Научная статья
УДК 338.31; 004.05
DOI: 10.18127/j19997493-202403-03

Фреймворки управления информационными технологиями и киберрисками при цифровой трансформации организации

М.А. Павлов[1]

[1] ФБГОУ ВО Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет) (Москва, Россия)
[1] mikhail.pavlov.mgimosgp@gmail.com

Аннотация

Постановка проблемы. Для обеспечения кибербезопасности информационной системы в условиях цифровой трансформации и минимизации риски возможных потерь и нарушений безопасности необходимо эффективное управлением внедрением мер цифровой безопасности организации.
Цель. Выполнить комплексный анализ и бенчмаркинг фреймворков в данном области.
Результаты. Проанализированы основные документы, стандартные руководства, рекомендации и фреймворки, регулирующие кибербезопасность и ИТ-риски при цифровой трансформации. Определены системные решения по разработке стратегии кибер- и цифровой безопасности.
Практическая значимость. Предложена модель системы управления кибербезопасности и непрерывности бизнеса в контексте цифровой трансформации организации. Описаны рекомендации к механизму ее управления.

Ключевые слова

Кибербезопасность, информационные технологии, фреймворки, цифровая безопасность

Для цитирования

Павлов М.А. Фреймворки управления информационными технологиями и киберрисками при цифровой трансформации организации // Динамика сложных систем. 2024. Т. 18. № 3. С. 23–33. DOI: 10.18127/j19997493-202403-03

A brief version in English is given at the end of the article

Введение

Цифровая трансформация предприятий включает в себя использование информационных технологий для оптимизации бизнес-процессов, улучшения взаимодействия с клиентами и повышения эффективности работы компании. Однако в процессе цифровой трансформации предприятия сталкиваются с различными киберрисками – кибератаками, утечкой данных, вредоносными программами и др. [1–3].

Потенциальные потери от нарушений кибербезопасности могут проявиться в виде нескольких негативных последствий для организации [1–3].

1. Финансовые потери – ущерб финансового состояния компании, включая кражи денежных средств, финансовых данных, интеллектуальной собственности, штрафы и санкции регулирующих органов, а также ущерб репутации.

2. Потери данных – утрата или утечка конфиденциальной информации, включая персональные данные клиентов, предприятий или партнеров, государственные секреты и коммерческие секреты.

3. Прерывание бизнеса – прерывание работы компании, временным или длительным сбоям систем, что приведет к потере продуктивности, отрицательному воздействию на репутацию и клиентов.

4. Юридические и регуляторные последствия – судебные тяжбы, нарушение законодательных или регуляторных требований, штрафы и репутационный ущерб.

Эффективное внедрение таких мер позволит организациям обеспечить кибербезопасность информационной системы в условиях цифровой трансформации и минимизировать риски возможных потерь и нарушений безопасности [1–3].

Применение фреймворков управления информационными технологиями в компаниях и адаптация бизнес-процессов кибербезопасности и непрерывности бизнеса становятся все более актуальными и критически важными для них, так как есть вероятность столкновения с рядом проблем при правильном *применении фреймворков управления информационными технологиями* [3–5]:

1. Сложность выбора – множество фреймворков управления информационными технологиями, и правильный их выбор может быть сложным для компании, поскольку требуется анализ потребностей, целей и возможностей.

2. Ресурсы – внедрение и поддержание фреймворков управления информационными технологиями требует больших затрат в виде времени, финансов и человеческих ресурсов, что может быть особенно сложно для малых и средних предприятий.

3. Изменения в культуре компании – внедрение новых фреймворков часто требует изменений в культуре компании и рабочих процессах, а это то может вызывать сопротивление со стороны сотрудников.

Адаптация бизнес-процессов кибербезопасности и непрерывности бизнеса под системное применение руководств и фреймворков также влечет за собой ряд проблем [4–6]:

1. Комплексность угроз – сталкивание кибербезопасности и непрерывности бизнеса со все более сложными и разнообразными угрозами, что требует постоянного обновления и реагирования на новые вызовы.

2. Отношение к рискам – уязвимость перед угрозами некоторых компаний из-за игнорирования или недооценивания рисков, связанных с кибербезопасностью и непрерывностью бизнеса.

3. Совместимость с бизнес-целями – уравновешивание с бизнес-целями, интеграции кибербезопасности и непрерывности бизнес-процессов, чтобы избежать излишней сложности и издержек.

Решение этих проблем требует внимательного организационно-экономического анализа, понимания организационных потребностей (бизнес-целей) и грамотного управления изменениями [7].

Ц е л ь р а б о т ы – выполнить комплексный анализ и бенчмаркинг фреймворков в данном области.

Материалы и методы исследования рекомендаций по управлению кибербезопасностью

Исследование рекомендаций по управлению кибербезопасностью и ИТ-рисками – важный шаг для организаций, стремящихся эффективно защитить свои информационные ресурсы. Существует несколько методов, которые можно использовать для проведения такого исследования.

1. Анализ стандартов и регуляторных требований – изучение стандартов и регуляторных требований, которые существуют в отрасли или стране.

2. Обзор научных исследований и публикаций – изучение научных исследований, публикаций и отчетов относительно управления кибербезопасностью и ИТ-рисками (статьи, конференции и веб-сайты специализированных организаций, таких как CERT).

