Публично-правовой механизм защиты информации в Словацкой Республике

Коробов Илья Андреевич
Магистр, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), ya.korobov6@yandex.ru

Исследуется публично-правовой механизм защиты информации в Словацкой Республике. Проблема состоит в разрыве между конституционными пределами обработки, распределением компетенции и фактическим исполнением защитных обязанностей. Объект исследования – отношения по защите информации в публичном управлении и регулируемой предпринимательской деятельности. Использованы формально-юридический и системный методы. Научная новизна заключается в обосновании критериев проверки связей между правовым основанием, решением компетентного субъекта и подтверждённым результатом. На материалах конституционного правосудия и надзорной практики показано, что техническая защищённость не устраняет незаконность обработки, а передача задач подрядчику не прекращает собственных обязанностей организации. Разграничены защита персональных данных, достоверность государственных ресурсов и устойчивость инфраструктуры. Рассмотрены положения Конституции Словацкой Республики, законов о кибербезопасности, об информационных технологиях публичной администрации и о критической инфраструктуре, а также Общего регламента по защите данных. Обоснована необходимость раздельной квалификации обязанностей при происшествии: уведомление надзорного органа о нарушении защиты персональных данных и сообщение о серьёзном киберинциденте не подменяют друг друга. Показано, что полнота механизма определяется не числом выданных предписаний, а подтверждённым исправлением выявленных нарушений. Предложенный подход применим при мотивировании властных решений, организации контроля и определении обязанностей компаний.

Ключевые слова: информационная безопасность, Словацкая Республика, конституционные гарантии, государственное управление, персональные данные, кибербезопасность, надзор, критическая инфраструктура.

Введение

Публично-правовая защита информации требует согласовать допустимость вмешательства в права, компетенцию государственных органов и обязанности владельцев информационных процессов. Раздельное рассмотрение этих вопросов создаёт практический разрыв: технически защищённая система может осуществлять незаконную обработку, а обработка, имеющая законное основание, – оставаться незащищённой. Объект исследования составляют отношения по защите информации в публичном управлении и регулируемой предпринимательской деятельности Словакии. Цель – определить, какие связи обеспечивают исполнение защитных требований. Формально-юридический и системный методы используются для сопоставления норм, полномочий и результатов их применения.

Материалы и методы исследования

М. Рампашек разграничивает защиту информации, безопасность сетей и систем и киберустойчивость, связанную с сохранением функций и восстановлением деятельности [1, с. 32–36]. Для правового анализа это позволяет различать три результата: защиту человека, достоверность государственного ресурса и непрерывность услуги. Предлагаемый подход состоит в проверке переходов между правовым основанием, решением компетентного субъекта и подтверждённым результатом. Это авторская организация анализа, а не новая законодательная классификация.

Результаты и обсуждение

Конституция Словацкой Республики от 1 сентября 1992 г. № 460/1992 Zb. (Собрание законов Словацкой Республики. 1992. № 460; редакция с 01.11.2025; URL: https://static.slov-lex.sk/pdf/SK/ZZ/1992/460/ZZ_1992_460_20251101.pdf; дата обращения: 29.09.2026) устанавливает взаимосвязанные гарантии: ст. 19 защищает частную жизнь и данные о личности, ст. 22 – тайну сообщений, ст. 26 – выражение мнения, получение и распространение информации. Статья 13 определяет условия ограничения прав, ст. 46 – судебную защиту. Поэтому ссылка на безопасность требует проверки законного основания, допустимой цели и соразмерности конкретного вмешательства.

Т. Лялик обоснованно связывает действенность теста пропорциональности с определённостью цели ограничения: чрезмерно абстрактная цель облегчает оправдание вмешательства [2, с. 100–102]. Практическое значение этого положения видно в постановлении Конституционного суда Словакии от 5 ноября 2025 г. по делу PL. ÚS 6/2025. Суд признал неконституционными оспоренные нормы о плате за особо объёмный поиск информации: разгрузка административного аппарата в сформулированном законодателем виде не соответствовала целям ограничения по п. 4 ст. 26 Конституции (пп. 48, 52–54; с. 12–13 PDF; URL: https://www.ustavnysud.sk/docDownload/f27a3229-367f-4fef-9848-b567ba454e3c; дата обращения: 29.09.2026). Удобство органа, следовательно, не создаёт самостоятельного основания ограничить доступ.

