
ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ/PUBLIC LAW (STATE LAW) SCIENCES

DOI: <https://doi.org/10.60797/IRJ.2026.171.73> EDN: OBAWID**ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ГОСУДАРСТВЕННОЙ ТАЙНЫ В ЗАРУБЕЖНЫХ СТРАНАХ В УСЛОВИЯХ ИНФОРМАТИЗАЦИИ ОБЩЕСТВА**

Научная статья

Нафигин И.А.^{1,*}, Ревина С.Н.²¹ ORCID : 0009-0005-3739-9152;² ORCID : 0000-0001-9565-1356;^{1,2} Самарский государственный экономический университет, Самара, Российская Федерация

* Корреспондирующий автор (nafigin.ilya[at]yandex.ru)

Предложена: 01.05.2026; Принята: 19.08.2026; Опубликовано: 17.09.2026

Аннотация

Статья посвящена анализу особенностей правового регулирования административно-правового режима государственной тайны в зарубежных странах с различными системами права в условиях информатизации общества. Использование цифровых технологий для незаконного получения государственной тайны является всемирной проблемой. Совершенствование законодательства в сфере регламентации режима государственной тайны должно быть направлено на предупреждение и устранение возможных угроз, возникающих в связи с развитием технологий. Таким образом, адаптация зарубежного опыта правового регулирования рассматриваемой сферы отношений имеет достаточно весомую роль. Цель: проанализировать основные нормативные правовые акты зарубежных государств, регулирующие отношения в сфере защиты информации, составляющей государственную тайну, раскрыть их основные преимущества и недостатки. Результаты: проведенный анализ показал, что в действующем законодательстве зарубежных стран закреплена возможность использования искусственного интеллекта для выявления утечек государственной тайны и обязанность для сотрудников, приступающих к работе с такой информацией, проходить специальный обучающий курс, направленный на обеспечение защиты государственной тайны при работе с информационными технологиями.

Ключевые слова: нормативные правовые акты, государственная тайна, информационная безопасность, угроза безопасности, кибербезопасность, защита государственной тайны, законодательство зарубежных стран, искусственный интеллект.

SPECIFICS OF THE LEGAL REGULATION OF STATE SECRETS IN OTHER COUNTRIES IN THE CONTEXT OF THE DIGITALISATION OF SOCIETY

Research article

Nafigin I.A.^{1,*}, Revina S.N.²¹ ORCID : 0009-0005-3739-9152;² ORCID : 0000-0001-9565-1356;^{1,2} Samara State University of Economics, Samara, Russian Federation

* Corresponding author (nafigin.ilya[at]yandex.ru)

Suggested: 01.05.2026; Accepted: 19.08.2026; Published: 17.09.2026

Abstract

The article analyses the specifics of the legal regulation of the administrative and legal regime governing state secrets in foreign countries with different legal systems, in the context of the digitalisation of society. The use of digital technologies to illegally obtain state secrets is a global problem. Improvements to legislation governing the regime of state secrets must be aimed at preventing and eliminating potential threats arising from technological developments. Consequently, adapting foreign experience of legal regulation in this area plays a significant role. Objective: to analyse the main legislative acts of foreign states governing relations in the field of protecting information constituting state secrets, and to identify their main advantages and disadvantages. Results: The analysis carried out has shown that the current legislation of foreign countries enshrines the possibility of using artificial intelligence to detect leaks of state secrets and the obligation for staff commencing work with such information to undertake a specialised training course aimed at ensuring the protection of state secrets when working with information technology.

Keywords: regulatory legal acts, state secrets, information security, security threats, cybersecurity, protection of state secrets, legislation of foreign countries, artificial intelligence.