3. Консультации с экспертами – сотрудничество как с внутренними экспертами (сотрудниками ИТ-отдела или специалисты по безопасности), а также с внешними консультантами, имеющими профессиональный опыт и практические знания в данной области.

4. Участие в профессиональных сообществах – присоединение к профессиональным сообществам и форумам, посвященным кибербезопасности и ИТ-рискам, что может предоставить доступ к ценным рекомендациям и передовым практикам, используемым другими компаниями.

5. Проведение самостоятельного исследования – исследование, основанного на анализе инцидентов безопасности, сборе данных и оценке текущего состояния безопасности в собственной компании (включает проведение аудита безопасности, реализацию тестирования на проникновение и анализ логов безопасности).

Комбинирование различных методов исследования может способствовать получению наиболее всестороннего обзора рекомендаций по управлению кибербезопасностью и ИТ-рисками и поможет компании разрабатывать и реализовывать эффективные меры безопасности.

Документы, регулирующие кибербезопасность и ИТ-риски

Рассмотрим информацию об основных международных и отечественных документах, регулирующих кибербезопасность и ИТ-риски при цифровой трансформации [8–14]:

Международные документы [8–14].

1. Главные принципы организации безопасности в информационном обществе ООН – документ разрабатывает подходы к обеспечению безопасности и стабильности в информационном обществе и включает рекомендации по кибербезопасности и мерам по укреплению ИТ-инфраструктуры.

2. Генеральная Ассамблея ООН – в рамках Организации Объединенных наций были приняты резолюции и документы, направленные на обеспечение безопасности информации и кибербезопасности: «Роль ООН в информационной и коммуникационной области в контексте международной безопасности» и «Кибербезопасность: защита критической информационной инфраструктуры».

3. Директива ЕС о кибербезопасности (NIS Directive) – документ стандартизирует подходы к обеспечению кибербезопасности в странах-членах ЕС и оказывает влияние на развитие мер и стандартов в области кибербезопасности.

4. Европейский союз (ЕС): ЕС принимает набор законодательных актов в области информационной безопасности, включая Общий регламент по защите данных (GDPR), который устанавливает стандарты для обработки и защиты персональных данных.

5. Стандарт ISO/IEC 27001:2013 – утверждает требования к системам управления информационной безопасностью и помогает организациям разрабатывать и внедрять подходы к защите информации и кибербезопасности.

6. Международная организация по стандартизации (ISO) – разработала ряд стандартов информационной безопасности (ISO/IEC 27001 и ISO/IEC 27002), описывающих систему управления информационной безопасностью, а также руководство по безопасности информации.

Отечественные документы [8–14].

1. Федеральный закон «О персональных данных» – регулирует обработку персональных данных и устанавливает требования к защите информации.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» – устанавливает базовые принципы охраны информации и правила использования информационных технологий.

3. Доктрина информационной безопасности РФ – описывает основные цели и задачи в области информационной безопасности, включая защиту критической информационной инфраструктуры, и меры по обеспечению информационной безопасности в России.

4. Концепция обеспечения информационной безопасности РФ до 2030 года – устанавливает основные подходы к обеспечению информационной безопасности, включая меры по защите от киберугроз, кибератак и других ИТ-рисков.

5. Концепции формирования и развития культуры информационной безопасности граждан РФ (2022) – предлагает принципы обеспечения безопасности информации и кибербезопасности в России.

6. Методические рекомендации по обеспечению информационной безопасности в сфере киберфизических систем (МР ИБ КФС), разработаны ФСТЭК – предлагают методики по анализу и обеспечению информационной безопасности в киберфизических системах.

Стандартные руководства, рекомендации и фреймворки, используемые для управления информационной безопасностью и кибербезопасностью [8–14].

1. ISO/IEC 27001 – методология управления информационной безопасностью. Устанавливает требования для управления рисками, связанными с информационной безопасностью.

2. NIST Cybersecurity Framework – фреймворк предоставляет методы для улучшения кибербезопасности организации и ряд базовых принципов безопасности (разработан Национальным институтом стандартов и технологий).

3. COBIT (Control Objectives for Information and Related Technologies) – фреймворк, предоставляющий руководство для управления и контроля информационных технологий в организации и помогающий улучшить процессы управления IT.

4. CIS Critical Security Controls – фреймворк, представляющий набор наиболее эффективных мер безопасности, которые могут быть реализованы для защиты организации от известных угроз.

Результаты

Фреймворк – структура, набор инструментов, библиотек и рекомендаций, предназначенных для разработки программного обеспечения. Фреймворк предоставляет основные элементы и функции, которые могут быть использованы разработчиками для построения приложений, веб-сайтов или других программных систем, обеспечивает рамки для организации кода, обработки ввода-вывода, управления памятью, взаимодействия с базой данных, а также других основных функций для упрощения процесса разработки.

Использование стандартных фреймворков кибербезопасности представляется важной необходимостью в контексте цифровой трансформации по нескольким причинам.

1. Безопасность данных – стандартные фреймворки помогают обеспечить защиту данных от утечек, несанкционированного доступа и других угроз, поскольку цифровая трансформация обычно включает в себя использование большого объема данных, которые часто содержат конфиденциальную информацию о клиентах, бизнес-процессах и операциях компании.

2. Соответствие требованиям – стандартные фреймворки помогают компаниям обеспечить соответствие нормативным требованиям к информационной безопасности и представить свою деятельность в соответствии с законодательными нормами.

