УДК 65.012.8

КОРПОРАТИВНАЯ КУЛЬТУРА КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦВЕТНЫХ ОРГАНИЗАЦИЯХ

Захарова У.М.

магистрант[1],

Тульский государственный педагогический университет им. Л. Н. Толстого,

Тула, Россия

Аннотация

Статья посвящена исследованию влияния корпоративной культуры на информационную безопасность в организациях, классифицированных согласно концепции цветных организаций Фредерика Лалу. Рассматривается, как особенности корпоративной культуры влияют на восприятие сотрудниками норм и правил защиты данных, а также на их готовность к соблюдению этих норм. Особое внимание уделяется роли человеческого фактора в современных угрозах информационной безопасности.

Ключевые слова: Корпоративная культура, информационная безопасность, цветные организации, управление рисками, управление предприятием, экономическая безопасность, стратегии защиты данных, культура безопасности.

CORPORATE CULTURE AS A FACTOR OF INFORMATION SAFETY IN COLOR ORGANIZATIONS

Zakharova U.M.

Master's Degree Student

[1] *Научный руководитель: к.э.н., доцент, доцент Н.Н. Левкина, Тульский государственный педагогический университет им. Л.Н. Толстого, Тула, Россия*
N.N. Levkina, PhD in economics, docent, Associate Professor, *Tula State Pedagogical University named after L.N. Tolstoy, Tula, Russia*

Tula State Pedagogical University named after L.N. Tolstoy,
Tula, Russia

Abstract

The article is dedicated to investigating the impact of corporate culture on information security within organizations classified according to Frederic Laloux's concept of colored organizations. It examines how the characteristics of corporate culture influence employees' perceptions of data protection norms and rules, as well as their willingness to adhere to these standards. Special emphasis is placed on the role of the human factor in contemporary information security threats.

Keywords: corporate culture, information safety, color organizations, risk management, enterprise management, economic security, data protection strategies, safety culture.

В условиях стремительного развития технологий и увеличения объемов информации, вопросы информационной безопасности становятся особенно актуальными для организаций всех типов. Корпоративная культура представляет собой важный элемент, который способствует обеспечению информационной безопасности и экономической стабильности организаций [3, с. 908]. Она не только формирует внутренние нормы и ценности, но и служит основой для устойчивого развития, объединяя интересы всех заинтересованных сторон на основе материальных и духовных ценностей [6, с. 127]. В этом контексте корпоративная культура становится защитным механизмом против внутренних угроз, создавая среду, в которой сотрудники осознают важность безопасности и придерживаются этичного поведения. [1, с. 31].

Анализ современных угроз показывает, что атаки, осуществляемые с использованием технических уязвимостей систем, становятся все более редкими. Вместо этого наблюдается рост атак, основанных на взаимодействии с

человеком. По информации компании Innostage, 80% инцидентов информационной безопасности связаны с человеческим фактором. Например, 48,9% инцидентов произошли из-за того, что сотрудник случайно опубликовал в общедоступном хранилище код с чувствительной информацией. Это привело к утечке данных клиентов, краже денежных средств и репутационному ущербу компании [5].

Одним из наиболее распространенных методов социальной инженерии является целевой фишинг, при котором текст электронного письма составляется с учетом специфики конкретного предприятия и знаний о сотруднике. Злоумышленники используют психологические приемы и социологические знания для того, чтобы вызвать у жертвы желание открыть прикрепленный файл или перейти по ссылке.

Как отмечает Paweł Kobis, «Человек — это непрограммируемый элемент системы», и его поведение в управлении информацией сложно предсказать. Это подчеркивает значимость корпоративной культуры в формировании подходов к информационной безопасности внутри организации [10, с.150].

Корпоративная культура определяет восприятие сотрудниками правил защиты информации и их готовность к соблюдению этих норм. Без должного уровня осознания ценности информации и необходимости ее защиты даже самые современные технические решения могут оказаться неэффективными [4, с.145].

Таким образом, корпоративная культура не просто поддерживает систему информационной безопасности; она является ее основой, обеспечивая необходимую среду для формирования ответственного отношения к защите данных.

Концепция цветных организаций, предложенная Фредериком Лалу, представляет собой классификацию, основанную на различных управленческих подходах и культурных особенностях, присущих организациям [2, с. 289]. В рамках этой теории выделяются пять типов организаций: красные, янтарные, оранжевые, зеленые и бирюзовые. Каждый из этих типов характеризуется

определенными стилями управления и внутренними процессами, которые непосредственно влияют на подходы к информационной безопасности.

