

Уголовное право

DOI: 10.34670/AR.2026.73.26.069

Национальная политика кибербезопасности Чили: от стратегии 2017–2022 к стратегии 2023–2028**Яковлева Анна Валерьевна**

Доктор экономических наук, профессор,
Российский государственный
педагогический университет им. А.И. Герцена,
191186, Российская Федерация,
Санкт-Петербург, набережная реки Мойки, дом 48
e-mail: yeif@mail.ru

Аннотация

Данная статья посвящена анализу развития национальной политики кибербезопасности в Республике Чили посредством сопоставления стратегических документов на 2017-2022 и 2023-2028 годы. Рассматриваются предпосылки формирования государственной политики в области кибербезопасности, обусловленные цифровой трансформацией экономики, ростом использования информационно-коммуникационных технологий, увеличением числа киберинцидентов и необходимостью совершенствования нормативного регулирования цифровой среды. В статье исследуются положения первой Национальной политики кибербезопасности Чили на 2017-2022 годы, определившей базовые направления государственной политики, включая создание устойчивой информационной инфраструктуры, защиту прав граждан в киберпространстве, развитие культуры кибербезопасности, международное сотрудничество и формирование отрасли кибербезопасности. Отмечается роль цифровой повестки Agenda Digital 2020, в рамках которой была предусмотрена разработка национальной стратегии кибербезопасности, ставшей основой для формирования государственной политики в данной сфере. Особое внимание уделено Национальной политике кибербезопасности Чили на 2023-2028 годы, определяющей стратегические и сквозные цели развития системы кибербезопасности. В статье анализируются ключевые направления новой стратегии, включая развитие институциональной координации, защиту критической инфраструктуры, формирование культуры кибербезопасности, обеспечение прав личности в цифровой среде и поддержку научных исследований и индустрии кибербезопасности. Рассматривается План действий политики, содержащий приоритетные меры реализации государственной стратегии. Автором показана преемственность стратегий и их роль в формировании комплексной национальной системы кибербезопасности Чили, а также последовательный переход от базовой стратегии к институционально ориентированной модели государственной политики в данной сфере.

Для цитирования в научных исследованиях

Яковлева А.В. Национальная политика кибербезопасности Чили: от стратегии 2017–2022 к стратегии 2023–2028 // Вопросы российского и международного права. 2026. Том 16. № 4А. С. 563-573. DOI: 10.34670/AR.2026.73.26.069

Ключевые слова

Национальная политика кибербезопасности Чили, стратегия кибербезопасности, цифровая стратегия Чили, государственная политика кибербезопасности, план действий кибербезопасности, институциональная система кибербезопасности, правовое регулирование кибербезопасности.

Введение

Активное развитие цифровых технологий в Республике Чили стало одним из ключевых факторов формирования государственной политики в области кибербезопасности. Согласно Agenda Digital 2020, к началу 2015 года доступ к сети Интернет имели 67% домохозяйств страны, при этом около 70% населения являлись пользователями сети. Одновременно сохранялись значительные различия в уровне цифрового доступа: в городских районах проникновение технологий составляло около 70%, тогда как в сельской местности - лишь 42%. Существенные различия наблюдались и по уровню доходов: в наиболее обеспеченных домохозяйствах доступ к Интернету достигал 86%, тогда как в наименее обеспеченных - только 54%. Такие показатели свидетельствовали о наличии значительного цифрового неравенства, требующего формирования комплексной государственной политики цифрового развития и обеспечения безопасности цифровой среды. Кроме того, отмечалось, что нормативное регулирование цифровой сферы развивалось неравномерно и отставало от технологических изменений, что создавало риски для прав граждан и устойчивого развития цифровой экономики [Agenda Digital, [www](#)].

Одновременно с расширением цифровой инфраструктуры фиксировался рост киберинцидентов. В частности, Чили входила в число стран Латинской Америки с наибольшим количеством кибератак, при этом значительное распространение получили атаки с использованием вредоносного программного обеспечения и кражи информации с зараженных устройств. Отмечалось использование вредоносного кода типа Dorkbot, сформировавшего более 80 тыс. вредоносных действий, из которых около 44% приходилось на Чили. Кроме того, наблюдалось увеличение числа инцидентов в государственных сетях связи, включая атаки типа DDoS и нарушения функционирования правительственных веб-ресурсов. Также имели место крупные утечки данных, включая компрометацию государственных серверов с раскрытием миллионов персональных записей пользователей [Política Nacional de Ciberseguridad, [www](#)].