3. Эффективное управление рисками – стандартные фреймворки предоставляют методы и инструменты для эффективного управления рисками, которые увеличивает цифровая трансформация, позволяя выявить уязвимости, разработать проактивные стратегии защиты и реагировать на киберугрозы.

Исходя из этого, использование стандартных фреймворков кибербезопасности становится обязательным элементом стратегии цифровой трансформации компаний, поскольку помогает обеспечить безопасность информационных систем, соответствие нормативным требованиям и эффективное управление киберрисками.

ISO 27001 (Международный стандарт ISO/IEC 27001) – методология управления информационной безопасностью. Он устанавливает требования для управления рисками, связанными с информационной безопасностью в компании. Некоторые из основных принципов ISO 27001 включают установление и поддержание системы управления информационной безопасностью, идентификацию и оценку рисков, а также реализацию соответствующих контролов безопасности. Преимущества ISO 27001 включают его статус международно признанного стандарта, а также фокус на целостность, конфиденциальность и доступность информации. Однако ISO 27001 также требует значительных временных и финансовых затрат и носит относительно высокий уровень сложности, поскольку требует экспертизы в области информационной безопасности [8–14].

NIST Cybersecurity Framework (Фреймворк кибербезопасности NIST) – фреймворк, разработанный Национальным институтом стандартов и технологий (NIST) для улучшения кибербезопасности организации. Он представляет базовые принципы безопасности и включает такие элементы, как идентификация, защита, обнаружение, реагирование и восстановление. Он также применяет методы управления рисками и содействует формированию культуры безопасности. Преимущества NIST Cybersecurity Framework – гибкость и применимость к различным секторам и организациям, возможность непрерывного анализа и улучшения, взаимодействия с другими стандартами и руководствами. Однако NIST Cybersecurity Framework не предоставляет конкретных технических решений и требует адаптации к организационным потребностям [8–14].

COBIT (Control Objectives for Information and Related Technologies) – фреймворк для управления и контроля информационных технологий в организации. COBIT помогает связать бизнес-цели с IT-целями и защитить IT-ресурсы организации. Он включает управление процессами IT, защиту IT-ресурсов и др. Преимущества COBIT в том, что он включают улучшение процессов управления IT, стратегическое планирование в области IT и наличие различных ресурсов для реализации принципов COBIT. Однако COBIT имеет ограничения применимости в различных отраслях и требует значительных затрат на внедрение и сопровождение [8–14].

CIS Critical Security Controls (критические меры безопасности CIS) – набор эффективных мер безопасности для защиты организации от известных угроз. Он включает такие принципы, как защита от

угроз информационной безопасности, сдерживание наиболее критических атак и непрерывное улучшение безопасности, предоставляет конкретные списки контролей безопасности, которые помогают компаниям сфокусироваться на наиболее значимых рисках и угрозах. Однако CIS Critical Security Controls не предоставляет конкретных технических решений, а также требует от компании адаптации к своим особенностям и потребностям [8–14].

Взаимосвязь между фреймворками (таблица) заключается в том, что они все ориентированы на обеспечение безопасности информации в компании и управление рисками, связанными с информационной безопасностью. Однако каждый из них имеет свои особенности, уделение внимания определенным аспектам безопасности и различные подходы к управлению. Отличия между ними могут состоять в охвате области, уровне детализации, требованиях к компании и применимости в различных отраслях. При выборе фреймворка компании должны учитывать свои специфические потребности, секторальные требования и ресурсы, чтобы определить наиболее подходящий для них фреймворк.

Таблица. ***Стандартные руководства, рекомендации и фреймворки для управления кибербезопасностью и ИТ-рисками***

Название	Описание	Основные принципы	Преимущества	Ограничения
ISO/IEC 27001	Методология управления информационной безопасностью и установление требований для управления рисками, связанными с информационной безопасностью	Установление системы управления информационной безопасностью. Идентификация и оценка рисков. Реализация соответствующих контролей безопасности	Международно признанный стандарт. Целостность, конфиденциальность и доступность информации. Непрерывное улучшение системы управления	Требует значительных временных и финансовых затрат. Требует экспертизы в области информационной безопасности
NIST Cyber-security Framework	Фреймворк для улучшения кибербезопасности организации, представляющий базовые принципы безопасности	Идентификация/защита/обнаружение/реагирование/восстановление. Применение методов управления рисками. Содействие культуре безопасности	Гибкость и применимость к различным секторам и организациям. Проведение непрерывного анализа и улучшений. Взаимодействие с другими стандартами и руководствами	Не предоставляет конкретных технических решений. Требует адаптации к организационным потребностям
COBIT	Фреймворк для управления и контроля информационных технологий в организации	Управление процессами IT. Связь бизнес-целей и IT-целей. Защита IT-ресурсов	Улучшение процессов управления IT. Стратегическое планирование в области IT. Различные ресурсы для реализации принципов COBIT	Ограничения применимости в различных отраслях. Высокие затраты на внедрение и сопровождение
CIS Critical Security Controls	Набор эффективных мер безопасности для защиты организации от известных угроз	Защита от угроз информационной безопасности. Сдерживание наиболее критических атак. Непрерывное улучшение безопасности	Конкретный список мер безопасности. Ориентация на самые важные аспекты безопасности. Практическое руководство для реализации контролей	Ориентация на известные угрозы, может не учитывать новые. Не предоставляет интегрального подхода к управлению безопасностью

Обсуждение

Для обеспечения кибербезопасности информационных систем и непрерывности бизнеса в контексте цифровой трансформации организации необходимо принимать комплексное и системное решения [15–20].