Введение

Современные государства в связи с трансграничным характером процесса информатизации общества в большей или меньшей степени трансформировались в технологически сложные информационные общества [2, С. 182]. Последствием указанного процесса является наличие угрозы получения несанкционированного доступа к секретной информации и ее дальнейшее распространение и, следовательно, создание угрозы государственной (национальной)

безопасности. Правительства различных стран вне зависимости от правовой системы, политического режима или социально-экономических условий ставят для себя ориентир на развитие «государства национальной безопасности», в том числе посредством развития мер по защите государственной тайны.

В зависимости от принадлежности к той или иной правовой системе законодательство, регулирующее отношения по защите государственной тайны и обеспечению информационной безопасности, будет иметь свои особенности в форме и содержании нормативных правовых актов. В этой связи, в целях определения направлений совершенствования действующего российского законодательства, регулирующего отношения по защите государственной тайны, необходимо проанализировать законодательство представителей различных правовых семей, поскольку эффективность их правового регулирования может различаться как в форме закрепления правовых норм, так и в их самом содержании [22, С. 101].

В основе методологии исследования лежат общенаучные методы, сравнительно-правовой анализ и формально-юридический подход. В ходе проведенного исследования были изучены законодательство зарубежных государств и научные труды экспертов в области права.

Основные результаты

Анализ законодательства представителей англосаксонской правовой семьи позволил выделить ряд положений их действующего, которые направлены на регулирование защиты государственной тайны в условиях информационного общества и повсеместной цифровизации. Так, на территории Великобритании решения субъекта административно-правового режима государственной тайны может быть обжалованы гражданами в случае засекречивания информации, которая в соответствии с законом не может быть засекречена. В Великобритании для указанной цели существует должность Информационного уполномоченного (Information commissioner). С одной стороны, его решения являются обязательным к исполнению. Однако они могут быть обжалованы в Трибунале по информации (Information tribunal) или в суде [16]. Наличие отдельного органа, регулирующего отношения по засекречиванию должно упростить процедуру обжалования решений должностных лиц посредством использования досудебного порядка. В то же время, поскольку окончательное решение по указанному вопросу стоит за судом, возникает вопрос о целесообразности его наличия в системе органов по защите государственной тайны.

Федеральные органы власти США, по аналогии с российским законодательством, обязаны соблюдать требования по обеспечению кибербезопасности, в том числе посредством прохождения специальной процедуры сертификации информационных систем [15]. Отдельный интерес вызывают следующие положения законодательства США. Во-первых, уголовная ответственность за несанкционированное разглашение секретной информации установлена в отношении определенных типов информации [27]. Таким образом, законодательство США допускает отсутствие ответственности за разглашение государственной тайны — например, ее опубликование в средствах массовой информации в результате возникшей утечки таких сведений. Во-вторых, на территории США установлены требования по обнаружению и предотвращению угроз со стороны инсайдеров с целью противодействия утечке информации и создания угрозы национальной безопасности [14].

Особенностью законодательства стран-участниц Европейского Союза (далее — ЕС) является определяющая роль законодательства ЕС по отношению к национальному законодательству. Так, например, действие Директивы (ЕС) 2024/1418 направлено на правовое регулирование оборота конфиденциальной и секретной информации на территории ЕС, а также на обеспечение защиты такой информации от угроз, возникающих в информационном пространстве [13]. Страны-участницы ЕС обязаны имплементировать указанные нормы в свое национальное законодательство наравне с особенностями собственного правового регулирования.

На уровне национального законодательства стран-участниц ЕС в целях обеспечения информационной безопасности государственной тайны применяются следующие меры: в определение государственной тайны включаются компьютерные сети, компьютеризированные данные или файлы, имеющие отношение к национальной обороне (например, Франция [12], Испания [19], Нидерланды [28]); на государственном уровне принимаются нормативные правовые акты, направленные на обеспечение цифрового государственного суверенитета и противодействие киберугрозам, в том числе в части обеспечения безопасности сетей и информационных систем (Франция [10, С. 24], Германия [17], Испания [25]); закрепление обязанности получать соответствующий допуск у уполномоченного органа в сфере кибербезопасности (Дания [24]).