В докладе «Построение системы кибербезопасности в Чили, 2023» («Construyendo la Ciberseguridad en Chile, 2023») подчеркивается, что продвижение цифровой трансформации невозможно без разработки адекватной стратегии кибербезопасности, направленной на защиту информационных активов и обеспечение устойчивости к уязвимостям. Отмечается высокая зависимость государства, экономики и общества от цифровых технологий, а также уязвимость страны перед киберинцидентами, способными затронуть функционирование государственных сервисов и критической инфраструктуры. В связи с этим подчеркивается необходимость формирования комплексной государственной политики и развития правового регулирования в сфере кибербезопасности [Construyendo la Ciberseguridad en Chile, 2023, [www](#)].

В этих условиях правительство Чили приступило к формированию национальной политики в области кибербезопасности. Первым этапом стала Национальная политика кибербезопасности на 2017-2022 годы, направленная на создание базовых институциональных и нормативных основ обеспечения безопасности цифровой среды, развитие межведомственного

взаимодействия и повышение уровня готовности к реагированию на киберинциденты. Реализация данной стратегии позволила сформировать основные направления государственной политики в сфере кибербезопасности. Вместе с тем дальнейшая цифровизация экономики и государственного управления, а также появление новых угроз потребовали обновления стратегического подхода. В связи с этим на смену первой стратегии была принята Национальная политика кибербезопасности Чили на 2023-2028 годы, ориентированная на развитие институциональной системы, укрепление защиты критической инфраструктуры, формирование культуры кибербезопасности и обеспечение координации на национальном и международном уровнях.

Первая национальная политика кибербезопасности Чили, 2017-2022 годы

В апреле 2017 года в Республике Чили была, обнародовала первая Национальная политика кибербезопасности Чили на 2017-2022 годы [Política Nacional de Ciberseguridad, [www](http://www.pnciberseguridad.cl)], ставшая ключевым инструментом государственной политики страны, направленным на разработку национальной стратегии в этой области с целью создания свободного, открытого, безопасного и устойчивого киберпространства. Данный документ состоит из двух основных разделов: первый - устанавливает повестку дня с конкретными положениями, которые должны быть реализованы в период 2017-2018 годов, и второй включает долгосрочные цели, ориентированные на 2022 год. Целью данного проекта является предложение обзора того, в каком направлении должна двигаться страна в среднесрочной и долгосрочной перспективе, а также набора мер, которые могут быть реализованы и оценены правительством [Achavar V.B., [www](http://www.pnciberseguridad.cl)].

Данный документ базируется на пяти основных направлениях государственной политики (табл. 1) в области кибербезопасности и серии из 41 меры, которые должны быть реализованы в период с 2018 по 2022 год.

Таблица 1 - Пять направлений государственной политики Чили в сфере кибербезопасности на 2018-2022 гг.

Направление	Характеристика
Устойчивая и надежная информационная инфраструктура	Предусматривает создание информационной инфраструктуры, способной противостоять инцидентам в сфере кибербезопасности и восстанавливаться после них. Включает применение технических мер по предотвращению, управлению и преодолению рисков, определение приоритетных объектов критической информационной инфраструктуры, создание групп реагирования на инциденты, внедрение механизмов отчетности, а также установление дифференциальных стандартов кибербезопасности.
Защита прав граждан в киберпространстве	Ориентирована на предотвращение киберпреступности, укрепление доверия в киберпространстве, определение приоритетов при применении санкций, развитие многосекторальной профилактики, а также соблюдение основных прав граждан.
Развитие культуры кибербезопасности и кибергигиены граждан	Направлено на формирование культуры кибербезопасности, повышение осведомленности общества и развитие обучения по вопросам кибербезопасности.
Международное сотрудничество в области кибербезопасности	Включает реализацию принципов внешней политики Чили, развитие сотрудничества и содействия, расширение участия в многосторонних форумах, а также продвижение международных стандартов, способствующих укреплению доверия и безопасности в киберпространстве.