Европейские гарантии применяются с учётом собственной сферы действия. Пункт 1 ст. 51 Хартии основных прав Европейского союза (2016/C 202/02; Официальный журнал Европейского союза. 2016. C 202. С. 389–405; URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT; дата обращения: 29.09.2026) связывает её обязательность для государств-членов с осуществлением права ЕС. Поэтому сначала устанавливается связь спорной обработки с правом Союза и лишь затем применяются ст. 7 о частной жизни и ст. 8 о персональных данных. Само нахождение системы в Словакии такой проверки не заменяет.

Закон Словацкой Республики от 30 января 2018 г. № 69/2018 Z. z. «О кибербезопасности и об изменении и дополнении некоторых законов» (Собрание законов Словацкой Республики. 2018. № 69; редакция с 30.04.2026; URL: https://static.slov-lex.sk/pdf/SK/ZZ/2018/69/ZZ_2018_69_20260430.pdf; дата обращения: 29.09.2026) распределяет управление кибербезопасностью. По § 5 Национальное управление безопасности (NBÚ) осуществляет координацию и надзор. Параграф 6 закрепляет функции национальной команды реагирования; его п. 4 сохраняет собственную ответственность оператора основной услуги и соответствующего центрального органа.

Получение технической помощи не прекращает обязанность организации устранить нарушение.

Иное направление регулирует Закон Словацкой Республики от 27 марта 2019 г. № 95/2019 Z. z. «Об информационных технологиях публичной администрации и об изменении и дополнении некоторых законов» (Собрание законов Словацкой Республики. 2019. № 95; редакция с 30.04.2026; URL: https://static.slov-lex.sk/pdf/SK/ZZ/2019/95/ZZ_2019_95_20260430.pdf; дата обращения: 29.09.2026). Его § 5 различает общее руководство Министерства инвестиций, регионального развития и информатизации и управление технологиями конкретных органов. По п. 6 § 2 назначение лица, эксплуатирующего технологию, не снимает ответственности с её администратора.

Независимый надзор за персональными данными осуществляет Управление по защите персональных данных Словацкой Республики (ÚOOÚ). Его независимость и полномочия предусмотрены ст. 51–52, 57–58 Регламента Европейского парламента и Совета (ЕС) 2016/679 от 27 апреля 2016 г. «О защите физических лиц при обработке персональных данных и о свободном движении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент по защите данных)» (Официальный журнал Европейского союза. 2016. L 119. С. 1–88; URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679; дата обращения: 29.09.2026; далее – GDPR). Таким образом, восстановление сервера и надзорная оценка законности обработки представляют разные действия. Техническое заключение не заменяет решения компетентного органа.

Контроль должен охватывать последующее исправление. Параграф 29m Закона № 69/2018 допускает соглашение об исправлении, предусматривающее конкретное нарушение, меры, график устранения и предупреждение повторения. Возможность его заключения ограничена законными условиями; при неисполнении обязательств надзор может возобновляться. Значение этой конструкции – в юридически определённой связи обнаруженного недостатка с восстановлением законности, а не в свободном отказе от обязательных требований.

Персональные данные, государственные ресурсы и критические системы не образуют взаимоисключающих категорий. База заявлений граждан требует защиты людей; государственный реестр – также достоверности записей; система водоснабжения – непрерывности услуги. Статьи 5–6 GDPR требуют законной цели и основания обработки, ст. 32 – мер безопасности с учётом риска. Шифрование не оправдывает избыточный сбор, а наличие законного основания не освобождает от проверки восстановления данных.

Различие имеет непосредственное практическое выражение. В отчёте ÚOOÚ за 2025 г. описаны нарушения при опубликовании договоров в Центральном реестре: персональные данные не удалялись либо скрывались так, что копирование текста PDF в редактор вновь делало их доступными. В зависимости от обстоятельств устанавливались нарушения принципа законности или ст. 32 GDPR [3, с. 39]. Следовательно, правомерное опубликование требует проверки фактически распространяемого файла. Визуальное закрытие текста не доказывает удаления защищаемых сведений.

Для инфраструктуры существенны специальные условия охвата. Параграф 17 Закона № 69/2018 связывает обязанности с видом субъекта, деятельностью и предусмотренными критериями. Отдельный статус устанавливает Закон Словацкой Республики от 27 ноября 2024 г. № 367/2024 Z. z. «О критической инфраструктуре и об изменении и дополнении некоторых законов» (Собрание законов Словацкой Республики. 2024. № 367; редакция с 01.01.2025; URL: https://static.slov-lex.sk/pdf/SK/ZZ/2024/367/ZZ_2024_367_20250101.pdf; дата обращения: 29.09.2026). Его § 9 регулирует идентификацию критического субъекта, §§ 10–11 – защитные меры и оценку рисков; применяются секторные исключения п. 3 § 19. Поэтому требования к критической инфраструктуре нельзя автоматически адресовать любой компании с клиентской базой.

