УКД 33

Эволюция стандартов безопасности данных в условиях цифровой трансформации: от оцифровки к smart-предприятиям

Цибулина Екатерина Владимировна

Аспирант,
Московский государственный
технологический университет «СТАНКИН»,
127994, Российская Федерация, Москва, пер. Вадковский, 1;
e-mail: katsibulina@gmail.com

Попов Дмитрий Владимирович

Кандидат экономических наук, профессор,
Московский государственный
технологический университет «СТАНКИН»,
127994, Российская Федерация, Москва, пер. Вадковский, 1;
e-mail: d.popov@stankin.ru

Аннотация

В статье рассматривается эволюция стандартов обеспечения безопасности данных в контексте цифровой трансформации предприятий – от этапа оцифровки до перехода к smart-предприятиям. Проанализированы ключевые нормативные документы и международные стандарты (включая ISO/IEC 27001, NIST, GDPR, ФЗ-152), отражающие изменения в подходах к защите информации. Особое внимание уделено вызовам, возникающим при внедрении облачных технологий, Интернета и автоматизированных систем управления. Обоснована необходимость гибкой адаптации регуляторных механизмов к новым цифровым рискам. На основе анализа кейсов в промышленности и финансовом секторе предложены направления совершенствования стандартов безопасности, способствующие устойчивому развитию цифровых организаций.

Для цитирования в научных исследованиях

Цибулина Е.В., Попов Д.В. Эволюция стандартов безопасности данных в условиях цифровой трансформации: от оцифровки к smart-предприятиям // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 4А. С. 795-801.

Ключевые слова

Цифровая трансформация, информационная безопасность, стандарты, ISO/IEC 27001, smart-предприятие, регулятор, риски.

Введение

Цифровая трансформация представляет собой многоэтапный процесс внедрения цифровых технологий в деятельность организации. Первоначальным этапом является оцифровка (digitization), под которой понимается технический процесс преобразования аналоговых данных в цифровой формат посредством сканирования, оцифровки документов и баз данных. На данном этапе основное внимание уделяется вопросам корректного перевода информации в цифровую форму и обеспечения её долговременного хранения. Следующей стадией выступает цифровизация (digitalization), предполагающая использование цифровых технологий для модернизации бизнес-процессов. В рамках этого этапа происходит внедрение специализированных цифровых инструментов, таких как системы электронного документооборота и онлайн-сервисы, что приводит к трансформации традиционных методов работы с данными, автоматизации рутинных операций и созданию новых цифровых сервисов.

Более глубоким уровнем преобразований является цифровая трансформация (digital transformation), представляющая собой комплексное переосмысление бизнес-моделей организации на основе цифровых технологий. Согласно определению Gartner, данный процесс включает модернизацию IT-инфраструктуры, внедрение методов цифровой аналитики и разработку инновационных бизнес-моделей. В отличие от цифровизации, цифровая трансформация затрагивает все аспекты деятельности предприятия: операционные процессы, систему управления, а также характеристики выпускаемой продукции и оказываемых услуг.

Высшей стадией развития рассматриваемого процесса выступает формирование smart-предприятий, соответствующих принципам Индустрии 4.0. Такие предприятия характеризуются наличием интеллектуальной автоматизированной инфраструктуры, включающей технологии интернета вещей (IoT), промышленного интернета вещей (IIoT), искусственного интеллекта и обработки больших данных. Цифровые платформы smart-предприятий обеспечивают мониторинг и оптимизацию производственных процессов в режиме реального времени. При этом достижение данного уровня цифровой зрелости требует разработки новых подходов к обеспечению кибербезопасности, направленных на защиту не только информационных систем, но и встроенных киберфизических компонентов производственной инфраструктуры.

Основное содержание

Рассмотрим основные стандарты управления информационной безопасностью.

Стандарт ISO/IEC 27001 задает требования к системе менеджмента информационной безопасности (ISMS). По нему организация должна определить политику и процедуры защиты конфиденциальности, целостности и доступности данных. ISO 27001 – широко признанный «золотой стандарт» в сфере ИБ, обеспечивающий системный подход к управлению рисками (люди, процессы, технологии). Соответствие ему означает, что компания внедрила комплексную систему защиты данных.

Регламент GDPR (ЕС). В Евросоюзе действует Регламент (ЕС) 2016/679 (GDPR), вступивший в силу в мае 2018 года. GDPR установил единые правила обработки персональных данных во всех странах ЕС и Шенгенской зоны, существенно усилив права субъектов данных (право доступа, удаления «право быть забытым», уведомление об утечках). Регламент вводит

жесткие требования к безопасности и конфиденциальности, а за их нарушение предусмотрены крупные штрафы (до 4% годового оборота компании). Кроме того, в рамках кибербезопасности ЕС принял Директиву NIS (2016) и новую NIS2 (2022) для защиты критических цифровых сервисов, а также Регламент DORA (2022) для повышения устойчивости цифровых систем в финансовом секторе.