Отдельно стоит выделить возможность применения на территории Нидерландов искусственного интеллекта для автоматического обнаружения атаки по аномалиям в работе информационной сети [18]. С одной стороны, использование искусственного интеллекта в качестве инструмента поиска и устранения угроз безопасности имеет место быть в системе защиты государственной тайны. Однако в научном сообществе отмечается, что сотрудничество с технологическими гигантами при разработке государственных ИИ-моделей может повысить их эффективность, но в то же время увеличивает риск утечки данных в связи наличием системной уязвимости у организаций-подрядчиков [20, С. 7]. В условиях, когда утечка секретной информации может оказать особенно чувствительное влияние на безопасность государства, необходимо достаточно конкретно формулировать правовые нормы, регламентирующие разработку и дальнейшее использование ИИ-моделей.

Внимания заслуживает и Турецкая Республика. Несмотря на то, что она является кандидатом на вступление в ЕС, ее законодательство основано на романо-германской правовой семье. Отличительной особенностью понимания государственной тайны в Турции является учет ущерба международным отношениям государства как одного из признаков государственной тайны [11]. На территорию Турции также действуют Стратегия национальной безопасности и Национальная стратегия кибербезопасности, которые направлены на усиление национальной безопасности в информационной сфере, в том числе в сфере государственного управления [1, С. 584].

Особый интерес представляют законодательные акты стран юго-восточной Азии, поскольку в них уровень информатизации общества достиг достаточно высоких значений. В целях регулирования информации в информационном пространстве на территории Японии был принят Основной закон о кибербезопасности, в соответствии с которым при работе с информацией ограниченного доступа должна быть обеспечена кибербезопасность при одновременном обеспечении свободного потока информации [29]. Таким образом, законодательство направлено на соблюдение баланса между государственным и общественным интересами в рамках информационных отношений.

В южнокорейских законах о государственной тайне и о военной тайне отсутствуют положения, устанавливающие требования об обеспечении информационной безопасности при работе с информацией, составляющей государственную тайну [21], [23]. С одной стороны, данные нормы могут быть закреплены в подзаконных нормативных актах. Но в то же время закон, как акт, имеющий большую юридическую силу, должен предусматривать в себе правила, влияющие на безопасность государства.

В этом плане значительно отличается Китайский закон о государственной тайне, который устанавливает требования по борьбе с угрозами информационной безопасности при работе с секретной информацией. Так, например, данный закон обязывает соблюдать режим секретности при разработке и производстве оборудования и продукции. Данное положение является одним из важнейших механизмов по обеспечению информационной безопасности, поскольку оно направлено на предупреждение возможности установки в используемое оборудование устройств, способствующих утечке секретной информации. Кроме того, закреплены правила по обращению государственной тайны в специальных информационных системах и в общественных информационных сетях, а также обязанность сотрудников, допускаемых к работе с такой информацией, пройти курс обучения по соблюдению секретности. Таким образом, китайский законодатель принял меры по противодействию такому источнику угрозы информационной безопасности как человеческий фактор. В дополнение к указанным требованиям в законе установлена обязанность операторов и провайдеров услуг Интернета по оказанию содействия государственным органам в обеспечении режима секретности [8].

В связи с действием Модельного закона Содружества Независимых Государств «О государственных секретах», содержащего типовые нормы, направленные на защиту государственной тайны, законодательство стран постсоветского пространства в сфере регулирования правового режима государственной тайны, например Армении, Белоруссии, Казахстана и Кыргызстана, содержит в себе нормы аналогичные российскому закону о государственной тайне, в частности о сертифицировании средств защиты информационных систем, используемых для работы с такой информацией, установлении требований к условиям хранения и средствам передачи государственной тайны [5], [6], [7], [9]. Законодательство ряда стран содержит в себе значительные отличия. Например, в Законе Грузии в определение государственной тайны также входит информация, переданная в рамках международных отношений, установлен более краткий срок для пересмотра — 1 год, что особенно важно в условиях быстро меняющегося мира. Кроме того, установлены требования для опубликования такой информации [4]. Закон Эстонии включает в себя положения, регулирующие использование государственной тайны иностранных государств [26].

