УДК 004.056.5, 005.934.2, 005.57

Никитина Т.О.,
старший преподаватель кафедры экономической информатики, учёта и коммерции,
Гомельский государственный университет имени Ф. Скорины,
Республика Беларусь, г. Гомель

КИБЕРУСТОЙЧИВОСТЬ БИЗНЕСА: ВНЕДРЕНИЕ КУЛЬТУРЫ JUST CULTURE В ПРОЦЕССЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В статье рассматривается концепция киберустойчивости бизнеса и её отличие от традиционной информационной безопасности. Особое внимание уделено интеграции принципов Just Culture в процессы управления информационной безопасностью, что позволяет формировать среду доверия, стимулировать открытость и использовать ошибки сотрудников как ресурс для совершенствования. Показана роль организационной культуры, руководства, HR и CISO в обеспечении устойчивости, а также обозначены барьеры и пути их преодоления. Сделан вывод о значении Just Culture как перспективной модели повышения киберустойчивости в условиях современной цифровой экономики.

Ключевые слова: киберустойчивость, информационная безопасность, Just Culture, организационная культура, аудит информационной безопасности, управление рисками, цифровая экономика, человеческий фактор.

Nikitina T.O.,
Senior Lecturer, Department of Economic Informatics, Accounting, and Commerce,
F. Skorina Gomel State University,
Republic of Belarus, Gomel

BUSINESS CYBERRESILIENCE: IMPLEMENTING JUST CULTURE IN INFORMATION SECURITY PROCESSES

Annotation

This article examines the concept of business cyberresilience and its differences from traditional information security. Particular attention is paid to integrating

Just Culture principles into information security management processes, which helps create an environment of trust, encourage openness, and utilize employee errors as a resource for improvement. The role of organizational culture, management, HR, and CISO in ensuring resilience is demonstrated, and barriers and ways to overcome them are identified. A conclusion is drawn regarding the importance of Just Culture as a promising model for enhancing cyberresilience in the modern digital economy.

Keywords: cyber resilience, information security, Just Culture, organizational culture, information security audit, risk management, digital economy, human factor.

Современная экономика всё более зависит от цифровых технологий, что делает бизнес уязвимым к киберугрозам и инцидентам информационной безопасности. Традиционные подходы, основанные на жёстком контроле и наказании за ошибки, часто оказываются недостаточными для обеспечения устойчивости в условиях динамично меняющейся среды. Концепция киберустойчивости предполагает не только техническую защиту, но и способность организации адаптироваться, восстанавливаться и учиться на собственных ошибках. В этом контексте особое значение приобретает модель Just Culture, ориентированная на баланс между ответственностью и доверием. Она позволяет рассматривать ошибки сотрудников не как повод для санкций, а как источник знаний для совершенствования процессов. Такой подход способствует развитию культуры доверия, ускоряет обмен информацией и повышает эффективность аудита ИБ.

Концепция Just Culture (культура справедливости) возникла в авиации и медицине, где цена ошибки особенно высока. Её теоретическую основу заложил Дж. Ризон в рамках исследований человеческого фактора и модели «швейцарского сыра» [1]. Суть подхода заключается в том, что ошибки сотрудников рассматриваются не как повод для наказания, а как источник информации для совершенствования процессов. Основные принципы включают: баланс между ответственностью и доверием;

открытость и возможность сообщать об ошибках без страха санкций; обучение на основе анализа ошибок; системный подход к выявлению причин инцидентов.

В контексте информационной безопасности Just Culture позволяет формировать среду, где сотрудники активно вовлечены в выявление уязвимостей, а организация получает возможность быстрее реагировать и адаптироваться.

Исследования показывают, что даже при наличии современных технических средств защиты человеческий фактор остаётся слабым звеном [2]. Культура доверия и вовлечённости способствует своевременному выявлению инцидентов, тогда как культура страха ведёт к сокрытию ошибок. Кроме того, зрелая организационная культура облегчает внедрение стандартов ИБ и повышает эффективность аудита. Таким образом, организационная культура выступает невидимым, но критически важным фактором, определяющим результативность даже самых передовых технических мер защиты.

