ЗАКОНОДАТЕЛЬСТВО ЗАРУБЕЖНЫХ СТРАН

Дата поступления рукописи в редакцию: 20.09.2026 г. **DOI: 10.24412/3033-6775-2026-4-49-53**
Дата принятия рукописи в печать: 05.11.2026 г.

КОРОБОВ Илья Андреевич,
соискатель ученой степени кандидата юридических наук,
Университет имени О. Е. Кутафина (МГЮА), Москва, Россия,
e-mail: ya.korobov6@yandex.ru

Научный руководитель:
МИНБАЛЕЕВ Алексей Владимирович,
доктор юридических наук, профессор, заведующий кафедрой информационного права и цифровых технологий Университета имени О. Е. Кутафина (МГЮА),
e-mail: alexmin@bk.ru

ТЕНДЕНЦИИ РАЗВИТИЯ ПУБЛИЧНО-ПРАВОВОГО МЕХАНИЗМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЛОВАЦКОЙ РЕСПУБЛИКЕ

Аннотация. *Исследуются тенденции развития публично-правового механизма обеспечения информационной безопасности в Словацкой Республике. Обосновывается переход от формального подтверждения соответствия к управляемой киберустойчивости, при которой правовая обязанность связывается с измеримым результатом и проверяемым доказательством. На основе словацких стратегических и методических документов, материалов государственного контроля и постинцидентных обзоров раскрывается замкнутый цикл управления: обязанность, показатель, доказательство, контроль, корректирующее решение и повторная проверка. Предлагаются требования к плану реализации государственной стратегии и минимальный порядок действий для частной организации.*

Ключевые слова: *Словакия, информационная безопасность, киберустойчивость, публичное управление, управление риском, аудит, киберинцидент, малое и среднее предпринимательство.*

KOROBOV Ilya Andreevich,
Candidate of Legal Sciences degree applicant,
Kutafin Moscow State Law University (MSAL), Moscow, Russia

Academic Supervisor:
MINBALEEV Alexey Vladimirovich,
Doctor of Legal Sciences, Professor, Head of the Department of Information Law and Digital Technologies at the Kutafin Moscow State Law University (MSAL)

TRENDS IN THE DEVELOPMENT OF THE PUBLIC-LAW INFORMATION SECURITY MECHANISM IN THE SLOVAK REPUBLIC

Annotation. *The article examines trends in the development of the public-law information security mechanism in the Slovak Republic. It substantiates a transition from formal compliance to managed cyber resilience, in which a legal duty is linked to a measurable outcome and verifiable evidence. Slovak strategic and methodological documents, public*

audit findings, and post-incident reviews are used to formulate a closed governance cycle consisting of duty, indicator, evidence, control, corrective decision, and repeated verification. Requirements for a public strategy implementation plan and a minimum action sequence for private organisations are proposed.

Key words: *Slovakia, information security, cyber resilience, public administration, risk management, audit, cyber incident, small and medium-sized enterprises.*

Развитие публично-правового механизма обеспечения информационной безопасности в Словацкой Республике определяется не количеством принятых актов, а способностью государства и регулируемых субъектов поддерживать общественно значимые функции при инциденте. Национальная стратегия кибербезопасности на 2026–2030 годы связывает защиту киберпространства с устойчивостью публичных услуг, поддержкой малых и средних предприятий, развитием компетенций и международным взаимодействием [1, с. 18–25, 33–36]. Из этого следует критерий правовой результативности: обязанность исполнена не тогда, когда утверждён очередной документ, а когда субъект может обнаружить нарушение, ограничить его последствия, восстановить услугу и подтвердить устранение причины.

Стратегический документ задаёт направление, но не определяет сам по себе исполнителя, срок, ресурс и способ проверки. Поэтому первой тенденцией становится переход от декларативной цели к измеримому плану. В словацких материалах цифровой политики используются показатели, относящиеся к работе центров мониторинга безопасности, команд реагирования на компьютерные инциденты, непрерывности деятельности и учениям [1, с. 33]. Для правового контроля показатель полезен лишь при наличии исходного и целевого значения, ответственного органа, источника данных и порядка независимой проверки. Число совещаний или закупленных средств отражает действие, но не доказывает готовность восстановить государственную услугу в установленный срок.

Для правовой оценки следует различать мероприятие, меру защиты, доказательство и результат. Их смешение создаёт формальное соответствие: наличие политики выдаётся за защищённость, а поставка оборудования — за устойчивость. Минимальная структура государственного плана должна включать исполнителя, срок, ресурс, показатель результата, источник доказательств, проверяющий орган и последствия невыполнения. Изменение срока или показателя требует мотивированного решения.