При происшествии обязанности квалифицируются раздельно. По ст. 33 GDPR контролёр сообщает о нарушении защиты данных надзорному органу без неоправданной задержки и, по возможности, в пределах 72 часов после осведомлённости, кроме случая маловероятного риска для прав и свобод. Статья 34 предусматривает отдельное информирование человека при высоком риске и с установленными исключениями. Параграф 24 Закона № 69/2018 для серьёзного киберинцидента предусматривает раннее предупреждение до 24 часов, уведомление, как правило, до 72 часов и итоговый отчёт; специальные правила зависят от субъекта и развития события. Отправка одного сообщения не подтверждает исполнения всех обязанностей.

Для предпринимателя отправной точкой служит описание реальных операций и роли в обработке. Компания может определять цели собственной кадровой базы и одновременно обрабатывать клиентские сведения по поручению заказчика. Во втором случае применяются требования ст. 28 GDPR, но договор не заменяет фактического ограничения доступа и возврата либо удаления данных. Проверку следует завершать определением конкретного действия, ответственного лица и доказательства исполнения. Сбор документов без проверки действующих процессов не подтверждает исполнения обязанности по существу.

Предупредительное действие рассматриваемого механизма начинается до ввода информационной системы в эксплуатацию. Статья 25 GDPR требует учитывать защиту данных при определении средств обработки и при самой обработке, а по умолчанию ограничивать её необходимыми для конкретной цели сведениями. Для публичной администрации это означает, что правовая оценка должна влиять на устройство электронного сервиса: состав обязательных полей, круг пользователей, сроки хранения и порядок выгрузки. Если соответствующие ограничения не включены в проект, последующая инструкция сотрудникам может оказаться неисполнимой без изменения программного обеспечения.

Более углублённая предварительная проверка предусмотрена ст. 35 GDPR для обработки, которая, вероятно, создаёт высокий риск для прав и свобод физических лиц. Оценка воздействия включает описание операций, проверку их необходимости и соразмерности, анализ рисков и мер их снижения. Поэтому её нельзя отождествлять с проверкой устойчивости оборудования. Например, объединение сведений из нескольких реестров может повысить точность административного решения, одновременно позволяя сформировать избыточно подробное представление о частной жизни. При сохранении высокого риска, который контролёр не может снизить надлежащими мерами, применяется предварительная консультация с надзорным органом по ст. 36 GDPR. Сам статус государственной системы не означает, что такая консультация обязательна в каждом случае.

В предлагаемой модели предметом проверки становится весь путь сведений от получения до прекращения обработки. Для каждой операции следует установить цель, правовое основание, получателя и условие завершения. Особенно важно различать доступ сотрудника для исполнения должностной задачи и последующее использование тех же данных для иной цели. Техническая возможность просмотреть запись сама по себе не подтверждает правомерность обращения к ней. Поэтому распределение доступа целесообразно связывать с конкретными функциями, а при переводе или увольнении работника проверять прекращение соответствующих полномочий в системе.

Подтверждение исполнения опирается на принцип подотчётности, закреплённый в п. 2 ст. 5 и конкретизированный ст. 24 GDPR. Контролёр должен быть способен показать, как принятые меры обеспечивают соблюдение требований в реальных условиях. Для этого в зависимости от характера обработки могут использоваться результаты контрольных проверок доступа, сведения о пересмотре сроков хранения и протоколы восстановления данных. Это предлагаемые способы доказывания, а не установленный регламентом универсальный комплект документов. Их ценность определяется возможностью связать конкретный риск с применённой мерой и проверенным результатом.

Практическую связь законности и достоверности можно раскрыть на условном примере муниципального реестра. Если при переносе сведений ошибочная запись начинает использоваться для рассмотрения заявления гражданина, одного восстановления доступности сервиса недостаточно. Необходимо установить источник ошибки, проверить затронутые записи и исключить дальнейшее использование недостоверных сведений. Право на исправление по ст. 16 GDPR и право на ограничение обработки при оспаривании точности на период её проверки по подп. «а» п. 1 ст. 18 связывают состояние ресурса с возможностью человека защитить свои интересы.