1. Разработка стратегии кибер- и цифровой безопасности – определяются цели и приоритеты безопасности информационной системы, а также разрабатывается политика безопасности, которая бы отражала основные принципы обеспечения безопасности в контексте цифровой трансформации.

2. Внедрение современных технологий – уделяется особое внимание использованию современных технологий для защиты информационной системы в связи с развитием цифровой трансформации (использование криптографических методов защиты данных, облачных технологий, средств мониторинга и аналитики безопасности) [15–20].

3. Обучение сотрудников компании – важный аспект обеспечения безопасности. Регулярное обучение сотрудников по вопросам информационной безопасности помогает снижать риски внутренних угроз [15–20].

4. Мониторинг и реагирование – устанавливается система мониторинга и реагирования на угрозы информационной безопасности (использование системы обнаружения вторжений, а также создание процедур реагирования на инциденты безопасности).

5. Аудит безопасности – регулярное проведение аудитов информационной безопасности, что позволяет выявлять слабые места и недостатки в системе безопасности, а также корректировать стратегию защиты с учетом новых угроз [15–20].

6. Соответствие законодательству – необходимость учета требования законодательства в области защиты персональных данных и информационной безопасности при разработке стратегии цифровой безопасности [15–20].

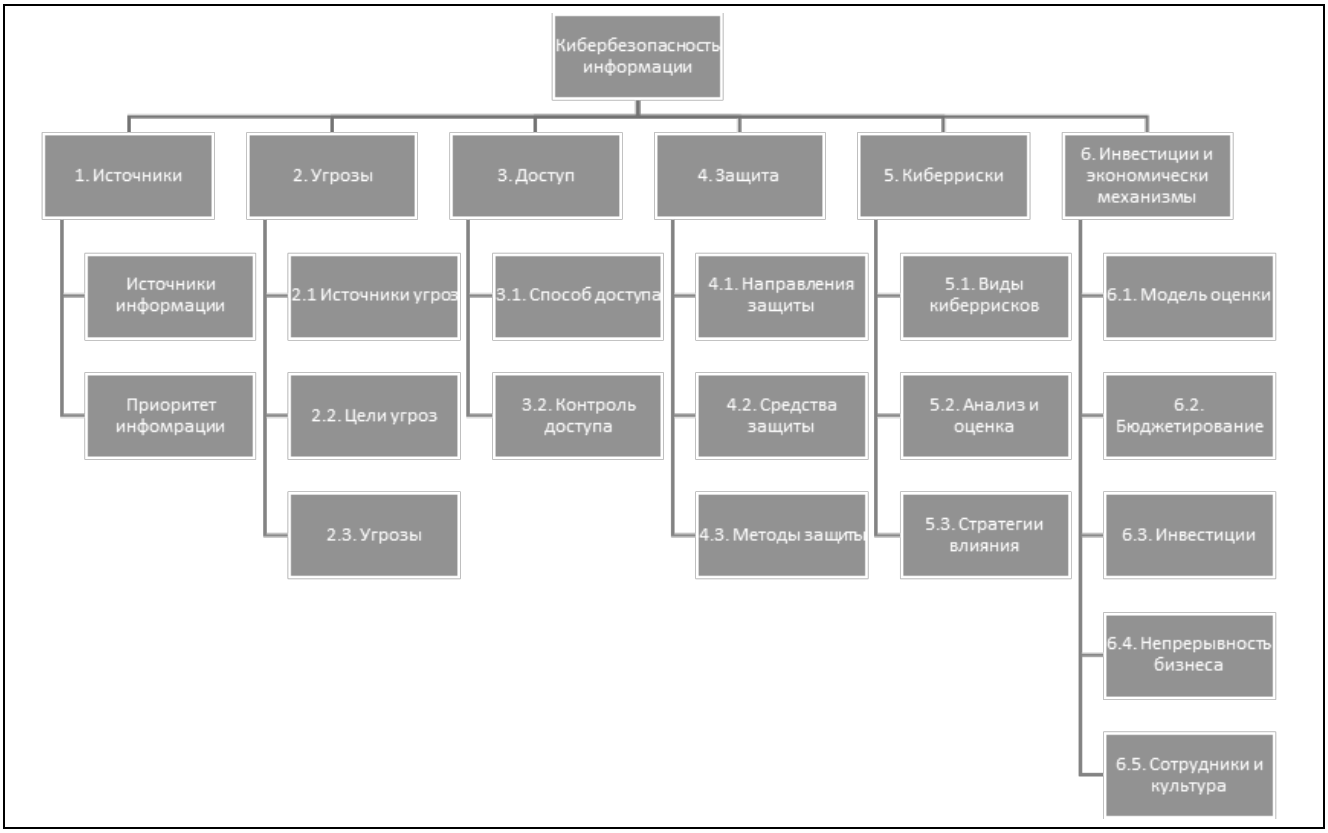

Рис. 1. Модель системы управления кибербезопасности и непрерывности бизнеса в контексте цифровой трансформации компании
Fig. 1. The model of the cybersecurity and business continuity management system in the context of the company's digital transformation

Управление кибербезопасностью и ИТ-рисками является важным бизнес-процессом, который направлен на обеспечение безопасности информационных систем и защиту компании от возможных киберугроз и технических рисков [15–20].