Направление	Характеристика
Развитие отрасли кибербезопасности	Предполагает поддержку инноваций и развития в сфере кибербезопасности, использование кибербезопасности как инструмента цифрового развития Чили, развитие национальной индустрии кибербезопасности, содействие формированию предложения со стороны местной промышленности и стимулирование спроса со стороны государственного сектора в соответствии со стратегическими интересами государства.

Источник: составлено автором

Этот документ стал отправной точкой для развития институциональных и нормативных механизмов Чили в области информационной безопасности, включая создание центров реагирования на инциденты, укрепление межведомственного сотрудничества и повышение уровня защищённости критических информационных систем.

Данная национальная политика кибербезопасности является частью комплекса мер, которые правительство Чили уже реализовало и разрабатывало в цифровой сфере с целью формирования чётких и системных подходов к определению и регулированию киберпространства. Эти меры были объединены в рамках инициативы «Цифровая повестка Чили 2020» (Agenda Digital 2020). Данный документ представляет собой стратегическую дорожную карту цифрового развития страны, в которой определены среднесрочные цели, приоритетные направления действий и конкретные меры государственной политики. Она была запущена во второй половине 2015 года и направлена на то, чтобы превратить широкое распространение цифровых технологий в инструмент сокращения социального неравенства, создания новых и более качественных возможностей для развития, а также продвижения и защиты прав всех граждан Чили [Agenda Digital, [www](http://www.agendadigital.cl)].

В рамках Цифровой повестки Чили 2020 была предусмотрена специальная мера № 25, нацеленная на разработку национальной стратегии в области кибербезопасности. В документе цифровой повестки эта мера входит в состав блока, связанного с «Государственным цифровым развитием» (Gobierno Digital), среди других инициатив по расширению цифровизации госуслуг и укреплению цифровой инфраструктуры [Agenda Digital, www].

Именно реализацией этой меры и стала Национальная политика кибербезопасности Чили на 2017-2022 годы, которая заложила основы государственного подхода к обеспечению безопасности, доверия и устойчивости в цифровом пространстве страны.

Однако в связи с ростом угроз в киберсфере, и острой необходимостью в укреплении безопасности и устойчивости цифрового пространства страны, а также обеспечении более комплексного, системного и эффективного государственного подхода к кибербезопасности, в августе 2022 года правительство Чили объявило о разработке новой национальной политики кибербезопасности на 2023-2028 годы.

Цели национальной политики кибербезопасности Чили на 2023-2028 годы

16 июня 2023 года Министерством внутренних дел и общественной безопасности Чили был обнародован Указ № 164 утверждающий «Национальную политику кибербезопасности на 2023-2028 годы», который вступил в силу 04 декабря 2023 года. В данном документе кибербезопасность рассматривается как не самоцель, а необходимое условие, позволяющее в полной мере использовать интернет и веб-ресурсы - инструменты, расширяющие возможности

и повышающие эффективность деятельности человека. Отмечается, что усилия по решению различного рода проблем современного мира могут быть облегчены или, напротив затруднены в зависимости от наличием либо отсутствия средств коммуникации, предоставляемых компьютерными сетями и информационными системами [Decreto № 164, [www](#)].

Национальная политика кибербезопасности Чили на 2023-2028 годы носит комплексный характер и направлена на формирование устойчивой национальной системы кибербезопасности, охватывающей институциональные, нормативные, технологические и социальные аспекты обеспечения безопасности цифровой среды [Política Nacional de Ciberseguridad, [www](#)].

Следует отметить, что в документе выделяются две группы целей: стратегические цели и сквозные цели. Стратегические цели определяют основные направления государственной политики в области кибербезопасности и формируют ее содержательную основу. Наряду с ними документ устанавливает сквозные цели, которые носят межсекторальный характер и должны учитываться при реализации всех стратегических направлений политики.