Директива NIS (ЕС). Директива (ЕС) 2016/1148 по безопасности сетей и информационных систем (NIS) требует от государств – членов ЕС внедрения мер защиты критических информационных систем (энергетика, транспорт, финансы, инфраструктура и т.д.). Компании обязаны сообщать о киберинцидентах национальным органам. NIS стала первым общеевропейским нормативом в области кибербезопасности и сейчас заменяется директивой NIS2, расширяющей круг защищаемых объектов и ужесточения требований.

Российские законы (152№ФЗ, 187№ФЗ и др.). В РФ главным законом по защите персональных данных является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Закон регламентирует порядок сбора, хранения и защиты персональной информации граждан (право на согласие, обязанности оператора, меры безопасности при обработке). Для критических отраслей принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» (2017), устанавливающий требования к организациям из энергетики, финансов, транспорта, здравоохранения и другим секторам, обеспечивающим жизненно важные функции. Кроме того, существуют стандарты ФСТЭК и ФСБ, регламенты Центробанка РФ для финансов (PCI DSS и др.), а также ГОСТ Р 56939-2016 (менеджмент ИБ). Эта нормативная база ориентирована в основном на традиционные ИТ- и телеком-системы, хотя постепенно охватывают и новые технологии (например, криптозащита, системы обнаружения атак).

Законодательство США (HIPAA, GLBA и др.). В Соединенных Штатах нет единого комплексного закона по безопасности ИТ, вместо этого действуют отраслевые регламенты. Так, HIPAA Security Rule (1996/2003) устанавливает федеральные стандарты для защиты электронной медицинской информации (электронного PHI) в здравоохранении. HIPAA требует от «контроллеров» и «обработчиков» (больницы, страховые) вводить административные, технические и физические меры защиты данных о пациентах. Другой крупный закон – Gramm-Leach-Bliley Act (1999) – обязывает финансовые организации защищать данные клиентов и раскрывать им политику обмена информацией. Кроме того, регуляторы отраслей (Федрезерв, SEC, CFPB) устанавливают свои рекомендации и правила (например, требования FFIEC к банкам). В США также широко используются стандарты NIST (Cybersecurity Framework) и ISO, но многие требования носят добровольный характер или реализуются через нормативы на уровне отдельных штатов (например, калифорнийский CCPA).

Приведем примеры инцидентов, связанных и цифровизацией промышленности.

CDK Global (США, 2024) – атака с использованием шифровальщика на поставщика ИТ-услуг для автодилеров США. В результате пострадали около 15 000 компаний, прямой ущерб оценён в ~$1 млрд. Этот инцидент показал уязвимость экосистемы малого и среднего бизнеса при отсутствии единых требований к безопасности поставщиков.

Hoya Corporation (Япония, 2024) – крупнейший японский производитель оптических линз подвергся кибератаке, в ходе которой злоумышленники получили доступ к IT-системам предприятия. При атаке был нарушен операционный процесс и похищены небольшие объёмы данных. Инцидент выявил риски для промышленности при недостаточной сегментации сетей и

слабой защите серверов.

Equifax (США, 2017) – одна из крупнейших утечек данных в финансовом секторе: пострадали персональные данные ~147 млн человек. Причиной стали давно известные уязвимости в ПО и ошибки компании (несвоевременное применение патчей, слабые пароли). После этого США ужесточили надзор за финансовыми и кредитными учреждениями, хотя законодательства (например, обязательные уведомления клиентов) были введены уже после факта.

Рост числа инцидентов в промышленности (Россия, 2023–2025). Отраслевые СМИ отмечают рост кибератак на российские промышленные предприятия (энергетика, машиностроение, пищевая промышленность и др.) на фоне цифровизации бизнеса. Скорость цифрового развития заводов опережает темпы внедрения мер киберзащиты. Частые случаи хакерских атак и программ-вымогателей свидетельствуют, что регуляторные требования (многие из которых заточены под традиционные ИТ) пока не успевают покрыть новые связанные с IoT и автоматизацией риски.