Этот бизнес-процесс состоит из нескольких этапов [15–20]:

1. Идентификация и анализ рисков – проводится оценка возможных угроз и рисков, связанных с информационными системами и ИТ-инфраструктурой организации. Определяются потенциальные уязвимости, уровень риска и потенциальные последствия инцидентов безопасности [3–6].

2. Разработка политики и стратегий – на основе анализа рисков разрабатывается политика безопасности информационных систем и стратегия управления кибербезопасностью, определяются цели, принципы безопасности, роли и ответственности сотрудников, а также меры по предотвращению и реагированию на инциденты безопасности [15–20].

3. Реализация контролей безопасности – внедряются технические и организационные меры безопасности, чтобы снизить риски и защитить информационные ресурсы организации. Это может включать установку файрволлов, антивирусных программ, систем мониторинга и обнаружения вторжений, а также разработку процедур доступа к информационным системам и обучение сотрудников правилам безопасности.

4. Мониторинг и аудит безопасности – непрерывный мониторинг состояния безопасности, а также аудит и оценка эффективности принятых мер безопасности, проверка соответствия политике безопасности, выявление возможных уязвимостей и регулярное обновление контролей безопасности.

5. Реагирование на инциденты безопасности – проведение незамедлительных действий по обнаружению инцидентов безопасности, анализу и реагированию: блокирование доступа, восстановление системы, сбор доказательств и расследование инцидента для предотвращения повторного вмешательства.

6. Постоянное совершенствование процесса – непрерывное изучение новых угроз и технологий, изменение политики и стратегии безопасности в соответствии с развитием информационных систем и потенциальными рисками, проведение обучения сотрудников по вопросам безопасности информационных систем [15–20].

Цель бизнес-процесса – обеспечение надежной защиты информационных ресурсов компании, минимизация рисков, связанных с инцидентами безопасности, и обеспечение непрерывности бизнес-процессов.

Заключение

Стандартные фреймворки обеспечивают набор рекомендаций, методологий и практик, которые помогают организациям разрабатывать и реализовывать солидные стратегии по обеспечению кибербезопасности.

Вложения в стандартные фреймворки кибербезопасности имеют ряд преимуществ.

1. Стандартные фреймворки обеспечивают системный подход к обеспечению безопасности, учитывая различные аспекты, такие как управление угрозами, управление доступом, мониторинг, реагирование на инциденты и т.д., что помогает предотвращать уязвимости и обнаруживать инциденты на ранних стадиях.

2. Стандартные фреймворки часто основываются на передовых практиках и опыте отрасли, что позволяет организациям использовать проверенные методы и рекомендации, что помогает сократить время и затраты на разработку и реализацию своих собственных моделей безопасности.

3. Инвестирование в стандартные фреймворки кибербезопасности демонстрирует серьезность и приверженность компании безопасности данных. Это может быть важным фактором для клиентов, партнеров и регуляторных органов, которые ценят компании, обеспечивающие надежную защиту своих систем и данных.

Разработка и внедрение стандартных фреймворков кибербезопасности – ключевой компонент в обеспечении безопасности информационных систем.

Использование таких фреймворков помогает систематизировать и улучшить уровень защиты, обеспечивая соответствие стандартам кибербезопасности, а также упрощает адаптацию к растущим угрозам.

Важно отметить, что стандарты ISO 27001, NIST, COBIT, CIS и другие могут использоваться совместно, чтобы создать комплексную программу безопасности информации в компании. Последние могут выбрать ту или иную комбинацию стандартов в зависимости от их потребностей, требований и сферы деятельности.

Инвестирование в стандартные фреймворки кибербезопасности поможет компаниям эффективно управлять киберрисками и реагировать на потенциальные угрозы, что имеет большое значение в современной цифровой среде.