В документе определены пять основных стратегических целей государственной политики в области кибербезопасности:

- Обеспечение устойчивой инфраструктуры. Предполагается формирование надежной и устойчивой информационной инфраструктуры, способной противостоять инцидентам кибербезопасности, а также социальным и экологическим катастрофам, и обеспечивать быстрое восстановление после них на основе подходов управления рисками;
- Защита прав личности. Государство стремится защищать и поощрять соблюдение прав личности в цифровой среде путем укрепления существующих институтов кибербезопасности, а также посредством создания, внедрения и продвижения механизмов и технологических инструментов, позволяющих каждому человеку полноценно интегрироваться в общество, развиваться и свободно выражать себя в интернете;
- Формирование культуры кибербезопасности. Документ предусматривает развитие культуры кибербезопасности, основанной на образовании, распространении передового опыта, ответственном использовании цифровых технологий, а также на соблюдении и поощрении прав человека в цифровой среде;
- Координация на национальном и международном уровнях. Государство предусматривает создание механизмов государственного управления для координации мер в области кибербезопасности. Государственные и частные организации должны взаимодействовать через кооперативные структуры для обмена информацией, предотвращения дублирования усилий и оптимизации использования ресурсов. На международном уровне предполагается координация действий с государствами, международными организациями и иными субъектами с целью более эффективного противодействия вредоносной деятельности и инцидентам в киберпространстве;
- Содействие развитию промышленности и научных исследований. Государство намерено поддерживать развитие индустрии кибербезопасности, направленной на защиту граждан и организаций и соответствующей стратегическим интересам страны. В этой связи предполагается стимулирование прикладных научных исследований в области кибербезопасности с учетом национальных потребностей [Decreto № 164, [www](#)].

Обобщенное представление стратегических целей Национальной политики кибербезопасности Чили на 2023-2028 годы приведено в таблице 2.

**Таблица 2 - Стратегические цели Национальной политики кибербезопасности
Чили на 2023-2028 годы**

Стратегическая цель	Объект воздействия	Ключевой акцент политики	Ожидаемый результат
Устойчивая инфраструктура	Критическая информационная инфраструктура	Управление рисками и устойчивость систем	Повышение устойчивости к киберинцидентам
Защита прав личности	Пользователи цифровой среды	Гарантии цифровых прав и безопасность онлайн	Защита граждан в цифровом пространстве
Культура кибербезопасности	Общество и организации	Образование и ответственное использование технологий	Повышение уровня цифровой грамотности
Национальная и международная координация	Государство и частный сектор	Межведомственное взаимодействие и сотрудничество	Согласованная система реагирования
Развитие индустрии и исследований	Научный и технологический сектор	Поддержка исследований и отрасли кибербезопасности	Развитие национального рынка кибербезопасности

Источник: составлено автором

Как мы можем отметить, представленные цели отражают преемственность с целями, установленными Первой национальной политикой по кибербезопасности на 2017-2022 годы. Вместе с тем новая политика носит инновационный характер, поскольку вводит четыре сквозные цели, направленные на защиту и поощрение прав отдельных лиц и их семей в цифровой среде:

- Обеспечение гендерного равенства. Все инициативы должны учитывать необходимость повышения безопасности женщин в цифровой среде, поскольку именно они чаще становятся жертвами цифрового насилия. Одновременно предусматриваются меры по расширению участия женщин в сфере кибербезопасности посредством позитивных действий, направленных на устранение существующего гендерного дисбаланса. Несмотря на то что женщины составляют более половины населения Чили, их доля в секторе кибербезопасности страны не превышает примерно 15%;
- Защита детей. Все инициативы должны предусматривать приоритетную защиту девочек, мальчиков и подростков при использовании цифровых технологий и интернет-ресурсов;
- Защита пожилых людей. Политика предусматривает разработку мер, направленных на снижение цифровых рисков для пожилого населения и повышение уровня их защищенности в цифровой среде;
- Охрана окружающей среды. Реализация инициатив в области кибербезопасности должна учитывать необходимость минимизации негативного воздействия на окружающую среду [Ciberseguridad en Chile, www; Decreto № 164, www].

Рассмотренные сквозные цели Национальной политики кибербезопасности Чили на 2023-2028 годы обобщены в таблице 3.