На основании вышеизложенного, можно сделать следующие выводы. Законодатели зарубежных стран вне зависимости от особенностей правовой традиции в условиях глобализации и непрерывного развития технологий стремятся развивать свое правовое регулирование системы обеспечения информационной безопасности в сфере защиты государственной тайны. Совершенствование правовой базы осуществляется в различных формах: вносятся изменения в закон, регулирующий отношения по защите государственной тайны либо принимаются отдельные правовые акты, которые направлены на обеспечение национальной (в том числе информационной) безопасности государства, а защита государственной тайны является одним из ее составляющих элементов.

Заключение

Проведенный анализ показал, что в действующем законодательстве зарубежных стран закреплена возможность использования различных организационных, программных и программно-технических средств защиты, чье применение направлено на противодействие угрозам государственной тайне, возникающим в том числе в информационном пространстве. В этой связи предлагается учесть опыт зарубежных государств и дополнить статью 21 Закона Российской Федерации «О государственной тайне» нормой об обязательном прохождении сотрудниками, в отношении которых осуществляется процедура оформления допуска к такой информации, специального обучающего курса, направленного на обеспечение защиты государственной тайны при работе с информационными технологиями. Кроме того, предлагается рассмотреть вопрос о принятии ведомственного акта Федеральной службы безопасности Российской Федерации, которым бы предусматривалась возможность использования искусственного интеллекта для выявления утечек государственной тайны. Внедрение указанных положений в действующее российское законодательство позволит усилить систему защиты государственной тайны, поскольку они предусматривают противодействие угрозам, возникающим как внутри организации—обладателя информации, составляющей государственную тайну, так и извне, в связи с несовершенством используемого технологического оборудования (информационных систем) или ввиду человеческого фактора.

Конфликт интересов

Не указан.

Рецензия

Вербицкая Т.В., Государственный архив Свердловской области, Екатеринбург Российская Федерация
DOI: <https://doi.org/10.60797/IRJ.2026.171.73.1>

Conflict of Interest

None declared.

Review

Verbitskaia T.V., Ural State Archives, Ekaterinburg Russian Federation
DOI: <https://doi.org/10.60797/IRJ.2026.171.73.1>