Список источников

1. *Дроговоз П.А., Коренькова Д.А., Павлов М.А*. Кибербезопасность в международной космической индустрии: кооперативно-игровой подход к гармонизации экономических интересов стейкхолдеров // XLVI Академические чтения по космонавтике, посвященные памяти академика С.П. Королева и других отечественных ученых – пионеров освоения космического пространства (Москва, 25–28 янв. 2022 г.): Сб. тез. Всерос. науч. конф. / РАН [и др.]; ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: Изд-во МГТУ им. Н.Э. Баумана. 2022. Т. 2. С. 48–54.
2. *Дроговоз П.А., Коренькова Д.А*. Современный инструментарий гибкого управления ИТ-проектами и перспективы его совершенствования с использованием технологий искусственного интеллекта // Экономика и предпринимательство. 2019. № 10. С. 829–833.
3. *Дроговоз П.А., Юсуфова О.М., Коренькова Д.А*. Цифровая трансформация производственных систем: обзор основных направлений и факторов развития / X Чарновские чтения (Москва, 4–5 дек. 2020 г.): Сб. трудов Всерос. науч. конф. по организации производства / ФГБОУ ВО «Московский государственный университет имени Н.Э. Баумана (национальный исследовательский университет)» [и др.]. М.: НОЦ «Контроллинг и управленческие инновации». 2021. С. 61–68.
4. *Дроговоз П.А., Пушкарева П.П.* Специфика управления инвестиционными рисками в наукоемкой промышленности // Будущее машиностроения России (Москва, 22–25 сен. 2020 г.): Сб. докладов XXIII Всерос. науч. конф. молодых ученых и специалистов (с междунар. участием): в 2 т. Т. 2 / Союз машиностроителей России, Московский государственный университет имени Н.Э. Баумана (национальный исследовательский университет). М.: Изд-во МГТУ им. Н.Э. Баумана. 2020. С. 371–373.
5. *Дроговоз П.А., Ралдугин О.В*. Математическое моделирование рисков кооперации по созданию системы воздушно-космической обороны / XLIII Академические чтения по космонавтике, посвященные памяти академика С.П. Королева и других отечественных ученых – пионеров освоения космического пространства (Москва, 29 янв. – 1 фев. 2019 г.): Сб. тез. Всерос. науч. конф. / РАН [и др.]; ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: Изд-во МГТУ им. Н.Э. Баумана, 2019. Т. 1. С. 167–169.
6. *Дроговоз П.А., Ралдугин О.В*. Информационно-технологические факторы развития кооперации в оборонно-промышленном комплексе и риск-ориентированный подход к ее формированию при создании системы воздушно-космической обороны // Экономические стратегии. 2016. Т. 18. № 7 (141). С. 76–89.
7. *Drogovoz P.A., Kashevarova N.A., Dadonov V.A., Sadovskaya T.G. and Trusevich M.K*. Industry 4.0 in Russia: Digital Transformation of Economic Sectors / in Industry 4.0 in SMEs Across the Globe: Drivers, Barriers, and Opportunities, edited by J.M. Müller, N. Kazantsev (CRC Press, Boca Raton, 2021). P. 195–211. https://doi.org/10.1201/9781003165880-15
8. *Jerman-Blažič B*. et al. An economic modelling approach to information security risk management // International Journal of Information Management. 2008. Т. 28. №. 5. P. 413–422.
9. *Huang C.D., Hu Q., Behara R.S.* An economic analysis of the optimal information security investment in the case of a risk-averse firm // International journal of production economics. 2008. Т. 114. №. 2. P. 793–804.
10. *Shiau W.L., Wang X., Zheng F*. What are the trend and core knowledge of information security? A citation and co-citation analysis // Information & Management. 2023. Т. 60. №. 3. С. 103774.
11. *Arora H., Raghu T.S., Vinze A*. Autonomic Computing and Information Security // Information Assurance. Security and Privacy Services. 2009. С. 141.
12. *Liu P., Zang W., Yu M*. Incentive-based modeling and inference of attacker intent, objectives, and strategies // ACM Transactions on Information and System Security (TISSEC). 2005. Т. 8. №. 1. P. 78–118.
13. *Veselovsky M.Y., Izmailova M.A., Lobacheva E.N., Pilipenko P.P. and Rybina G.A*. Strategic management of innovation development: Insights into a role of economic policy // Entrepreneurship and Sustainability Issues. 2019. 7 (2), 1296–1307. https://doi.org/10.9770/jesi.2019.7.2(34)
14. *Skvortsova M., Terekhov V., Proletarsky A., Skvortsov V., Kochneva M*. Visualization of Integrated Indicators of Information Risk in Decision Support Systems // in 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2020. P. 2101–2105. https://doi.org/10.1109/EIConRus49466.2020.9038952
15. *Марченкова О.В., Шиболденков В.А*. Анализ перспективных технологий цифровизации в наукоемком секторе экономики / XLVI Академические чтения по космонавтике, посвященные памяти академика С.П. Королева и других отечественных ученых – пионеров освоения космического пространства (Москва, 25–28 янв. 2022 г.): Сб. тез. Всеросс. науч. конф. / РАН [и др.]; ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: Изд-во МГТУ им. Н.Э. Баумана. 2022. Т. 2. С. 87–89.
16. *Шипкова А.Д., Шиболденков В.А*. Научно-аналитическое исследование эффективности использования сквозных цифровых технологий в космической отрасли / XLVI Академические чтения по космонавтике, посвященные памяти академика С.П. Королева и других отечественных ученых – пионеров освоения космического пространства (Москва, 25–28 янв. 2022 г.): Сб. тез. Всеросс. науч. конф. / РАН [и др.]; ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: Изд-во МГТУ им. Н.Э. Баумана. 2022. Т. 2. С. 195–202.
17. *Михненко П.А*. Цифровой менеджмент: модели развития концепции // Инновации в менеджменте. 2020. № 3 (25). С. 30–39.
18. *Авдеева М.В., Воротникова С.С., Шиболденков В.А*. Обзор цифровых решений на основе технологии распределенного реестра для обеспечения верифицируемости бизнес-процессов на наукоемком предприятии аэрокосмической отрасли / XLVII Академические чтения по космонавтике, посвященные памяти академика С.П. Королева и других отечественных ученых – пионеров освоения космического пространства (Москва, 24–27 янв. 2023 г.): Сб. тез. / РАН [и др.]; ФГБОУ ВО «Москов-

ский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: Изд-во МГТУ им. Н.Э. Баумана. 2023. Т. 1. С. 384–385.