При этом исправление записи и пересмотр принятого на её основе административного решения относятся к разным процедурам.

Реализация прав зависит и от доступности обращения к контролёру. Пункты 3–4 ст. 12 GDPR предусматривают предоставление информации о действиях по запросу без неоправданной задержки, в пределах одного месяца; при необходимости, с учётом сложности и числа запросов, срок может продлеваться ещё на два месяца с уведомлением о причинах в течение первого месяца. Если меры не принимаются, человеку сообщаются причины и возможности обращения за защитой. Для оценки механизма поэтому важно исследовать не только наличие формы запроса на сайте, но и прохождение обращения между подразделениями, полноту ответа и фактическое исполнение удовлетворённого требования.

Пределы отдельных прав также должны объясняться применительно к конкретной обработке. Право на удаление не устраняет необходимость хранения сведений для исполнения законной обязанности либо публичной задачи в случаях, предусмотренных п. 3 ст. 17 GDPR. Однако общая ссылка на государственный характер деятельности не обосновывает бессрочное сохранение любой информации. Контролёру необходимо определить, какие данные и для какой задачи продолжают требоваться. Если спор касается точности сведений, правовой результат может состоять в их исправлении или ограничении использования, а не в полном уничтожении записи.

Надзорная и судебная защита дополняют внутреннее рассмотрение обращений. Статья 77 GDPR закрепляет право жалобы надзорному органу, ст. 78 – право на судебную защиту в отношении его обязательного решения, а также предусмотренного регламентом бездействия; ст. 79 относится к защите против контролёра или обработчика. Эти процедуры различаются по адресату и предмету проверки. Обращение гражданина становится самостоятельным источником выявления недостатков, которые могли остаться вне технического аудита.

Национальный порядок конкретизирует Закон Словацкой Республики от 29 ноября 2017 г. № 18/2018 Z. z. «О защите персональных данных и об изменении и дополнении некоторых законов» (Собрание законов Словацкой Республики. 2018. № 18; редакция с 18.08.2026; URL: https://static.slov-lex.sk/pdf/SK/ZZ/2018/18/ZZ_2018_18_20260818.pdf; дата обращения: 30.10.2026). По п. 3 § 100 заявление в ÚOOÚ должно содержать указание на предположительно нарушенные права и доказательства в поддержку изложенных доводов. Подпункт «e» того же пункта предусматривает подтверждение осуществления соответствующего права либо объяснение особых причин его неосуществления. Пункт 5 § 102 обязывает контролёра или обработчика письменно сообщить об исполнении назначенных мер в установленный органом срок. Тем самым связь между решением и последующим исправлением получает прямое процедурное выражение.

Выбор надзорной меры следует связывать с характером установленного нарушения. Пункт 2 ст. 58 GDPR предусматривает, в частности, предписание привести обработку в соответствие с регламентом, исправить или удалить данные, ограничить обработку; денежное взыскание не исчерпывает полномочий органа. В аналитическом отношении полезно различать прекращение противоправной операции и устранение условий её повторения. Так, в предлагаемой модели прекращение избыточного доступа следует сопровождать проверкой порядка выдачи полномочий, иначе исправление единичной учётной записи не обеспечивает устойчивого результата. Конкретный объём предписания при этом должен оставаться в пределах компетенции органа и учитывать обстоятельства дела.

Для оценки последующего исполнения предлагается учитывать долю проверенных мер, время устранения опасного состояния и повторяемость нарушений. Это авторские показатели, а не установленная словацким законом система отчётности. Они позволяют проверить фактические изменения после властного решения. Если после обновления регламента сохраняется возможность неправомерной выгрузки данных, документальное исполнение не подтверждает достижения защитной цели. Проверяемое изменение процесса завершает связь между обязанностью и результатом.

Заключение

Публично-правовой механизм защиты информации в Словакии объединяет конституционные ограничения, распределённую компетенцию и обязанности по обеспечению безопасности. Предлагается оценивать его полноту по трём связям: законное основание – допустимая операция; компетентный субъект – исполнимая обязанность; обнаруженное нарушение – подтверждённое исправление. Самостоятельность каждого элемента исключает подмену законности технической защищённостью, ответственности – привлечением подрядчика, а результата надзора – числом выданных предписаний. Такой подход применим при мотивировании решений органов и организации защиты в компаниях. Для сравнительного исследования перспективно оценивать именно способы подтверждения исполнения, не предполагая заранее необходимости заимствования всей словацкой модели.