Политика также предусматривает разработку Плана действий, содержащего конкретные меры реализации поставленных целей, а также проведение периодических обзоров для оценки эффективности политики в период с 2023 по 2028 годы. Такой план был опубликован позднее в виде отдельного документа - 6 августа 2025 года было принято Постановление № 28, реализующее соглашение Межведомственного комитета по кибербезопасности, которым

утвержден План действий Национальной политики кибербезопасности на 2023-2028 годы [Resolución exenta № 28, www].

Таблица 3 - Сквозные цели Национальной политики кибербезопасности Чили на 2023-2028 годы

Сквозная цель	Приоритетная группа	Основной акцент политики	Направление реализации
Гендерное равенство	Женщины	Повышение безопасности в цифровой среде и расширение участия в сфере кибербезопасности	Снижение цифрового насилия, устранение гендерного дисбаланса
Защита детей и подростков	Несовершеннолетние	Приоритетная защита при использовании цифровых технологий	Безопасная цифровая среда, снижение онлайн-рисков
Защита пожилых людей	Пожилое население	Снижение уязвимости к цифровым угрозам	Повышение цифровой защищенности и доступности технологий
Охрана окружающей среды	Общество в целом	Минимизация экологического воздействия цифровой инфраструктуры	Учет экологических факторов при реализации инициатив

Источник: составлено автором

План действий был сформирован из 76 предложений, из которых отобраны 15 приоритетных мер для реализации политики кибербезопасности на 2023-2028 годы. Автором статьи данные меры условно сгруппированы по следующим направлениям: нормативное и методологическое обеспечение кибербезопасности, институциональное развитие и координация, защита критической инфраструктуры, развитие кадрового потенциала и культуры кибербезопасности, а также развитие индустрии и научных исследований (рис. 1).



Рисунок 1 - Основные направления реализации 15 приоритетных мер Плана действий Национальной политики кибербезопасности Чили на 2023-2028 годы

Представленная Национальная политика кибербезопасности Чили на 2023-2028 годы и План действий по ее реализации сформировали стратегическую основу дальнейшего развития правового регулирования в данной сфере. В последующем положения политики получили нормативное закрепление в Законе № 21.663 о кибербезопасности, который установил институциональную структуру, обязанности субъектов и механизмы контроля. Автор более подробно раскрывает данные аспекты в исследовании, посвященном правовому регулированию кибербезопасности в Республике Чили, где анализируются институциональная модель национальной системы кибербезопасности, функции Национального агентства кибербезопасности (ANCI), порядок взаимодействия государственных органов, а также обязанности поставщиков основных услуг и операторов жизненно важного значения. Таким образом, политика 2023–2028 годов стала важным этапом становления национальной системы кибербезопасности Чили, получившим дальнейшее развитие в законодательном закреплении и формировании комплексной институциональной архитектуры обеспечения кибербезопасности [Яковлева А.В., 2025, 50-59].

Заключение

Подводя итог вышеизложенному отметим, что развитие национальной политики кибербезопасности Чили характеризуется последовательным переходом от стратегии 2017-2022 годов, направленной на формирование базовых институциональных и нормативных основ обеспечения безопасности цифровой среды, к стратегии 2023-2028 годов, предусматривающей комплексный подход к развитию национальной системы кибербезопасности. Вторая политика дополняется Планом действий, содержащим приоритетные меры в области нормативного регулирования, институциональной координации, защиты критической инфраструктуры, развития кадрового потенциала и формирования культуры кибербезопасности. Реализация данных стратегических документов способствовала созданию устойчивой модели государственного управления кибербезопасностью и дальнейшему развитию правового регулирования в данной сфере. Последующие институциональные преобразования и совершенствование нормативной базы позволили Чили значительно повысить уровень киберустойчивости. Согласно данным Национального индекса кибербезопасности (NCSI), на раннем этапе формирования национальной системы кибербезопасности Чили занимала 56-е место в мире с показателем около 59,7%, тогда как по состоянию на апрель 2026 года страна занимает 25-е место, достигнув уровня около 85% [National Cyber Security Index, [www](http://www.nationalcybersecurityindex.org)]. Это свидетельствует о результативности реализуемой государственной политики и подтверждает, что принятие последовательных национальных стратегий стало важным этапом формирования современной системы кибербезопасности в Республике Чили.

