for continuous development of the legislative framework in this area are emphasized.

*Keywords*: information security, corporate culture, risk management, strategic planning, legislative framework, systemic approach, violation control.

***Трубин Александр Евгеньевич***
*Кандидат экономических наук, доцент, НОЧУ ВО Московский финансово-промышленный университет «Синергия»*
*niburt@yandex.ru*
***Тимофеев Евгений Олегович***
*Аспирант, НОЧУ ВО Московский финансово-промышленный университет «Синергия»*
*teror1716@yandex.ru*

*Аннотация*. В статье рассматривается интеграция информационной безопасности в корпоративную культуру современных предприятий как критический элемент устойчивого развития и конкурентоспособности на рынке. Освещаются аспекты разработки стратегических документов, включающих политики информационной безопасности, и внедрения системы контроля для минимизации рисков и недопущения нарушений. Анализируются правовые основы управления информационными потоками и необходимость системного подхода к обеспечению безопасности информации в организациях различного масштаба. Подчеркивается значимость корпоративной культуры в обеспечении информационной безопасности и потребность в постоянном развитии законодательной базы в этой сфере.

*Ключевые слова*: информационная безопасность, корпоративная культура, управление рисками, стратегическое планирование, законодательная база, системный подход, контроль нарушений.

Информация представляет собой один из ключевых, стоимостных и склонных к быстрому устареванию активов в современном обществе. Ее роль и важность в общественных взаимоотношениях подчеркнуты законодателем через установление законодательных требований к содержанию и способам распространения различных видов информации. Для эффективного управления и принятия верных стратегических решений критически важны доступ к информации разной направленности и умение эффективно ею манипулировать в интересах организации. Владение информацией напрямую связано не только с профессиональным успехом специалистов на всех уровнях и процветанием предприятия, но также способствует прогрессу государства в целом.

Анализ правовых аспектов управления информационными потоками имеет как теоретическое, так и прикладное значение, учитывая их всеобъемлющее применение как среди субъектов экономической деятельности, так и в деятельности государственных структур. Это обусловлено потребностью в классификации и систематизации существующих нормативных документов для их эффективного применения на практике, а также необходимостью дальнейшего развития законодательной базы в этой области и улучшения практики ее применения.

В основе понятия «корпоративная культура» лежат идеи, впервые высказанные известным стратегом и фельдмаршалом Мольтке в 19 веке. Он предложил концепцию, которая позволила эффективно наладить взаимоотношения между офицерами, заполнив ниши, не охваченные уставами и официальными документами. В современном мире можно встретить разнообразные интерпретации данного термина, однако его сущность остается неизменной и заключается в наборе убеждений, традиций, этических норм и поведенческих правил, которые являются общими и обязательными для всех сотрудников организации.

Эти принципы способствуют тому, что коллектив работает слаженно, двигаясь к общей цели и чувствуя себя составной частью большого механизма. Без глубокого анализа формальной стороны вопроса можно отметить, что подобные ощущения присущи практически каждому сотруднику, независимо от масштабов компании, в которой он занят [6].

В рамках любой организационной структуры наблюдается существование специфических правил, признание которых является непреложным. Спектр развития корпоративной культуры охватывает широкий диапазон, начиная с практически минимального уровня и до-

стигая значительных высот. Диверсификация данных уровней корпоративной культуры обусловлена множеством факторов, присущих разнообразию самих организаций. В контексте масштабных корпораций, система управления и организационного функционирования формируется на основе практической необходимости, находя своё отражение в годами отлаженных методиках и стандартах, тогда как в среде малых предприятий подобный порядок носит скорее утилитарный характер. Разнообразие в методах закрепления и характере данных правил также заслуживает внимания: они могут быть зафиксированы в письменной форме, существовать в неписаном виде, исполняться на основе добровольной инициативы или под давлением обязательств.