Литература

1. Andraško J., Dražová P., Kordík M., Mesarčík M., Rampášek M. a kol. Regulácia kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality [Регулирование кибербезопасности, защиты частной жизни и киберпреступности]. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2026. Гл. 1 (автор – М. Рампашек). С. 32–36. URL: https://cusec.flaw.uniba.sk/wp-content/uploads/2026/06/Regulacia-kybernetickej-bezpecnosti-ochrany-sukromia-a-kybernetickej-kriminality_CUSEC_2026.pdf (дата обращения: 29.09.2026).

2. Ľalík T. Test legitímneho účelu v judikatúre Ústavného súdu SR [Проверка легитимной цели в практике Конституционного суда Словацкой Республики] // 30 rokov Ústavy Slovenskej republiky: skúsenosti a perspektívy v dobrom aj v zlom počasí [30 лет Конституции Словацкой Республики: опыт и перспективы в благоприятных и неблагоприятных условиях]. Bratislava: Univerzita Komenského, 2022. С. 100–102. URL: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF/2022/Zbornik_BPF_2021_Sekcia_5_Ustavne_pravo.pdf (дата обращения: 29.09.2026).

3. ÚOOÚ SR. Správa o stave ochrany osobných údajov za rok 2025 [Отчёт о состоянии защиты персональных данных за 2025 год]. Разд. 9.2.3. С. 39 (с. 41 PDF). URL: https://dataprotection.gov.sk/files/annual-reports/uoou_sprava-stave-ochrany-osobnych-udajov_2025.pdf (дата обращения: 29.09.2026).

Public-law mechanism for information protection in the Slovak Republic

Korobov I.A.

Kutafin Moscow State Law University (MSAL)

The article examines the public-law mechanism for information protection in the Slovak Republic. It addresses the gap between constitutional limits on processing, the allocation of institutional powers and actual compliance with protective duties. The study focuses on information protection in public administration and regulated business activities, using formal legal and systemic methods. Its contribution is a set of criteria connecting a legal basis, a decision by a competent actor and a demonstrable outcome. Constitutional case law and supervisory practice show that technical security cannot legitimise unlawful processing and that outsourcing does not extinguish an organisation's own duties. Personal data protection, the reliability of public information resources and infrastructure resilience are distinguished. The provisions of the Constitution of the Slovak Republic, the laws on cybersecurity, on information technologies in public administration and on critical infrastructure, as well as the General Data Protection Regulation are examined. The need for separate qualification of duties in an incident is substantiated: notifying the supervisory authority of a personal data breach and reporting a serious cyber incident do not replace each other. It is shown that the completeness of the mechanism is determined not by the number of orders issued but by the confirmed remedying of the violations detected. The proposed approach can support reasoned administrative decisions, supervision and the identification of corporate obligations.

Keywords: information security, Slovak Republic, constitutional guarantees, public administration, personal data, cybersecurity, supervision, critical infrastructure.

References

1. Andraško J., Dražová P., Kordík M., Mesarčík M., Rampášek M. et al. Regulation of cybersecurity, privacy protection and cybercrime. Bratislava: Comenius University in Bratislava, Faculty of Law, 2026. Chapter 1 (author: M. Rampášek). Pp. 32–36. (In Slovak). URL: https://cusec.flaw.uniba.sk/wp-content/uploads/2026/06/Regulacia-kybernetickej-bezpecnosti-ochrany-sukromia-a-kybernetickej-kriminality_CUSEC_2026.pdf (accessed: 29.09.2026).

2. Ľalík T. Legitimate aim test in the case-law of the Constitutional Court of the Slovak Republic // 30 years of the Constitution of the Slovak Republic: experience and prospects in good and bad times. Bratislava: Comenius University, 2022. Pp. 100–102. (In Slovak). URL: https://www.flaw.uniba.sk/fileadmin/praf/Veda/Konferencie_a_podujatia/BPF/2022/Zbornik_BPF_2021_Sekcia_5_Ustavne_pravo.pdf (accessed: 29.09.2026).

3. Office for Personal Data Protection of the Slovak Republic. Report on the state of personal data protection for 2025. Section 9.2.3. P. 39 (PDF p. 41). (In Slovak). URL: https://dataprotection.gov.sk/files/annual-reports/uoou_sprava-stave-ochrany-osobnych-udajov_2025.pdf (accessed: 29.09.2026).