19. *Шиболденков В.А*. Цифровая трансформация проектной деятельности в наукоемкой организации космической отрасли / Аэрокосмические технологии (Реутов, 28 мая 2019 г.): Сб. материалов Междунар. молодеж. науч.-техн. конф., посвященной 105-летию со дня рождения академика В.Н. Челомея / ОАО «ВПК «НПО машиностроения»; ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: ВПК «НПО машиностроения»; МГТУ им. Н.Э. Баумана. 2019. С. 135–136.
20. *Кашеварова Н.А., Шиболденков В.А*. Цифровые инструменты гибкого проектного управления при организации инкрементальных инноваций в космической отрасли / XLIV Академические чтения по космонавтике, посвященные памяти академика С.П. Королева и других отечественных ученых – пионеров освоения космического пространства (Москва, 28–31 янв. 2020 г.): Сб. тез. Всерос. науч. конф. / РАН [и др.]; ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)». М.: Изд-во МГТУ им. Н.Э. Баумана. 2020. Т. 1. С. 364–366.

Информация о авторе

Михаил Александрович Павлов – соискатель
SPIN-код: не представлен

Статья поступила в редакцию 03.07.2024
Одобрена после рецензирования 15.07.2024
Принята к публикации 23.07.2024

Original article

Management frameworks information technology and cyber risks during the digital transformation of the organization

M.A. Pavlov[1]

[1] Bauman Moscow State Technical University (Moscow, Russia)
[1] mikhail.pavlov.mgimosgp@gmail.com

Abstract

Problem statement. It is necessary to effectively manage the implementation of digital security measures of an organization to ensure the cybersecurity of an information system in the context of digital transformation and minimize the risk of possible losses and security breaches.
Goal. Perform a comprehensive analysis and benchmarking of frameworks in this area.
Results. The main documents regulating cybersecurity and IT risks in digital transformation are analyzed, standard guidelines, recommendations and frameworks for information security and cybersecurity management are analyzed. System solutions for the development of a cyber and digital security strategy have been identified.
Practical significance. A model of a cybersecurity and business continuity management system in the context of an organization's digital transformation is proposed. Recommendations for the organization's digital security management mechanism are described.

Keywords

Cybersecurity, information technology, frameworks, digital security

For citation

Pavlov M.A. Management frameworks information technology and cyber risks during the digital transformation of the organization. Dynamics of complex systems. 2024. V. 18. № 3. P. 23–33. DOI: 10.18127/j19997493-202403-03 (in Russian).

References

1. Drogovoz P.A., Koren'kova D.A., Pavlov M.A. Kiberbezopasnost' v mezhdunarodnoj kosmicheskoj industrii: kooperativno-igrovoj podhod k garmonizacii jekonomicheskih interesov stejkholderov. XLVI Akademicheskie chtenija po kosmonavtike, posvjashhennye pamjati akademika S.P. Koroleva i drugih otechestvennyh uchenyh – pionerov osvoenija kosmicheskogo prostranstva (Moskva, 25–28 janv. 2022 g.): Sb. tez. Vseros. nauch. konf. / RAN [i dr.]; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: Izd-vo MGTU im. N.Je. Baumana. 2022. T. 2. S. 48–54.
2. Drogovoz P.A., Koren'kova D.A. Sovremennyj instrumentarij gibkogo upravlenija IT-proektami i perspektivy ego sovershenstvovanija s ispol'zovaniem tehnologij iskusstvennogo intellekta. Jekonomika i predprinimatel'stvo. 2019. № 10. S. 829–833.
3. Drogovoz P.A., Jusufova O.M., Koren'kova D.A. Cifrovaja transformacija proizvodstvennyh sistem: obzor osnovnyh napravlenij i faktorov razvitija. X Charnovskie chtenija (Moskva, 4–5 dek. 2020 g.): Cb. trudov Vseros. nauch. konf.i po organizacii proizvodstva / FGBOU VO «Moskovskij gosudarstvennyj universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)» [i dr.]. M.: NOC «Kontrolling i upravlencheskie innovacii». 2021. S. 61–68.
4. Drogovoz P.A., Pushkareva P.P. Specifika upravlenija investicionnymi riskami v naukoemkoj promyshlennosti. Budushhee mashinostroenija Rossii (Moskva, 22–25 sen. 2020 g.): Cb. dokladov XXIII Vseros. nauch. konf. molodyh uchenyh i specialistov (s mezhdunar. uchastiem): v 2 t. T. 2 / Sojuz mashinostroitelej Rossii, Moskovskij gosudarstvennyj universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet). M.: Izd-vo MGTU im. N.Je. Baumana. 2020. S. 371–373.
5. Drogovoz P.A., Raldugin O.V. Matematicheskoe modelirovanie riskov kooperacii po sozdaniju sistemy vozdushno-kosmicheskoj oborony. XLIII Akademicheskie chtenija po kosmonavtike, posvjashhennye pamjati akademika S.P. Koroleva i drugih otechestvennyh uchenyh – pionerov osvoenija kosmicheskogo prostranstva (Moskva, 29 janv. – 1 fev. 2019 g.): Sb. tez. vseross. nauch. konf. / RAN [i dr.]; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: Izd-vo MGTU im. N.Je. Baumana. 2019. T. 1. S. 167–169.
6. Drogovoz P.A., Raldugin O.V. Informacionno-tehnologicheskie faktory razvitija kooperacii v oboronno-promyshlennom komplekse i risk-orientirovannyj podhod k ee formirovaniju pri sozdanii sistemy vozdushno-kosmicheskoj oborony. Jekonomicheskie strategii. 2016. T. 18. № 7 (141). S. 76–89.
7. Drogovoz P.A., Kashevarova N.A., Dadonov V.A., Sadovskaya T.G. and Trusevich M.K. Industry 4.0 in Russia: Digital Transformation of Economic Sectors. in Industry 4.0 in SMEs Across the Globe: Drivers, Barriers, and Opportunities, edited by J.M. Müller, N. Kazantsev (CRC Press, Boca Raton, 2021). P. 195–211. https://doi.org/10.1201/9781003165880-15
8. Jerman-Blažič B. et al. An economic modelling approach to information security risk management. International Journal of Information Management. 2008. V. 28. №. 5. S. 413–422.
9. Huang C.D., Hu Q., Behara R.S. An economic analysis of the optimal information security investment in the case of a risk-averse firm. International journal of production economics. 2008. V. 114. №. 2. S. 793–804.
10. Shiau W. L., Wang X., Zheng F. What are the trend and core knowledge of information security? A citation and co-citation analysis. Information & Management. 2023. V. 60. №. 3. S. 103774.
11. Arora H., Raghu T.S., Vinze A. Autonomic Computing and Information Security. Information Assurance, Security and Privacy Services. 2009. S. 141.
12. Liu P., Zang W., Yu M. Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security (TISSEC). 2005. V. 8. №. 1. S. 78–118.