Регулирование кибербезопасности отличается в зависимости от стадии цифровой зрелости и региона. В *начальной оцифровке* (перевод данных в цифровую форму) основное внимание уделяется базовым правовым нормам хранения информации (архивация, ИТ-безопасность первичной обработки). По мере *цифровизации процессов* правительства вводят отраслевые стандарты и нормативы на защиту сетей и систем (например, законы об информатизации, регламенты для госсектора и Банка России). С началом *цифровой трансформации* усиливаются требования к комплексному управлению рисками: в ЕС принят GDPR, регулирующий массовую обработку персональных данных, и DORA для финансов, а в РФ действуют ФЗ-152 и ФЗ-187. В США продолжает доминировать *секторный подход*: отраслевые акты (HIPAA для медицины, GLBA для финансов и т.д.) адаптируются к новым реалиям через доп. требования регуляторов, но нет единого закона для всех секторов.

Сходства и различия: ЕС стремится к унификации (общие стандарты, строгие штрафы), США – к гибкости и инновационному саморегулированию, Россия – к централизованному контролю в стратегических отраслях. Для каждого этапа трансформации важна *комбинация технологий и права*: на стадии smart-предприятия требуются новые регламенты для IoT, облаков и ИИ, а также адаптация существующих норм (например, ФЗ-149 «Об информации» постепенно включает положения об электронной подписи и блокчейне). Наработки стандартов (ISO/IEC 27001:2022) и международный опыт (NIST CSF, COBIT, CIS Controls) помогают выравнивать подходы, но различия в акцентах остаются.

Заключение

В современных условиях цифровой трансформации выявлены следующие проблемы существующих нормативов:

1) *Фрагментарность законодательства*. Часто новые технологии (IoT, облака, ИИ) выпадают из сферы действия устаревших законов. Например, ФЗ-152 не изначально учитывал алгоритмическую обработку или киберугрозы.
2) *Отставание регуляторов*. Законодательство плохо успевает за стремительным развитием технологий: инциденты выявляют «белые пятна» в правилах (как показал рост кибератак на автоматизированные системы предприятий.

3) *Нехватка координации на глобальном уровне*. Несмотря на GDPR, нет единых международных норм для обмена данными и совместной защиты, что создает сложности для транснационального бизнеса и облачных сервисов.

Возможные пути решения:

1) *Комплексная модернизация стандартов*. Рекомендуется регулярное обновление стандартов ИБ (ISO, ГОСТ), учитывающее новые типы угроз (например, киберфизические атаки, квантовую криптографию).
2) *Унификация и интернационализация регуляций*. Координация между странами (двусторонние соглашения, участие в глобальных инициативах) поможет выработать общие правила защиты персональных и критических данных.
3) *Интеграция «Security by Design».* Нормативы должны требовать закладывать ИБ на этапе проектирования цифровых систем и «умных» производств security by design, а не вводить меры постфактум.
4) *Повышение ответственности бизнеса.* Ужесточение контроля и повышение штрафов за несоблюдение требований (как в GDPR) стимулирует компании активнее инвестировать в защиту. Одновременно нужны меры поддержки (стандартизация, сертификация) для малых предприятий.
5) *Обучение и кадры.* Для эффективного применения новых правил критически важно готовить квалифицированных специалистов в области кибербезопасности, особенно в промышленности и финансовом секторе, что позволит быстрее адаптироваться к изменяющимся угрозам.

В целом, дальнейшее повышение безопасности данных при цифровой трансформации возможно только при сбалансированном подходе «технологии + право»: нужно оперативно обновлять законодательство по новым видам цифровых рисков и параллельно развивать лучшие практики и стандарты защиты.

Библиография

1. ГОСТ Р ИСО/МЭК 27001-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.
2. О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 05.04.2024).
3. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31 июля 2020 г. № 259-ФЗ. URL: http://www.kremlin.ru/acts/bank/45766 (дата обращения: 05.04.2024).
4. Об утверждении концепции регулирования искусственного интеллекта и робототехники в Российской Федерации до 2030 года: постановление Правительства РФ от 13.12.2021 № 2299. URL: https://www.garant.ru/products/ipo/prime/doc/402963342 (дата обращения: 05.04.2024).
5. Попов Д.В., Ральникова К.В., Кутикова С.П. Оценка уровня цифровой трансформации организации на основе управленческой документации // Цифровая экономика. 2023. № 3(24). С. 65-75.
6. Цибулина Е.В., Попов Д.В. Разработка модели уровня цифровой трансформации на основе рисков, связанных с безопасностью организации // Экономика: вчера, сегодня, завтра. 2024. Т. 14. № 4А. С. 732-738.
7. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 05.04.2024).
8. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization. URL: https://www.iso.org/standard/27001 дата обращения: 05.04.2024).
9. National Institute of Standards and Technology (NIST). (2020). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата обращения: 05.04.2024).