Библиография

1. Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) / А.В. Яковлева // Социально-политические науки. - 2021. - Том 11, N 4. - С. 70-81. - DOI: 10.33693/2223-0092-2021-11-4-70-81.
2. Яковлева А.В. Правовое регулирование кибербезопасности в Республике Чили / А.В. Яковлева // Проблемы экономики и юридической практики. - 2025. - Том 21, N 5. - С. 50-59. - DOI: 10.33693/2541-8025-2025-21-5-50-59.
3. Яковлева А.В. Проблемы правового обеспечения в становлении института кибергигиены / А.В. Яковлева // Вестник Университета имени О.Е. Кутафина (МГЮА). - 2023. - № 2. - С. 62-70. - DOI: 10.17803/2311-5998.2023.102.2.062-070.

4. Яковлева А.В. Проблемы правового регулирования информационной безопасности в условиях развития цифровой экономики / А.В. Яковлева. - Саратов : Амирит, 2021. - 272 с.
5. Яковлева А.В. Цифровая грамотность: право, экономика, государственная политика : монография / Яковлева А. В. - Москва : ООО «Издательский дом «Юр-ВАК», 2024. - 168 с.
6. Яковлева А.В., Конюховский П.В. Проблемы кибербезопасности в современном мире: закономерности и перспективы / А.В. Яковлева, П.В. Конюховский // Проблемы экономики и юридической практики. - 2025. - Т. 21. № 2. - С. 39-55. DOI: 10.33693/2541-8025-2025-21-2-39-55. EDN: UBEXHK
7. Яковлева А.В., Конюховский П.В. Проблемы киберпреступности в эпоху гиперволатильности: правовой аспект / А.В. Яковлева, П.В. Конюховский // Проблемы экономики и юридической практики. - 2024. - Т. 20. № 6. - С. 14-34. DOI: 10.33693/2541-8025-2024-20-6- 14-34. EDN: ZZHBYA
8. Achavar V.B. Política Nacional de Ciberseguridad: 2017-2022. - Julio 2018. - [Электронный ресурс] - Режим доступа: URL: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf (дата обращения: 11.11.2025).
9. Agenda Digital 2020. Chile Digital para Tod@s. - [Электронный ресурс] - Режим доступа: URL: https://www.alejandrobarras.com/wp-content/uploads/old/Agenda_Digital_2015-2020_Bachelet_.pdf?utm_source=chatgpt.com (дата обращения: 11.01.2026).
10. Ciberseguridad en Chile: panorama normativo e institucional. Documento de política pública. - Diciembre, 2023 / Noviembre, 2024. - [Электронный ресурс] - Режим доступа: URL: <https://www.derechosdigitales.org/wp-content/uploads/Ciberseguridad-en-Chile-panorama-normativo-e-institucional.pdf> (дата обращения: 01.11.2025).
11. Construyendo la Ciberseguridad en Chile. - Julio, 2023. - [Электронный ресурс] - Режим доступа: URL: https://www.forociber.cl/foro/site/docs/20240322/20240322150520/edicion_construyendo_la_ciberseguridad_en_chile_v2.pdf (дата обращения: 01.04.2026).
12. Decreto № 164. Aprueba Política Nacional de Ciberseguridad 2023-2028. - Promulgación: 16.06.2023. Publicación: 04.12.2023. - [Электронный ресурс] - Режим доступа: URL: <https://www.bcn.cl/leychile/navegar?idNorma=1198702> (дата обращения: 01.11.2025).
13. National Cyber Security Index (NCSI). - [Электронный ресурс] - Режим доступа: URL: <https://ncsi.ega.ee/ncsi-index/> (дата обращения: 01.02.2026).
14. Política Nacional de Ciberseguridad (PNCS) 2016-2022. - [Электронный ресурс] - Режим доступа: URL: <https://generoyparticipacion.interior.gob.cl/media/2023/02/Politica-Nacional-Ciberseguridad-2018-2022.pdf> (дата обращения: 12.11.2025).
15. Política Nacional de Ciberseguridad 2023-2028. Aprobada por S.E. el Presidente de la República, mediante Decreto Supremo №164, de 16 de junio de 2023, publicado en el Diario Oficial de fecha 4 de diciembre de 2023. - [Электронный ресурс] - Режим доступа: URL: <https://lockbits.cl/wp-content/uploads/2024/04/Politica-Nacional-de-Ciberseguridad-2023-2028.pdf> (дата обращения: 12.11.2025).
16. Resolución exenta № 28 que implementa acuerdo del Comité Interministerial sobre Ciberseguridad, que aprueba Plan de Acción de la Política Nacional de Ciberseguridad 2023 - 2028.- Promulgación: 11.07.2025. Publicación: 06.08.2025. - [Электронный ресурс] - Режим доступа: URL: <https://www.bcn.cl/leychile/navegar?idNorma=1215589&idVersion=2025-08-06> (дата обращения: 01.11.2025).