Список литературы / References

1. Аватков В.А. Подходы Турецкой Республики к обеспечению цифровой безопасности и регуляции СМИ / В.А. Аватков, Л.Д. Мишин // Вестник Российского университета дружбы народов. Серия: Политология. — 2025. — Т. 27, № 3. — С. 579–589.
2. Ильина Н.Е. Влияние информационно-культурных процессов на безопасность Российской Федерации в условиях приграничья / Н.Е. Ильина // Приграничный регион в историческом развитии: партнёрство и сотрудничество : Материалы Международной научно-практической конференции, посвященной 100-летию Революции 1917 года, 80-летию со дня образования Читинской области, 50-летию атомной промышленности в Забайкалье. В 3-х частях, Чита, 22 сентября 2017 года / гл. ред. Е.В. Дроботушенко. — Чита: Забайкальский государственный университет, 2017. — Ч. 1. — С. 179–182.
3. Корсун Р.В. Анализ систем отнесения сведений к государственной тайне в России и в США / Р.В. Корсун // Законы России: опыт, анализ, практика. — 2007. — № 1. — С. 125–128.
4. О государственной тайне : Закон Грузии от 19 февраля 2015 г. № 3099-III // Законодательный вестник Грузии. — URL: <https://matsne.gov.ge/ru/document/view/2750311?publication=8> (дата обращения: 06.04.2026).
5. О государственной тайне : Закон Республики Армения от 01 марта 2023 г. № ЗР-49 // СоюзПравоИнформ. — URL: https://base.spinform.ru/show_doc.fwx?rgn=149957 (дата обращения: 06.04.2026).
6. О государственных секретах : Закон Республики Беларусь от 19 июля 2010 г. № 170-З // Национальный правовой Интернет-портал Республики Беларусь. — URL: <https://pravo.by/document/?guid=3961&p0=H11000170> (дата обращения: 06.04.2026).
7. О государственных секретах : Закон Республики Казахстан от 15 марта 1999 г. № 349-1 // Информационно-правовая система нормативных правовых актов Республики Казахстан. — URL: https://adilet.zan.kz/rus/docs/Z990000349_ (дата обращения: 06.04.2026).
8. О защите государственной тайны : Закон Китайской Народной Республики от 05 сентября 1988 г. // Бизнес в Китае. Информационно-аналитический портал. — URL: <https://asia-business.ru/law/law3/secret/> (дата обращения: 29.03.2026).
9. О защите государственных секретов Кыргызской Республики : Закон Кыргызской Республики от 15 декабря 2017 г. № 210 (15) // Веб-версия Централизованного Банка Данных Правовой Информации Кыргызской Республики. — URL: <https://cbd.minjust.gov.kg/111719/edition/1229912/ru> (дата обращения: 06.04.2026).
10. Сеитмедиева И.Р. Обеспечение кибербезопасности во Французской республике. Национальный и международный правовые аспекты / И.Р. Сеитмедиева // Океанский менеджмент. — 2023. — № 1 (19). — С. 22–25.
11. Bilgi edinme hakkı kanunu, № 4982 of October 24, 2003 // T.C. Adalet Bakanlığı Bilgi İşlem Genel Müdürlüğü. — URL: <https://mevzuat.adalet.gov.tr/mevzuat/117055?query=devlet%20s%C4%B1r%C4%B1> (erişim tarihi: 04.04.2026).
12. Code pénal français, 1992 // WIPO Lex. — URL: <https://www.wipo.int/wipolex/ru/legislation/details/23309> (consulté le: 04.04.2026).
13. Delegated Decision No 19/2024 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information, 2024/1418 of May 24, 2024 // EUR-Lex. — URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024Q01418&qid=1775482046038> (accessed: 04.04.2026).
14. Executive Order 13587 of October 7, 2011 «Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information» // Wikisource. — URL: https://en.wikisource.org/wiki/Executive_Order_13587 (accessed: 01.04.2026).
15. Federal Information Security Management Act of 2002 // U.S. Government Publishing Office. — URL: <https://www.govinfo.gov/content/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf> (accessed: 27.03.2026).
16. Freedom of Information Act, 2000 // Legislation.gov.uk. — URL: <https://www.legislation.gov.uk/ukpga/2000/36/contents> (accessed: 27.03.2026).
17. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, 2025 // Bundesgesetzblatt. — URL: <https://www.recht.bund.de/bgbl/1/2025/301/VO> (Abrufdatum: 04.04.2026).
18. Government-wide vision on generative AI of the Netherlands, 2024 // Government of the Netherlands. — URL: <https://www.government.nl/documents/parliamentary-documents/2024/01/17/government-wide-vision-on-generative-ai-of-the-netherlands> (accessed: 05.04.2026).
19. Ley 9/1968, de 5 de abril, sobre secretos oficiales // Agencia Estatal Boletín Oficial del Estado. — URL: <https://www.boe.es/buscar/doc.php?id=BOE-A-1968-444> (fecha de consulta: 04.04.2026).
20. Li C. AI-Driven Governance: Enhancing Transparency and Accountability in Public Administration / C. Li // Digital Society & Virtual Governance. — 2025. — Vol. 1, Issue 1. — P. 1–16. — DOI: 10.6914/dsvg.010101.
21. Military secret protection act, No. 19076, Dec. 13, 2022 // Korea Legislation Research Institute. — URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=61739&lang=ENG (accessed: 03.04.2026).
22. Muqem Islam M. Comparative Analysis of Various Judicial Systems across the World and Their Effectiveness / M. Muqem Islam // Khyber Journal of Public Policy. — 2022. — Vol. 1, Issue 1. — P. 97–113.
23. National security act, No. 13722, Jan. 6, 2016 // Korea Legislation Research Institute. — URL: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=39798&lang=ENG (accessed: 03.04.2026).
24. Net-og informationssikkerhedsloven, 2015 // Danske Love. — URL: <https://danskelove.dk/net-og-informationssikkerhedsloven> (besøgt: 05.04.2026).



25. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información // Agencia Estatal Boletín Oficial del Estado. — URL: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257> (fecha de consulta: 04.04.2026).
26. Riigisaladuse ja salastatud välisteabe seadus, 2007 // Riigi Teataja. — URL: <https://www.riigiteataja.ee/akt/12791615> (vaadatud: 07.04.2026).
27. U.S. Code: Table Of Contents // Legal Information Institute. — URL: <https://www.law.cornell.edu/uscode/text/18> (accessed: 31.03.2026).
28. Wetboek van Strafrecht, 1881 // Wetboek-online. — URL: <http://www.wetboek-online.nl/wet/Sr.html#1010> (geraadpleegd op: 05.04.2026).
29. サイバーセキュリティ基本法, 2014 // e-Gov 法令検索. — URL: <https://laws.e-gov.go.jp/law/426AC1000000104/> (参照日: 03.04.2026).

Список литературы на английском языке / References in English

1. Avatkov V.A. Podkhody Turetskoy Respubliki k obespecheniyu tsifrovoy bezopasnosti i regulyatsii SMI [Approaches of the Republic of Turkey to ensuring digital security and media regulation] / V.A. Avatkov, L.D. Mishin // Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Politologiya [Bulletin of the Peoples' Friendship University of Russia. Series: Political Science]. — 2025. — Vol. 27, № 3. — P. 579–589. [in Russian]
2. Il'ina N.E. Vliyanie informatsionno-kul'turnykh protsessov na bezopasnost' Rossiyskoy Federatsii v usloviyakh prigranich'ya [The influence of information and cultural processes on the security of the Russian Federation in border areas] / N.E. Il'ina // Prigranichnyy region v istoricheskom razviti: partnyorstvo i sotrudnichestvo : Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii, posvyashchennoy 100-letiyu Revolyutsii 1917 goda, 80-letiyu so dnya obrazovaniya Chitinskoy oblasti, 50-letiyu atomnoy promyshlennosti v Zabaykal'e. V 3-kh chastyakh, Chita, 22 sentyabrya 2017 goda [Border region in historical development: partnership and cooperation : Proceedings of the International Scientific and Practical Conference dedicated to the 100th anniversary of the 1917 Revolution, the 80th anniversary of the formation of the Chita Region, the 50th anniversary of the nuclear industry in Transbaikalia. In 3 parts, Chita, September 22, 2017] / chief ed. E.V. Drobotushenko. — Chita: Trans-Baikal State University, 2017. — Part 1. — P. 179–182. [in Russian]
3. Korsun R.V. Analiz sistem otneseniya svedeniy k gosudarstvennoy tayne v Rossii i v SShA [Analysis of systems for classifying information as state secrets in Russia and the USA] / R.V. Korsun // Zakony Rossii: opyt, analiz, praktika [Laws of Russia: experience, analysis, practice]. — 2007. — № 1. — P. 125–128. [in Russian]
4. O gosudarstvennoy tayne : Zakon Gruzii ot 19 fevralya 2015 g. № 3099-IIႆ [On State Secrets : Law of Georgia of February 19, 2015 No. 3099-IIႆ] // Zakonodatel'nyy vestnik Gruzii [Legislative Bulletin of Georgia]. — URL: <https://matsne.gov.ge/ru/document/view/2750311?publication=8> (accessed: 06.04.2026). [in Russian]