10. Stewart H. Digital transformation security challenges // Journal of Computer Information Systems. 2023. No. 63(4). P. 919-936.

Evolution of data security standards in the context of digital transformation: from digitization to smart enterprises

Ekaterina V. Tsibulina

Postgraduate Student,
Moscow State Technological University "STANKIN",
127994, 1 Vadkovskii lane, Moscow, Russian Federation;
e-mail: katsibulina@gmail.com

Dmitrii V. Popov

PhD in Economics, Professor,
Moscow State Technological University "STANKIN",
127994, 1 Vadkovskii lane, Moscow, Russian Federation;
e-mail: d.popov@stankin.ru

Abstract

The article examines the evolution of data security standards in the context of digital transformation — from the digitization phase to the emergence of smart enterprises. It analyzes key regulatory frameworks and international standards (including ISO/IEC 27001, NIST, GDPR, and Federal Law No. 152) that reflect the changing approaches to information protection. Special attention is given to challenges related to the implementation of cloud technologies, the Internet of Things, and automated control systems. The need for flexible adaptation of regulatory mechanisms to new digital risks is substantiated. Based on case studies in the industrial and financial sectors, the paper outlines directions for improving security standards that support the sustainable development of digitally transformed organizations.

For citation

Tsibulina E.V., Popov D.V. (2025) Evolyutsiya standartov bezopasnosti dannykh v usloviyakh tsifrovoi transformatsii: ot otsifrovki k smart-predpriyatiyam [Evolution of data security standards in the context of digital transformation: from digitization to smart enterprises]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (4A), pp. 795-801.

Keywords

Digital transformation, information security, standards, ISO/IEC 27001, smart enterprise, regulation, risks.

References

1. European Union. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 05.04.2024].
2. GOST R ISO/IEC 27001-2021. (2021) Informatsionnye tekhnologii. Metody i sredstva obespecheniya bezopasnosti.

Sistemy menedzhmenta informatsionnoy bezopasnosti. Trebovaniya [Information Technology. Security Techniques. Information Security Management Systems. Requirements]. Moscow: Standartinform Publ.

3. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization. (2022). Available at: https://www.iso.org/standard/27001 [Accessed 05.04.2024].
4. National Institute of Standards and Technology (NIST). (2020) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 05.04.2024].
5. O personalnykh dannykh: feder. zakon ot 27 iyulya 2006 g. № 152-FZ [On Personal Data: Federal Law No. 152-FZ of July 27, 2006]. (2006). Available at: https://www.consultant.ru/document/cons_doc_LAW_61801 [Accessed 05.04.2024].
6. O tsifrovykh finansovykh aktivakh, tsifrovoy valyute i o vnesenii izmeneniy v otdelnye zakonodatelnye akty Rossiyskoy Federatsii: feder. zakon ot 31 iyulya 2020 g. № 259-FZ [On Digital Financial Assets, Digital Currency and on Amending Certain Legislative Acts of the Russian Federation: Federal Law No. 259-FZ of July 31, 2020]. (2020). Available at: http://www.kremlin.ru/acts/bank/45766 [Accessed 05.04.2024].
7. Ob utverzhdenii kontseptsii regulirovaniya iskusstvennogo intellekta i robototekhniki v Rossiyskoy Federatsii do 2030 goda: postanovlenie Pravitelstva RF ot 13.12.2021 № 2299 [On Approval of the Concept for Regulating Artificial Intelligence and Robotics in the Russian Federation until 2030: Decree of the Government of the Russian Federation No. 2299 of December 13, 2021]. (2021). Available at: https://www.garant.ru/products/ipo/prime/doc/402963342 [Accessed 05.04.2024].
8. Popov D.V., Ralnikova K.V., Kutikova S.P. (2023) Otsenka urovnya tsifrovoy transformatsii organizatsii na osnove upravlencheskoy dokumentatsii [Assessing the Level of Digital Transformation of an Organization Based on Management Documentation]. Tsifrovaya ekonomika [Digital Economy], 3(24), p. 65-75.
9. Stewart H. (2023) Digital transformation security challenges. Journal of Computer Information Systems, 63(4), p. 919-936.
10. Tsibulina E.V., Popov D.V. (2024) Razrabotka modeli urovnya tsifrovoy transformatsii na osnove riskov, svyazannykh s bezopasnostyu organizatsii [Developing a Model of Digital Transformation Level Based on Security-Related Risks of the Organization]. Ekonomika: vchera, segodnya, zavtra [Economics: Yesterday, Today, Tomorrow], 14 (4A), p. 732-738.