Chile's National Cybersecurity Policy: From the 2017–2022 Strategy to the 2023–2028 Strategy

Anna V. Yakovleva

Doctor of Economic Sciences, Professor,
Herzen State Pedagogical University of Russia,
191186, 48, Moyki river embankment, Saint Petersburg, Russian Federation;
e-mail: yeif@mail.ru

Abstract

This article is devoted to the analysis of the development of the national cybersecurity policy in the Republic of Chile by comparing the strategic documents for 2017–2022 and 2023–2028. The

prerequisites for the formation of state policy in the field of cybersecurity are considered, conditioned by the digital transformation of the economy, the growth in the use of information and communication technologies, the increase in the number of cyber incidents, and the need to improve the regulatory framework of the digital environment. The article examines the provisions of Chile's first National Cybersecurity Policy for 2017–2022, which defined the basic directions of state policy, including the creation of a resilient information infrastructure, the protection of citizens' rights in cyberspace, the development of a cybersecurity culture, international cooperation, and the formation of a cybersecurity industry. The role of the Agenda Digital 2020 is noted, within the framework of which the development of a national cybersecurity strategy was envisaged, which became the basis for the formation of state policy in this sphere. Particular attention is paid to Chile's National Cybersecurity Policy for 2023–2028, which defines the strategic and cross-cutting goals of developing the cybersecurity system. The article analyzes the key directions of the new strategy, including the development of institutional coordination, the protection of critical infrastructure, the formation of a cybersecurity culture, ensuring individual rights in the digital environment, and support for scientific research and the cybersecurity industry. The Policy Action Plan, containing priority measures for implementing the state strategy, is considered. The author shows the continuity of the strategies and their role in the formation of a comprehensive national cybersecurity system of Chile, as well as the consistent transition from a basic strategy to an institutionally oriented model of state policy in this sphere.

For citation

Yakovleva A.V. (2026) Natsional'naya politika kiberbezopasnosti Chili: ot strategii 2017–2022 k strategii 2023–2028 [Chile's National Cybersecurity Policy: From the 2017–2022 Strategy to the 2023–2028 Strategy]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (4A), pp. 563–573. DOI: 10.34670/AR.2026.73.26.069

Keywords

Chile's national cybersecurity policy, cybersecurity strategy, Chile's digital strategy, state cybersecurity policy, cybersecurity action plan, institutional cybersecurity system, legal regulation of cybersecurity.