Интеграция принципов Just Culture в систему управления информационной безопасностью предполагает переход от репрессивной модели реагирования на ошибки к модели обучения и совершенствования процессов. Основные этапы внедрения включают:

1. Формирование политики доверия: закрепление в нормативных документах принципа недопустимости наказания за непреднамеренные ошибки.
2. Создание каналов обратной связи: внедрение анонимных систем сообщения об инцидентах и уязвимостях.
3. Систематический анализ ошибок: использование методов root cause analysis для выявления первопричин инцидентов.
4. Обучение и развитие персонала: регулярные тренинги, моделирование сценариев атак и обсуждение ошибок как учебных кейсов.

5. Интеграция в стратегию управления рисками: включение показателей зрелости Just Culture в систему KPI по информационной безопасности [3].

Аудит информационной безопасности традиционно ориентирован на проверку соответствия стандартам (ISO/IEC 27001, NIST CSF и др.). Однако в условиях цифровой экономики формальное соответствие не гарантирует реальной устойчивости бизнеса [4]. Внедрение Just Culture позволяет расширить задачи аудита:

1. От проверки к оценке зрелости: аудит фиксирует не только наличие процедур, но и уровень вовлечённости сотрудников.

2. Фокус на человеческом факторе: анализируется, как сотрудники реагируют на инциденты и сообщают о них.

3. Интеграция качественных показателей: в дополнение к техническим метрикам учитываются показатели доверия, открытости и скорости обмена информацией.

Таким образом, аудит становится инструментом не только контроля, но и развития организационной культуры, что повышает его стратегическую ценность.

Классическая триада «человек — процесс — технология» является основой большинства моделей информационной безопасности [5]. В контексте Just Culture она приобретает новые акценты:

1. Человек: рассматривается не как «слабое звено», а как активный участник системы, способный выявлять и предотвращать угрозы.

2. Процесс: ошибки сотрудников интерпретируются как индикаторы несовершенства процессов, требующих корректировки.

3. Технология: технические средства защиты поддерживают процессы обучения и анализа, обеспечивая прозрачность и фиксацию инцидентов.

Таким образом, Just Culture трансформирует триаду в динамическую

систему, где взаимодействие человека, процессов и технологий направлено на повышение киберустойчивости.

Внедрение Just Culture в практику информационной безопасности требует системного подхода и последовательных шагов:

1. Диагностика текущего состояния: анализ организационной культуры, уровня доверия и практики реагирования на инциденты.

2. Формулирование политики: закрепление принципов Just Culture в локальных нормативных актах, стратегиях ИБ и корпоративных кодексах.

3. Создание инфраструктуры обратной связи: внедрение анонимных каналов сообщения об ошибках и уязвимостях.

4. Обучение и вовлечение персонала: проведение тренингов, моделирование сценариев киберинцидентов, обсуждение ошибок как учебных кейсов.

5. Интеграция в процессы управления рисками: включение показателей зрелости Just Culture в KPI и систему аудита ИБ.

6. Мониторинг и корректировка: регулярная оценка эффективности, адаптация подходов в зависимости от динамики угроз и внутреннего климата [6].

Роль руководства, HR и CISO в формировании среды доверия:

• Руководство: задаёт тон организационной культуре, демонстрируя готовность рассматривать ошибки как ресурс для развития, а не как повод для наказания. Поддержка топ-менеджмента является ключевым фактором успешного внедрения.

• HR-служба: отвечает за формирование программ обучения, развитие soft skills сотрудников, внедрение инструментов обратной связи и мониторинг уровня доверия в коллективе. HR также играет роль медиатора между персоналом и руководством.

• CISO (директор по информационной безопасности): интегрирует принципы Just Culture в процессы ИБ, обеспечивает баланс между

техническими мерами и культурными аспектами, участвует в разработке метрик зрелости и взаимодействует с аудиторами.

Для оценки уровня зрелости и эффективности внедрения Just Culture в организации используются как количественные, так и качественные показатели. Среди ключевых критериев выделяются:

1. Уровень доверия сотрудников: готовность персонала сообщать об ошибках и инцидентах без страха наказания [7].
2. Скорость и полнота выявления инцидентов: чем выше зрелость культуры, тем быстрее фиксируются и анализируются ошибки.
3. Качество обратной связи: наличие систематического анализа ошибок и доведения результатов до сотрудников.
4. Интеграция в процессы управления рисками: включение принципов Just Culture в стратегические документы и KPI.
5. Обучение и развитие персонала: регулярность тренингов, моделирование сценариев, вовлечённость сотрудников в обсуждение ошибок.
6. Метрики зрелости культуры: использование опросов, индексов вовлечённости и независимых аудитов для оценки уровня доверия и открытости [8].