В аспекте информационной безопасности корпоративная культура подразумевает важность наличия ответственности за нарушения, корреляцию такой ответственности с действующими законодательными нормами, а также подходы к реализации данной ответственности. В этом контексте особую роль играют механизмы мониторинга, контроля и проведения расследований, а также внедрение принципа неизбежности наказания. Совокупность этих факторов либо напрямую определяет, либо в значительной мере влияет на формирование корпоративной культуры предприятия.

В рамках настоящего исследования важно отметить, что ИБ в различных организационных контекстах подлежит значительным вариациям, определяемым спецификой деятельности каждой отдельно взятой организации. Такое многоаспектное рассмотрение ИБ предполагает анализ конкретных примеров, демонстрирующих разнообразие подходов к ее обеспечению.

В контексте организаций, функционирующих в сфере реальных временных платежных операций (например, платежные системы и с ними ассоциированные структуры), концепция ИБ неразрывно связана с обработкой финансовых потоков. В этом случае информационная безопасность прямо коррелирует с экономической выгодой, от которой зависит существование и успешное функционирование данных организаций. Риски в данном контексте носят ярко выраженный предпринимательский характер, поскольку непосредственно связаны с финансовыми результатами деятельности [9].

В противоположность этому, организации, деятельность которых классифицируется как критически значимая для обеспечения национальной безопасности и устойчивости государственного управления (например, объекты критической инфраструктуры), сталкиваются с кардинально иными вызовами в области ИБ [2].

В данном случае обеспечение информационной безопасности выступает как фундаментальное условие для осуществления их деятельности. Риски здесь представляются в более широком спектре, включая угрозы жизни и здоровью населения, защите государственной безопасности и предотвращении экологических катастроф. Следовательно, требования к ИБ в данных организациях носят строго обязательный характер, при этом отступление от них может привести к катастрофическим последствиям.

В контексте малого коммерческого предприятия, чья операционная деятельность не предполагает строгого соблюдения регулятивных норм или защиты результатов интеллектуальной деятельности, концепция ИБ не находит широкого признания среди сотрудников.

Основная задача такой коммерческой структуры заключается в генерации прибыли, и операции, направленные на достижение данной цели, не обусловлены необходимостью строгого следования принципам информационной безопасности, поскольку отсутствует давление со стороны регулирующих органов и выраженная потребность в таком следовании. В результате информационная безопасность воспринимается как излишняя нагрузка, несущая дополнительные финансовые издержки, и согласно механизмам рыночной экономики, она может быть исключена из рассмотрения в процессе деятельности предприятия [7].

В контексте анализа информационной безопасности в крупных коммерческих организациях можно утверждать, что данный аспект интегрируется в корпоративную культуру и структуру управления наравне с другими внутренними регулятивными механизмами, такими как правила внутреннего трудового распорядка и дресс-код. Информационная безопасность рассматривается не только как средство защиты данных и интеллектуальной собственности, но и как фундаментальный элемент обеспечения организационного порядка и эффективности процессов, присущих данной организации.

Эта интеграция информационной безопасности в корпоративные процессы может рассматриваться как создание специфической внутренней системы, имеющей собственные нормы, правила и методы контроля, аналогично функционированию государственных институтов в рамках общегосударственной системы. Таким образом, подход к информационной безопасности в крупных коммерческих организациях можно оценивать, как системно органичный, предполагающий её восприятие и реализацию как неотъемлемой части корпоративной культуры и управленческих процессов [10].

Изученные примеры демонстрируют крайние позиции, однако реальная ситуация обычно располагается на континууме между указанными экстремумами. Восприятие информационной безопасности в контексте

каждого анализируемого случая коррелирует с уровнем развития организации. В значительной мере, акцент на крупные организации обусловлен объективными факторами, которые ведут к тому, что вопросы, связанные с информационной безопасностью, оказывают непосредственное влияние на ключевые бизнес-процессы. Такое воздействие требует системного подхода к управлению соответствующими рисками.