References

1. Yakovleva A.V. Cybersecurity and its legal regulation (foreign and Russian experience) / A.V. Yakovleva // Social and political sciences. - 2021. - Vol. 11, No. 4. - pp. 70–81. - DOI: 10.33693/2223-0092-2021-11-4-70-81.
2. Yakovleva A.V. Legal regulation of cybersecurity in the Republic of Chile / A.V. Yakovleva // Economic Problems and Legal Practice. – 2025. - Vol. 21. No. 5. - Pp. 50–59. DOI: 10.33693/2541-8025-2025-21-5-50-59.
3. Yakovleva A.V. Problems of legal support in the formation of the institute of cyber hygiene / A.V. Yakovleva // Bulletin of the O.E. Kutafin Moscow State Law University (MSAL). - 2023. - No. 2. - Pp. 62–70. - DOI: 10.17803/2311-5998.2023.102.2.062-070.
4. Yakovleva A.V. Problems of legal regulation of information security in the context of the development of the digital economy / A.V. Yakovleva. - Saratov: Amirit, 2021. - 272 p.
5. Yakovleva A.V. Digital literacy: law, economics, state policy: monograph / Yakovleva A.V. - Moscow: OOO "Yur-VAK" Publishing house, 2024. - 168 p.
6. Yakovleva, A.V., Konyukhovskiy, P.V. Cybersecurity Problems in the Modern World: Regularities and Prospects / A.V. Yakovleva, P.V. Konyukhovskiy // Economic Problems and Legal Practice. - 2025. - Vol. 21. No. 2. - Pp. 39–55. DOI: 10.33693/2541-8025-2025-21-2-39-55. EDN: UBEXHK
7. Yakovleva A.V., Konyukhovskiy P.V. Problems of cybercrime in the era of hypervolatility: legal aspect / A.V. Yakovleva, P.V. Konyukhovskiy // Problems of Economics and Legal Practice. - 2024. - Vol. 20. No. 6. - Pp. 14–34.

DOI: 10.33693/2541-8025-2024-20-6-14-34. EDN: ZZHBYA

8. Achavar V.B. Política Nacional de Ciberseguridad: 2017-2022. - Julio 2018. - [Electronic resource] - Access mode: URL: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf (accessed on: 11.11.2025).
9. Agenda Digital 2020. Chile Digital para Tod@s. - [Electronic resource] - Access mode: URL: https://www.alejandrobarras.com/wp-content/uploads/old/Agenda_Digital_2015-2020_Bachelet_.pdf?utm_source=chatgpt.com (accessed on: 11.01.2026).
10. Ciberseguridad en Chile: panorama normativo e institucional. Documento de política pública. - Diciembre, 2023 / Noviembre, 2024. - [Electronic resource] - Access mode: URL: <https://www.derechosdigitales.org/wp-content/uploads/Ciberseguridad-en-Chile-panorama-normativo-e-institucional.pdf> (accessed on: 01.11.2025).
11. Construyendo la Ciberseguridad en Chile. - Julio, 2023. - [Electronic resource] - Access mode: URL: https://www.forociber.cl/foro/site/docs/20240322/20240322150520/edicion_construyendo_la_ciberseguridad_en_chile_v2.pdf (accessed on: 01.04.2026).
12. Decreto № 164. Aprueba Política Nacional de Ciberseguridad 2023-2028. - Promulgación: 16.06.2023. Publicación: 04.12.2023. - [Electronic resource] - Access mode: URL: <https://www.bcn.cl/leychile/navegar?idNorma=1198702> (accessed on: 01.11.2025).
13. National Cyber Security Index (NCSI). - [Electronic resource] - Access mode: URL: <https://ncsi.ega.ee/ncsi-index/> (accessed on: 01.02.2026).
14. Política Nacional de Ciberseguridad (PNCS) 2016-2022. [Electronic resource] - Access mode: URL: <https://generoyparticipacion.interior.gob.cl/media/2023/02/Politica-Nacional-Ciberseguridad-2018-2022.pdf> (accessed on: 12.11.2025).
15. Política Nacional de Ciberseguridad 2023-2028. Aprobada por S.E. el Presidente de la República, mediante Decreto Supremo №164, de 16 de junio de 2023, publicado en el Diario Oficial de fecha 4 de diciembre de 2023. - [Electronic resource] - Access mode: URL: <https://lockbits.cl/wp-content/uploads/2024/04/Politica-Nacional-de-Ciberseguridad-2023-2028.pdf> (accessed on: 12.11.2025).
16. Resolución exenta № 28 que implementa acuerdo del Comité Interministerial sobre Ciberseguridad, que aprueba Plan de Acción de la Política Nacional de Ciberseguridad 2023 - 2028.- Promulgación: 11.07.2025. Publicación: 06.08.2025. - [Electronic resource] - Access mode: URL: <https://www.bcn.cl/leychile/navegar?idNorma=1215589&idVersion=2025-08-06> (accessed on: 01.11.2025).