Красные организации представляют собой авторитарные структуры, где доминирует роль руководителя и отсутствует справедливость в отношениях. В таких организациях управление осуществляется сверху вниз, что ограничивает возможности для инноваций и гибкости. Янтарные организации сохраняют авторитет руководства, но сотрудникам необходимо его заслужить через соблюдение строгих норм и правил. Они часто ассоциируются с традиционными структурами, такими как армия или образовательные учреждения.

Оранжевые организации представляют собой более прогрессивный тип, в которых ценятся профессионализм и стремление к достижениям. Здесь наблюдается коллегиальность в принятии решений и акцент на инновациях. Однако такая культура может порождать карьеризм и стремление к успеху любой ценой. Зеленые организации делают акцент на ответственности перед будущими поколениями и уважении к личности сотрудников. Их подходы к управлению основаны на коллективном принятии решений и экологически устойчивых практиках.

На вершине этой классификации находятся бирюзовые организации, которые можно считать образцом эволюционного развития. В них объединяются положительные качества всех предыдущих типов: самоуправление, уважение к личности и стремление к инновациям при сохранении дисциплины. Бирюзовые организации характеризуются высокой степенью вовлеченности сотрудников в процессы принятия решений и служением общим ценностям.

Исследования подтверждают актуальность концепции цветных организаций в контексте организационного развития. Например, Е.В. Федюкевич подчеркивает, что организационные структуры и ценности развиваются в соответствии со спиральной динамикой Лалу, акцентируя внимание на том, что рост больше не является единственным показателем успеха [7, с. 115].

Anna Wasiluk утверждает, что концепция цветных организаций открывает новые возможности для практик управления организациями, потому что Лулу объединил в данной концепции два подхода: теорию психологии и менеджмент [8, с. 648].

Таким образом, концепция цветных организаций не только предоставляет многогранный взгляд на организационную теорию и практику, но также отражает изменения в обществе и культурные интерпретации управления. Она демонстрирует важность учета культурных аспектов при разработке стратегий информационной безопасности и управления в целом, что делает ее актуальной для современных исследователей и практиков в области управления.

Как уже отмечалось выше, каждый из пяти типов организаций обладает своими специфическими чертами, которые влияют и на организацию процессов защиты информации.

В красных организациях, где доминирует авторитарный стиль управления, акцент делается на строгой иерархии и контроле. В таких системах сотрудники, как правило, не участвуют в принятии решений, что может привести к недостаточному пониманию значимости информационной безопасности. Практики в области защиты информации часто сводятся к формальному выполнению предписаний, что не всегда оказывается действенным. Сотрудники могут воспринимать безопасность как дополнительное бремя, а не как ключевой элемент своей деятельности. В результате возрастает риск утечек данных и инцидентов, так как работники могут не чувствовать личной ответственности за защиту информации.

Янтарные организации сохраняют некоторые аспекты авторитарного подхода, однако акцент делается на строгом соблюдении норм и регламентов. Управление осуществляется посредством чётко прописанных процедур. Особую роль играет режим коммерческой тайны и вопросы ее защиты. Практики информационной безопасности в таких структурах нередко включают формальные тренинги и жесткие политики доступа к данным. Тем не менее,

такой подход может ограничивать гибкость и способность сотрудников реагировать на быстро меняющиеся угрозы. Важно отметить, что недостаточная вовлеченность сотрудников в обсуждение вопросов безопасности может негативно сказаться на эффективности реагирования на инциденты.

Оранжевые организации отличаются большей динамичностью, в сотрудниках таких организаций руководитель ценит профессионализм и инновационный подход. В таких условиях сотрудники имеют возможность участвовать в процессе принятия решений и вносить собственные предложения. Практики защиты информации могут включать внедрение современных технологий, использование методов проработки инцидентов информационной безопасности, методы геймификации для обучения сотрудников информационного сектора.

В зеленых организациях внимание акцентируется на коллективном решении проблемы и социальной ответственности. В таких организациях сотрудники активно участвуют в вопросах обеспечения информационной безопасности. При возникновении инцидентов информационной безопасности, такие организации не умалчивают произошедшее, а открыто заявляют о возможных утечках данных. Используемые практики включают регулярные тренинги по информационной безопасности, нацеленные на разъяснение важности информационной безопасности для всей команды. Создаются форматы открытого диалога об угрозах и инцидентах информационной безопасности, что способствует развитию доверия и открытости. Сотрудники понимают свою роль в обеспечении информационной безопасности и участвуют в разработке стратегий защиты данных.