Выбор стратегии оценки рисков в организации определяется не только размером компании, спецификой ведения бизнеса и уровнем информатизации бизнес-процессов, но и степенью зрелости организации. Управление рисками в сфере информационной безопасности превращается в ключевую бизнес-задачу, инициируемую владельцем предприятия на основе его осведомленности и понимания данных рисков. Ссылка на различные стандарты и методологии позволяет идентифицировать и описать все уровни зрелости организации, хотя дальнейшее их рассмотрение не является предметом данного анализа. Следует отметить, что, начиная с определенной стадии развития, процессы оценки и управления рисками интегрируются в систему управления организацией в целом.

Интеграция мероприятий по обеспечению ИБ в корпоративную культуру организации непременно коррелирует с первоначально определенными целями и бизнес-процессами данной организации. В случаях, когда такая инкорпорация не соответствует основным стратегическим направлениям деятельности организации, она может принимать форму действий, не имеющих непосредственного отношения к достижению ключевых целей организации, при этом влекущих за собой дополнительные затраты. В таком контексте, интеграция мероприятий по обеспечению информационной безопасности в корпоративную структуру может не обрести должного применения и, со временем, может быть прекращена или существенно пересмотрена в свете адаптации к стратегическим целям организации.

Далее следует рассмотреть ключевые аспекты прикладной взаимной интеграции ИБ и корпоративной культуры, выделив компоненты этой интеграции:

1. В организации должны быть разработаны и формализованы правила, направленные на обеспечение ИБ. Эти положения могут быть интегрированы в трудовые договора, правила внутреннего распорядка, должностные инструкции и другие корпоративные документы [8].
2. В структуре могут быть введены дополнительные мотивационные механизмы, стимулирующие соблюдение установленных правил поведения в сфере ИБ, в том числе через программы дополнительного премирования, не входящие в основной фонд заработной платы сотрудников [1].
3. Планирование среднесрочных перспектив развития предприятия обязано учитывать аспекты ИБ, преимущественно через процессы управления рисками [5].
4. Принцип неотвратимости наказания за нарушения в области ИБ должен быть реализован через систему контроля, выявления и расследования нарушений, которая включает в себя механизмы проверки как сотрудников, так и потенциальных контрагентов, а также процедуры по расследованию злоупотреблений и ошибок.
5. Стратегические документы, включая миссию, политики и концептуальные подходы организации, обязательно должны включать положения, касающиеся ИБ. Возможна разработка специализированных политик или концепций, посвященных исключительно этой теме [4].
6. Финансовое обеспечение, включая как оперативное, так и среднесрочное бюджетирование, должно предусматривать статьи, специально выделенные на обеспечение информационной безопасности. Существование отдельного бюджета на эти цели не является обязательным условием, однако важно, чтобы бюджеты организации были ориентированы на поддержку и развитие процессов информационной безопасности [3].

Подводя итоги настоящего исследования необходимо сформулировать следующие выводы. Корпоративная культура как часть ИБ, аналогично общей культурной парадигме организации, может быть, как предопределена базовыми установками («из коробки»), так и целенаправленно развиваться, и культивироваться через систематические усилия.

В контексте формирования и укрепления культуры информационной безопасности, ключевую роль играет вовлеченность и пример высшего руководства организации. Административный контингент не только инициирует и поддерживает стратегии и политики, направленные на обеспечение информационной безопасности, но и обеспечивает необходимое финансирование для их реализации, демонстрируя при этом личную приверженность установленным нормам и правилам.

Параллельно, сотрудники организации играют активную роль в адаптации и корректировке политик, инициированных руководством, способствуя формированию адекватного направления деятельности в области ИБ, что способствует эффективной интеграции механизмов защиты в стандартные бизнес-процессы предприятия. Важным аспектом является то, что каждый сотрудник, независимо от занимаемой позиции, стажа работы или иных характеристик, подчиняется унифицированным правилам в области информационной безопасности, несет равную ответственность и обязанности в отношении

защиты информации. Осознание каждым сотрудником своей индивидуальной роли и вклада в общую задачу по обеспечению информационной безопасности, а также понимание ценности защищаемой информации являются фундаментальными составляющими в формировании корпоративной культуры ИБ.