5. O gosudarstvennoy tayne : Zakon Respubliki Armeniya ot 01 marta 2023 g. № ZR-49 [On State Secrets : Law of the Republic of Armenia of March 1, 2023 No. ZR-49] // SoyuzPravoInform. — URL: https://base.spinform.ru/show_doc.fwx?rgn=149957 (accessed: 06.04.2026). [in Russian]
6. O gosudarstvennykh sekretakh : Zakon Respubliki Belarus' ot 19 iyulya 2010 g. № 170-Z [On State Secrets : Law of the Republic of Belarus of July 19, 2010 No. 170-Z] // Natsional'nyy pravovoy Internet-portal Respubliki Belarus' [National Legal Internet Portal of the Republic of Belarus]. — URL: <https://pravo.by/document/?guid=3961&p0=H11000170> (accessed: 06.04.2026). [in Russian]
7. O gosudarstvennykh sekretakh : Zakon Respubliki Kazakhstan ot 15 marta 1999 g. № 349-1 [On State Secrets : Law of the Republic of Kazakhstan of March 15, 1999 No. 349-1] // Informatsionno-pravovaya sistema normativnykh pravovykh aktov Respubliki Kazakhstan [Information and Legal System of Regulatory Legal Acts of the Republic of Kazakhstan]. — URL: https://adilet.zan.kz/rus/docs/Z990000349_ (accessed: 06.04.2026). [in Russian]
8. O zashchite gosudarstvennoy tayny : Zakon Kitayskoy Narodnoy Respubliki ot 05 sentyabrya 1988 g. [On the Protection of State Secrets : Law of the People's Republic of China of September 5, 1988] // Biznes v Kitae. Informatsionno-analiticheskiy portal [Business in China. Information and Analytical Portal]. — URL: <https://asia-business.ru/law/law3/secret/> (accessed: 29.03.2026). [in Russian]
9. O zashchite gosudarstvennykh sekretov Kyrgyzskoy Respubliki : Zakon Kyrgyzskoy Respubliki ot 15 dekabrya 2017 g. № 210 (15) [On the Protection of State Secrets of the Kyrgyz Republic : Law of the Kyrgyz Republic of December 15, 2017 No. 210 (15)] // Veb-versiya Tsentralizovannogo Banka Dannyykh Pravovoy Informatsii Kyrgyzskoy Respubliki [Web version of the Centralized Bank of Legal Information Data of the Kyrgyz Republic]. — URL: <https://cbd.minjust.gov.kg/111719/edition/1229912/ru> (accessed: 06.04.2026). [in Russian]
10. Seitmedieva I.R. Obespechenie kiberbezopasnosti vo Frantsuzskoy respublike. Natsional'nyy i mezhdunarodnyy pravovye aspekty [Ensuring cybersecurity in the French Republic. National and international legal aspects] / I.R. Seitmedieva // Okeanskiy menedzhment [Ocean Management]. — 2023. — № 1 (19). — P. 22–25. [in Russian]
11. Bilgi edinme hakki kanunu, № 4982 of October 24, 2003 [Freedom of Information Law, No. 4982 of October 24, 2003] // T.C. Adalet Bakanlığı Bilgi İşlem Genel Müdürlüğü [Republic of Turkey Ministry of Justice, Information Technology General Directorate]. — URL: <https://mevzuat.adalet.gov.tr/mevzuat/117055?query=devlet%20s%C4%B1rr%C4%B1> (accessed: 04.04.2026). [in Turkish]
12. Code pénal français, 1992 [French Criminal Code, 1992] // WIPO Lex. — URL: <https://www.wipo.int/wipolex/ru/legislation/details/23309> (accessed: 04.04.2026). [in French]
13. Delegated Decision No 19/2024 on implementing rules for handling CONFIDENTIEL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET information, 2024/1418 of May 24, 2024 // EUR-Lex. — URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024Q01418&qid=1775482046038> (accessed: 04.04.2026).