Второй тенденцией является замена разовой оценки непрерывным управлением риском. Методика Национального управления безопасности Словацкой Республики предлагает двигаться от активов и процессов к угрозам, уязвимостям, сценариям и последствиям, а затем выбирать способ обращения с риском: его снижение, избегание, перенос либо принятие в допустимых пределах [3, с. 4–7, 20–21, 30–36]. Юридически значим не общий вывод о возможности кибератаки, а связь между конкретной услугой, сценарием нарушения, выбранной мерой, владельцем риска и остаточным риском. Назначение владельца не освобождает руководство от утверждения допустимого уровня риска и предоставления необходимых ресурсов.

Третья тенденция выражается в доказательном характере аудита. Словацкая методика аудита требует основывать вывод о соответствии или несоответствии на проверяемых записях и фактических сведениях [4, с. 4–9, 16–18]. Поэтому утверждённый регламент должен дополняться журналом событий, результатом восстановления резервной копии, протоколом тестирования, подтверждением устранения уязвимости и повторной проверкой. Государственный контроль в таком случае отвечает не на вопрос, имеется ли документ, а на вопрос, работает ли предусмотренная им мера в отношении установленного риска. Аудит, который заканчивается перечнем замечаний без владельцев, сроков и последующей проверки, не замыкает управленческий цикл.

Выводы Высшего контрольного управления Словацкой Республики о национальной системе управления киберинцидентами показывают: формальное распределение компетенции ещё не обеспечивает согласованного реагирования [5, с. 4–10]. Выявленное отклонение должно изменять план, бюджет, конфигурацию системы либо порядок взаимодействия. Иначе сведения о риске превра-

щаются в архивную отчётность.

Четвёртая тенденция связана с проверкой готовности посредством учений. Цель «повысить готовность» непригодна для оценки. Проверяемая цель должна устанавливать, способен ли орган за заданное время определить масштаб события, назначить руководителя реагирования, уведомить компетентные органы, сохранить доказательства и восстановить приоритетную услугу. Методика Агентства Европейского союза по кибербезопасности разделяет планирование, проведение и оценку учения и требует переводить выявленные недостатки в последующие действия [6, с. 36–50, 52–66]. Публично-правовая оценка охватывает не только технический успех: решение об изоляции системы должно быть принято уполномоченным лицом, учитывать последствия ограничения услуги и фиксироваться так, чтобы его можно было проверить.

Практическое значение подхода видно на примере словацкого кадастра. Государственный контроль установил множественность используемых систем, устаревание части решений и отсутствие единой завершённой платформы. Эти сведения не доказывают способ атаки 2025 года, но показывают среду зависимостей, затрудняющую восстановление. Заключённый после инцидента договор связывает приёмку с испытаниями, требует проверять известные уязвимости, покрытие исходного кода тестами и результаты статического анализа [7, с. 2, 5–6, 10; 8, с. 4, 7, 16–20, 29, 34]. Результат закупки определяется возможностью заказчика проверить безопасность решения, а не передачей оборудования.

Постинцидентные материалы подтверждают системный характер ущерба. Обзор атаки Conti на ирландскую службу здравоохранения установил длительное присутствие нарушителя, компрометацию привилегированных учётных записей и запоздалую централизованную реакцию [9, с. 34, 55–59, 99–103, 115–130]. При атаке WannaCry предупреждения и обновления существовали, но их установку не подтверждали, а национальный план не был проверен на местном уровне [10, с. 8, 11–12, 18–21, 26–27]. В обоих случаях кризис возник из совокупности организационных и технических зависимостей.

Правовая оценка мер безопасности также не допускает автоматической ответственности за сам факт успешной атаки. Суд Европейского союза в деле C-340/21 указал, что несанкционированный доступ третьих лиц сам по себе не доказывает ненадлежащий характер технических и организационных мер; суд должен оценить их содержание и достаточность с учётом обстоятельств конкретного случая [11, пп. 29–60; с. 10–14, 18]. Этот вывод усиливает значение доказательств: организация обязана показать, какой риск она учитывала, почему выбрала соответствующую меру, как проверяла её действие и что изменила после инцидента.

Предлагается замкнутый цикл публичного управления: обязанность — показатель — доказательство — контроль — корректирующее решение — повторная проверка. Обязанность определяет защищаемую функцию; показатель переводит её в проверяемое состояние; доказательство подтверждает исполнение; контроль выявляет отклонение; решение назначает действие, владельца и срок; повторная проверка устанавливает устранение причины. Показатель без надёжных данных, доказательство без критерия и решение без повторной проверки не подтверждают киберустойчивость.