В бирюзовых организациях, где акцент делается на самоуправлении, практики информационной безопасности становятся неотъемлемой частью корпоративной культуры. Благодаря вовлечению сотрудников в процессы принятия решений, каждый сотрудник имеет возможность закрепить за собой определенные правила поведения в контексте взаимодействия с

информационными ресурсами организации. Это служит основой для успешного реагирования на инциденты информационной безопасности и минимизации рисков. В таких организациях часто проводятся мероприятия, направленные на повышение общей культуры информационной безопасности. Это может включать различные тренинги по информационной безопасности от специалистов, а также использование корпоративных настольных игр, которые моделируют возможные угрозы.

Исследователи утверждают, что не существует универсального стиля управления, который мог бы эффективно применяться ко всем организациям. Каждый стиль управления адаптирован к определенным условиям и особенностям конкретной организации [9, с. 11384].

Даже бирюзовые структуры, находящиеся на высшем уровне эволюции организационного управления, не могут быть внедрены повсеместно, поскольку феномен доверия, реализованный в таких организациях, не всегда может быть эффективно применен в различных типах организаций.

Тем не менее, менеджменту организаций необходимо задуматься о внедрении в практику многих подходов, характерных для бирюзовых организаций [9, с. 11385] Это включает постоянное обучение сотрудников и развитие их вовлеченности в процессы принятия решений. Важно развивать эмоциональную открытость и лояльность между сотрудниками, что способствует созданию доверительной атмосферы и повышает уровень осознания важности защиты информации.

Таким образом, концепция цветных организаций предоставляет ценные инсайты для анализа влияния организационной культуры на практики информационной безопасности. Понимание этих типов организаций позволяет руководителям лучше оценивать существующие риски и разрабатывать стратегии повышения уровня защиты информации, адаптируя подходы к специфике своей организационной культуры. В условиях растущих угроз информационной безопасности важно учитывать не только технические аспекты

защиты данных, но и культурные факторы, которые формируют отношение сотрудников к безопасности информации.

Библиографический список:

1. Астахова Л. В. Проблемы культуры информационной безопасности в условиях цифровой экономики//Научно-техническая информация. Серия 1: Организация и методика информационной работы. – 2020. – № 2. – С. 28-37.

2. Велицкая С. В. «Цветные организации»: сравнительный анализ и сферы применения / С. В. Велицкая, В. Е. Целин // Актуальные вопросы права, экономики и управления: материалы XI Междунар. науч.-практ.конф. – Пенза: Изд-во «Наука и Просвещение», 2017. – С. 288-291.

3. Калюжный А.С. Организационная культура как условие экономической безопасности предприятия//Экономика и предпринимательство. – 2023. – №4. – С.908-911.

4. Мартыненко Д. Д. Направления обеспечения кадровой составляющей экономической безопасности организации / Д. Д. Мартыненко, С. В. Тактарова // Экономическая безопасность общества, государства и личности: проблемы и направления обеспечения : материалы XI науч.-практ.конф. – Пенза: Изд-во Пензенский государственный университет, 2024. – С. 144-147.

5. Почти в 80% инцидентов ИБ напрямую виноват человеческий фактор Innostage [Электронный ресурс]. – Режим доступа – URL: https://innostage-group.ru/press/news/innostage-pochti-v-80-intsidentov-ib-napryamuyu-vinovat-chelovecheskiy-faktor/ (дата обращения 10.11.2024)

6. Цыцарова Н. М. Сильная корпоративная культура как условие обеспечения прочности организации в условиях неопределенности // Экономика и управление. – 2022. – № 3. – С. 125-128.

7. Федюкович, Е. В. Изменение подходов к определению результатов деятельности современных организаций // Российское предпринимательство. – 2019. – Т. 20. – № 1. – С. 109-122.

8. Anna Wasiluk. On the way to turquoise organizations and turquoise Leadership // Scientific papers of silesian university of technology organization and management series. – 2020. – №158. P.647-661.

9. Anna Kamińska. Turquoise Management Model -Teal Organizations // Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges. – 2020. P.11380-11387.

10. Paweł Kobis. Protection of information resources of small enterprises, including the subsystem for management of non-technical aspects of information security // Zeszyty Naukowe Wyższej Szkoły Humanitas Zarządzanie. – 2023. – №24. P. 143-159.

Оригинальность 84%