14. Executive Order 13587 of October 7, 2011 «Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information» // Wikisource. — URL: https://en.wikisource.org/wiki/Executive_Order_13587 (accessed: 01.04.2026).
15. Federal Information Security Management Act of 2002 // U.S. Government Publishing Office. — URL: <https://www.govinfo.gov/content/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf> (accessed: 27.03.2026).
16. Freedom of Information Act, 2000 // Legislation.gov.uk. — URL: <https://www.legislation.gov.uk/ukpga/2000/36/contents> (accessed: 27.03.2026).
17. Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, 2025 [Act Implementing the NIS-2 Directive and Regulating Key Features of Information Security Management in the Federal Administration, 2025] // Bundesgesetzblatt [Federal Law Gazette]. — URL: <https://www.recht.bund.de/bgbl/1/2025/301/VO> (accessed: 04.04.2026). [in German]
18. Government-wide vision on generative AI of the Netherlands, 2024 // Government of the Netherlands. — URL: <https://www.government.nl/documents/parliamentary-documents/2024/01/17/government-wide-vision-on-generative-ai-of-the-netherlands> (accessed: 05.04.2026).
19. Ley 9/1968, de 5 de abril, sobre secretos oficiales [Law 9/1968, of April 5, on Official Secrets] // Agencia Estatal Boletín Oficial del Estado [State Agency Official State Gazette]. — URL: <https://www.boe.es/buscar/doc.php?id=BOE-A-1968-444> (accessed: 04.04.2026). [in Spanish]
20. Li C. AI-Driven Governance: Enhancing Transparency and Accountability in Public Administration / C. Li // Digital Society & Virtual Governance. — 2025. — Vol. 1, Issue 1. — P. 1–16. — DOI: 10.6914/dsvg.010101.
21. Military secret protection act, No. 19076, Dec. 13, 2022 // Korea Legislation Research Institute. — URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=61739&lang=ENG (accessed: 03.04.2026).
22. Muqem Islam M. Comparative Analysis of Various Judicial Systems across the World and Their Effectiveness / M. Muqem Islam // Khyber Journal of Public Policy. — 2022. — Vol. 1, Issue 1. — P. 97–113.
23. National security act, No. 13722, Jan. 6, 2016 // Korea Legislation Research Institute. — URL: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=39798&lang=ENG (accessed: 03.04.2026).
24. Net-og informationssikkerhedsloven, 2015 [Network and Information Security Act, 2015] // Danske Love [Danish Laws]. — URL: <https://danskelove.dk/net-og-informationssikkerhedsloven> (accessed: 05.04.2026). [in Danish]
25. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [Royal Decree-Law 12/2018, of September 7, on the Security of Networks and Information Systems] // Agencia Estatal Boletín Oficial del Estado [State Agency Official State Gazette]. — URL: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257> (accessed: 04.04.2026). [in Spanish]
26. Riigisaladuse ja salastatud välisteabe seadus, 2007 [State Secrets and Classified Foreign Information Act, 2007] // Riigi Teataja [State Gazette]. — URL: <https://www.riigiteataja.ee/akt/12791615> (accessed: 07.04.2026). [in Estonian]
27. U.S. Code: Table Of Contents // Legal Information Institute. — URL: <https://www.law.cornell.edu/uscode/text/18> (accessed: 31.03.2026).
28. Wetboek van Strafrecht, 1881 [Criminal Code, 1881] // Wetboek-online [Criminal Code Online]. — URL: <http://www.wetboek-online.nl/wet/Sr.html#1010> (accessed: 05.04.2026). [in Dutch]
29. Saibāsekyuriti kihonhō, 2014 [Basic Act on Cybersecurity, 2014] // e-Gov Hōrei Kensaku [e-Gov Law Search]. — URL: <https://laws.e-gov.go.jp/law/426AC1000000104/> (accessed: 03.04.2026). [in Japanese]