ЛИТЕРАТУРА


1. Архипова, И.С. Формирование корпоративной культуры в области информационной безопасности / И.С. Архипова, Д.Ю. Пантелеймонова // Современные технологии в мировом научном пространстве: сборник статей Международной научно-практической конференции: в 6 ч., Пермь, 25 мая 2017 года. Том Часть 3. — Пермь: Общество с ограниченной ответственностью «Аэтерна», 2017. — С. 15–18. — EDN YPPIQL.
2. Бойченко О.В., Аношкина А.А. Обеспечение безопасности критически важных объектов инфраструктуры Российской Федерации // Ученые записки Крымского федерального университета имени В. И. Вернадского. Экономика и управление. 2016. №2. URL: https://cyberleninka.ru/article/n/obespechenie-bezopasnosti-kriticheski-vazhnyh-obektov-infrastruktury-rossiyskoy-federatsii (дата обращения: 04.03.2024).
3. Горян Э.В., Баранник И.Н. Обеспечение информационной безопасности в финансовом секторе в рамках реализации национальной Программы «Цифровая экономика Российской Федерации» // Административное и муниципальное право. 2019. №4. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-finansovom-sektore-v-ramkah-realizatsii-natsionalnoy-programmy-tsifrovaya-ekonomika (дата обращения: 04.03.2024).
4. Иванова Е.А. Формирование корпоративной культуры и ее основные принципы // Наука. Инновации. Технологии. 2012. №2. URL: https://cyberleninka.ru/article/n/formirovanie-korporativnoy-kultury-i-ee-osnovnye-printsipy (дата обращения: 04.03.2024).
5. Косовец А.А. Информационная безопасность Российской Федерации: природа, сущность, содержание, основные понятия // Вестник экономической безопасности. 2011. №4. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-rossiyskoy-federatsii-priroda-suschnost-soderzhanie-osnovnye-ponyatiya (дата обращения: 04.03.2024).
6. Окатов А.В., Соловьев Д.А. Понятие и виды корпоративной культуры // Вестник Тамбовского университета. Серия: Общественные науки. 2017. №3 (11). URL: https://cyberleninka.ru/article/n/ponyatie-i-vidy-korporativnoy-kultury (дата обращения: 04.03.2024).
7. Пузанова Г.А., Пузанов А.А. Особенности обеспечения информационной безопасности предприятий малого и среднего бизнеса // Актуальные проблемы авиации и космонавтики. 2013. №9. URL: https://cyberleninka.ru/article/n/osobennosti-obespecheniya-informatsionnoy-bezopasnosti-predpriyatiy-malogo-i-srednego-biznesa (дата обращения: 04.03.2024).
8. Русецкая, И.А. Обеспечение информационной безопасности как элемент корпоративной культуры организации / И.А. Русецкая // Качество продукции: контроль, управление, повышение, планирование: сборник научных трудов 5-й Международной молодежной научно-практической конференции, Курск, 14 ноября 2018 года. Том 2. — Курск: Закрытое акционерное общество «Университетская книга», 2018. — С. 198–200. — EDN MIXAPB.
9. Самыгин С.И., Верещагина А.В., Кузнецова А.В. Информационные аспекты обеспечения финансовой безопасности российского общества // Гуманитарные, социально-экономические и общественные науки. 2015. №11. URL: https://cyberleninka.ru/article/n/informatsionnye-aspekty-obespecheniya-finansovoy-bezopasnosti-rossiyskogo-obschestva (дата обращения: 04.03.2024).
10. Шепелёва О.Ю., Шепелёв П.Ю., Газуль С.М. Оценка информационной безопасности предприятия как составная часть стратегического корпоративного управления // Правовая информатика. 2020. №4. URL: https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-predpriyatiya-kak-sostavnaya-chast-strategicheskogo-korporativnogo-upravleniya (дата обращения: 04.03.2024).



Журнал «Современная наука: актуальные проблемы теории и практики»