Для государственного органа этот цикл начинается с перечня критичных публичных функций и допустимого времени их недоступности. Затем функции связываются с системами, данными, помещениями, персоналом и поставщиками; назначаются владельцы рисков; устанавливаются показатели; планы проверяются техническими и управленческими учениями; результаты инцидентов переводятся в корректирующие меры. Для частной организации порядок может быть пропорциональным масштабу деятельности: определить услуги и обрабатываемые сведения, установить применимые правовые режимы, вести минимальный реестр активов и поставщиков, ограничить административные права, обеспечить обновления и проверяемое резервирование, подготовить порядок реагирования и провести учебную проверку. Рекомендации ENISA для малых и средних предприятий подтверждают необходимость учитывать безопасность уже на этапе проектирования и проверять её на протяжении жизненного цикла решения [12, с. 11–17, 37–48, 62–70].

Таким образом, основная тенденция развития словацкого механизма состоит в переходе от статического соответствия

к управляемой киберустойчивости. Итоговым показателем служит не отсутствие зарегистрированных инцидентов, которое может объясняться слабым обнаружением, а способность своевременно выявить событие, правомерно ограничить последствия, сохранить доказательства, восстановить услугу и подтвердить устранение системной причины. Предложенный цикл применим к государственному управлению и к бизнесу, но объём мер должен зависеть от критичности функции, состава данных, возможного ущерба и роли субъекта в цепочке поставок.

Список литературы:

[1] Nбrodnə bezpečnostnə ъrad SR. Nбrodnб stratйgia kybernetickej bezpečnosti na roky 2026 až 2030 [Национальная стратегия кибербезопасности на 2026–2030 годы]. 2026. URL: https://rokovania.gov.sk/download.dat?id=B542933D7DD04DB4B207556CA58C0B5D-4C1B546C830E76AB26453C5603555AEB (дата обращения: 03.10.2026).

[2] Ministerstvo investнcin, regionбlneho rozvoja a informatizбcie SR. Kľъčovй vəkonnostnй indikбtory digitбlnej transformбcie a kybernetickej bezpečnosti [Ключевые показатели цифровой трансформации и кибербезопасности]. 2025. URL: https://mirri.gov.sk/wp-content/uploads/2025/12/Klucove-vykonnostne-indikatory.pdf (дата обращения: 03.10.2026).

[3] Nбrodnə bezpečnostnə ъrad SR. Metodika analəzy rizнk kybernetickej bezpečnosti. Verzia 2.0 [Методика анализа рисков кибербезопасности. Версия 2.0]. 2025. URL: https://www.nbu.gov.sk/data/att/3446.pdf (дата обращения: 03.10.2026).

[4] Nбrodnə bezpečnostnə ъrad SR. Metodika auditu kybernetickej bezpečnosti. Verzia 3.0 [Методика аудита кибербезопасности. Версия 3.0]. 2023. URL: https://www.nbu.gov.sk/data/att/2787.pdf (дата обращения: 03.10.2026).

[5] Najvуľљn kontrolnə ъrad SR. Nбrodnə systйm riadenia incidentov kybernetickej bezpečnosti vo verejnej sprбve [Национальная система управления инцидентами кибербезопасности в публичном управлении]. 2023. URL: https://www.nku.gov.sk/documents/33855/590548/b8dabcf8-7393-4f30-a966-d925670fc667.pdf/0e48bf0e-28b0-3f8f-70d6-0a70c7a6eeb3?t=1699827181632 (дата обращения: 03.10.2026).

[6] ENISA. The ENISA Cybersecurity Exercise Methodology [Методика проведения учений по кибербезопасности]. 2026. URL: https://www.enisa.europa.eu/sites/default/files/2026-02/The%20ENISA%20Cybersecurity%20Exercise%20Methodology.pdf (дата обращения: 03.10.2026).

[7] Najvуľљn kontrolnə ъrad SR. Vklady do katastra nehnuteľnostн [Внесение записей в кадастр недвижимости]. 2025. URL: https://www.nku.gov.sk/documents/d/nku/vklady-do-katastra-nehnutelnosti-pdf (дата обращения: 03.10.2026).

[8] Ъrad geodйzie, kartografie a katastra SR. Zmluva o dielo a poskytnutн sъvisiacich služieb č. 1-500-0031-2025 [Договор на проектирование и внедрение решения для предупреждения повторения кибератаки]. 2025. URL: https://www.crz.gov.sk/data/att/6042365.pdf (дата обращения: 03.10.2026).