Превосходство Just Culture перед другими моделями построения информационной безопасности состоит в том, что традиционные модели построения информационной безопасности (например, основанные на принципах «нулевой терпимости» или исключительно техническом контроле) имеют ряд ограничений. В то время, как Just Culture обеспечивает баланс между ответственностью и доверием, стимулирует открытость и обмен информацией, рассматривает ошибки как ресурс для обучения и совершенствования процессов, повышает киберустойчивость бизнеса, интегрируя человеческий фактор в систему защиты [9].

Одним из показательных примеров является реакция компании

SolarWinds на атаку на цепочку поставок в 2020 году. После внедрения вредоносного кода в обновления Orion, компания не ограничилась устранением уязвимости, а провела глубокую перестройку процессов разработки. В рамках Just Culture подхода ошибки сотрудников и системные сбои были рассмотрены как индикаторы несовершенства процессов, а не как повод для наказания. В результате были внедрены параллельные независимые пайплайны сборки, многоуровневая проверка целостности артефактов, разделение обязанностей и независимая верификация [10]. Это позволило не только восстановить доверие клиентов и инвесторов, но и повысить уровень цифровой устойчивости компании.

Внедрение принципов Just Culture в процессы информационной безопасности формирует качественно новый уровень организационной зрелости. Такой подход обеспечивает баланс между ответственностью и доверием, стимулирует открытость и обмен информацией, а также превращает ошибки сотрудников в источник знаний для совершенствования процессов. В отличие от моделей, основанных на жёстком контроле и наказании, Just Culture способствует формированию среды доверия, что напрямую повышает эффективность аудита и стратегическую устойчивость бизнеса.

Организационная культура в данном контексте выступает ключевым фактором, определяющим результативность даже самых современных технических решений. Поддержка руководства, активное участие HR и CISO являются необходимыми условиями успешного внедрения.

Таким образом, Just Culture может рассматриваться как перспективная концептуальная модель, интегрирующая человеческий фактор, процессы и технологии в единую систему обеспечения киберустойчивости.

Использованные источники:

1. Reason J. Human Error. Cambridge: Cambridge University Press, 1990. — 302 p.
2. Построение культуры информационной безопасности [Электронный ресурс]. — Режим доступа: https://onlanta.ru/press/blog/postroenie-kultury-informatsionnoy-bezopasnosti/ (дата обращения: 09.10.2025).
3. Dekker S. Just Culture: Restoring Trust and Accountability in Your Organization. 3rd ed. Boca Raton: CRC Press, 2017. — 232 p.
4. Calder A. Nine Steps to Success: An ISO 27001 Implementation Overview. IT Governance Publishing, 2017. — 180 p.
5. Добрышин М. М. Концептуальная модель как инструмент познания процесса обеспечения информационной безопасности // Экономика и качество систем связи. — 2025. — № 1. — С. 45–53.
6. Hollnagel E., Woods D. D., Leveson N. Resilience Engineering: Concepts and Precepts. Aldershot: Ashgate, 2006. — 397 p.
7. Marx D. Patient Safety and the “Just Culture”: A Primer for Health Care Executives. New York: Columbia University, 2001. — 54 p.
8. The Just Culture Company. Just Culture Algorithm [Электронный ресурс]. — Режим доступа: https://www.justculture.com/learning/just-culture-algorithm/ (дата обращения: 09.10.2025).
9. Just culture — Wikipedia [Электронный ресурс]. — Режим доступа: https://en.wikipedia.org/wiki/Just_Culture (дата обращения: 09.10.2025)
10. Лазырин М. Киберриски – новая норма. Почему бизнесу пора внедрять Just Culture и роль директора по цифровой устойчивости // Cyber Media. — 30.09.2025. — Режим доступа: https://securitymedia.org/info/kiberriski-novaya-norma-pochemu-biznesu-pora-vnedryat-just-culture-i-rol-direktora-po-tsifrovoy-usto.html (дата обращения:

09.10.2025)