13. Veselovsky M.Y., Izmailova M.A., Lobacheva E.N., Pilipenko P.P. and Rybina G.A. Strategic management of innovation development: Insights into a role of economic policy. Entrepreneurship and Sustainability Issues. 2019. 7 (2), 1296–1307. https://doi.org/10.9770/jesi.2019.7.2(34)
14. Skvortsova M., Terekhov V., Proletarsky A., Skvortsov V., Kochneva M. Visualization of Integrated Indicators of Information Risk in Decision Support Systems. in 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2020. P. 2101–2105. https://doi.org/10.1109/EIConRus49466.2020.9038952
15. Marchenkova O.V., Shiboldenkov V.A. Analiz perspektivnyh tehnologij cifrovizacii v naukoemkom sektore jekonomiki. XLVI Akademicheskie chtenija po kosmonavtike, posvjashhennye pamjati akademika S.P. Koroleva i drugih otechestvennyh uchenyh – pionerov osvoenija kosmicheskogo prostranstva (Moskva, 25–28 janv. 2022 g.): Sb. tez. Vseros. nauch. konferencii / RAN [i dr.]; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: Izd-vo MGTU im. N.Je. Baumana. 2022. T. 2. S. 87–89.
16. Shipkova A.D., Shiboldenkov V.A. Nauchno-analiticheskoe issledovanie jeffektivnosti ispol'zovanija skvoznyh cifrovyh tehnologij v kosmicheskoj otrasli. XLVI Akademicheskie chtenija po kosmonavtike, posvjashhennye pamjati akademika S.P. Koroleva i drugih otechestvennyh uchenyh – pionerov osvoenija kosmicheskogo prostranstva (Moskva, 25–28 janv. 2022 g.): Sb. tez. Vseros. nauch. konferencii / RAN [i dr.]; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: Izd-vo MGTU im. N.Je. Baumana. 2022. T. 2. S. 195–202.
17. Mihnenko P.A. Cifrovoj menedzhment: modeli razvitija koncepcii. Innovacii v menedzhmente. 2020. № 3 (25). S. 30–39.
18. Avdeeva M.V., Vorotnikova S.S., Shiboldenkov V.A. Obzor cifrovyh reshenij na osnove tehnologii raspredelennogo reestra dlja obespechenija verificiruemosti biznes-processov na naukoemkom predprijatii ajerokosmicheskoj otrasli. XLVII Akademicheskie chtenija po kosmonavtike, posvjashhennye pamjati akademika S.P. Koroleva i drugih otechestvennyh uchenyh – pionerov osvoenija kosmicheskogo prostranstva (Moskva, 24-27 janv. 2023 g.): Sb. tez. / RAN [i dr.]; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: Izd-vo MGTU im. N.Je. Baumana. 2023. T. 1. S. 384–385.
19. Shiboldenkov V.A. Cifrovaja transformacija proektnoj dejatel'nosti v naukoemkoj organizacii kosmicheskoj otrasli. Ajerokosmicheskie tehnologii (Reutov, 28 maja 2019 g.): Sb. materialov Mezhdunar. molodezh. nauch.-tehn. konf., posvjashhennoj 105-letiju so dnja rozhdenija akademika V.N. Chelomeja / OAO «VPK «NPO mashinostroenija»; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: VPK «NPO mashinostroenija»; MGTU im. N.Je. Baumana. 2019. S. 135–136.
20. Kashevarova N.A., Shiboldenkov V.A. Cifrovye instrumenty gibkogo proektnogo upravlenija pri organizacii inkremental'nyh innovacij v kosmicheskoj otrasli. XLIV Akademicheskie chtenija po kosmonavtike, posvjashhennye pamjati akademika S.P. Koroleva i drugih otechestvennyh uchenyh – pionerov osvoenija kosmicheskogo prostranstva (Moskva, 28-31 janv. 2020 g.): Sb. tez. Vseros. nauch. konf. / RAN [i dr.]; FGBOU VO «Moskovskij gosudarstvennyj tehnicheskij universitet imeni N.Je. Baumana (nacional'nyj issledovatel'skij universitet)». M.: Izd-vo MGTU im. N.Je. Baumana, 2020. T. 1. S. 364–366.

Information about the authors

Mikhail A. Pavlov – Applicant

The article was submitted 03.07.2024
Approved after reviewing 15.07.2024
Accepted for publication 23.07.2024