[9] Health Service Executive; PwC. Conti Cyber Attack on the HSE: Independent Post Incident Review [Кибератака Conti на HSE: независимый постинцидентный обзор]. 2021. URL: https://about.hse.ie/api/v2/download-file/file_based_publications/conti_cyber_attack_on_the_hse_full_report.pdf (дата обращения: 03.10.2026).

[10] National Audit Office. Investigation: WannaCry Cyber Attack and the NHS [Расследование кибератаки WannaCry и Национальной службы здравоохранения]. 2018. URL: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (дата обращения: 03.10.2026).

[11] Court of Justice of the European Union. Judgment of 14 December 2023, C-340/21, Natsionalna agentsia za prihodite [Суд Европейского союза. Решение от 14 декабря 2023 г. по делу C-340/21]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021CJ0340 (дата обращения: 03.10.2026).

[12] ENISA. Secure by Design and Default Playbook for SMEs [Практическое руководство по безопасности на этапе проектирования и по умолчанию для малых и средних предприятий]. 2026. URL: https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_Secure_By_Design_and_Default_Playbook_v1.pdf (дата обращения: 03.10.2026).

References:

[1] Nбrodnə bezpečnostnə ъrad SR.

Nбrodnб stratйgia kybernetickej bezpečnosti na roky 2026 až 2030 [National Cyber Security Strategy for 2026–2030]. 2026. URL: https://rokovania.gov.sk/download.dat?id=B542933D7DD04DB4B207556CA58C0B5D-4C1B546C830E76AB26453C5603555AEB (access date: 10/03/2026).

[2] Ministerstvo investнcin, regionбlneho rozvoja a informatizбcie SR. Key indicators of digital transformation and cybersecurity]. 2025. URL: https://mirri.gov.sk/wp-content/uploads/2025/12/Klucove-vykonnostne-indikatory.pdf (access date: 10/03/2026).

[3] Nбrodnə bezpečnostnə ъrad SR. Metodika analəzy rizнk kybernetickej bezpečnosti. Verzia 2.0 [Methodology for analyzing cybersecurity risks. Version 2.0]. 2025. URL: https://www.nbu.gov.sk/data/att/3446.pdf (access date: 10/03/2026).

[4] Nбrodnə bezpečnostnə ъrad SR. Metodika auditu kybernetickej bezpečnosti. Verzia 3.0 [Cybersecurity audit methodology. Version 3.0]. 2023. URL: https://www.nbu.gov.sk/data/att/2787.pdf (accessed: 03.10.2026).

[5] Supreme Audit Office of the Slovak Republic. National Cybersecurity Incident Management System in Public Administration. 2023. URL: https://www.nku.gov.sk/documents/33855/590548/b8dabcf8-7393-4f30-a966-d925670fc667.pdf/0e48bf0e-28b0-3f8f-70d6-0a70c7a6eeb3?t=1699827181632 (accessed: 03.10.2026).

[6] ENISA. The ENISA Cybersecurity Exercise Methodology. 2026. URL: https://www.enisa.europa.eu/sites/default/files/2026-02/The%20ENISA%20Cybersecurity%20Exercise%20Methodology.pdf (accessed: 03.10.2026).

[7] Supreme Audit Office of the Slovak Republic. Entries in the Real Estate Cadastre. 2025. URL: https://www.nku.gov.sk/documents/d/nku/vklady-do-katastra-nehnutelnosti-pdf (accessed: 03.10.2026).

[8] Office of Geodesy, Cartography and Cadastre of the Slovak Republic. Contract for Work and Provision of Related Services No. 1-500-0031-2025 [Contract for the design and implementation of a solution to prevent the recurrence of a cyberattack]. 2025. URL: https://www.crz.gov.sk/data/att/6042365.pdf (accessed: 03.10.2026).

[9] Health Service Executive; PwC. Conti Cyber Attack on the HSE: Independent Post Incident Review. 2021. URL: https://about.hse.ie/api/v2/download-file/file_based_publications/conti_cyber_attack_on_the_hse_full_report.pdf (accessed: 03.10.2026).

[10] National Audit Office. Investigation: WannaCry Cyber Attack and the NHS. 2018. URL: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (accessed: 03.10.2026).

[11] Court of Justice of the European Union. Judgment of 14 December 2023, C-340/21, Natsionalna agentsia za prihodite. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021CJ0340 (accessed: 03.10.2026).

[12] ENISA. Secure by Design and Default Playbook for SMEs. 2026. URL: https://www.enisa.europa.eu/sites/default/files/2026-07/ENISA_Secure_By_Design_and_Default_Playbook_v1.pdf (accessed: 03.10.2026).