Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

УДК 341.6 https://doi.org/10.33619/2414-2948/126/59

БАЛАНС МЕЖДУ КИБЕРБЕЗОПАСНОСТЬЮ И ПРАВОМ НА ПРИВАТНОСТЬ В МЕЖДУНАРОДНОМ ПРАВЕ

©***Чатак уулу А.***, *Международный университет Кыргызстана, г. Бишкек, Кыргызстан*

THE BALANCE BETWEEN CYBERSECURITY AND THE RIGHT TO PRIVACY IN INTERNATIONAL LAW

©***Chatak uulu A.***, *International University of Kyrgyzstan, г. Бишкек, Кыргызстан*

Аннотация. Статья посвящена анализу соотношения требований кибербезопасности и права на приватность в системе международного права. В условиях стремительной цифровизации, роста трансграничных киберугроз и расширения инструментов государственного цифрового контроля проблема баланса между обеспечением национальной и международной безопасности и защитой фундаментальных прав человека приобретает особую актуальность. Исследование направлено на выявление правовых механизмов согласования интересов безопасности и частной жизни в рамках универсальных и региональных международных стандартов. В работе рассматриваются положения международных договоров в сфере прав человека, практика международных судебных органов и современные тенденции развития нормативного регулирования киберпространства. Особое внимание уделяется принципам законности, необходимости, пропорциональности и минимизации вмешательства как ключевым критериям допустимости ограничений права на приватность в условиях киберугроз. Анализируются риски расширения цифрового надзора, трансграничного обмена данными и применения технологий массового мониторинга.

Abstract. This article analyzes the relationship between cybersecurity requirements and the right to privacy in the international legal system. In the context of rapid digitalization, the growth of cross-border cyberthreats, and the expansion of state digital control tools, the issue of balancing national and international security with the protection of fundamental human rights has become particularly pressing. This study aims to identify legal mechanisms for reconciling security and privacy interests within the framework of universal and regional international standards. The paper examines the provisions of international human rights treaties, the practice of international judicial bodies, and current trends in the development of cyberspace regulation. Particular attention is paid to the principles of legality, necessity, proportionality, and minimization of interference as key criteria for the permissibility of restrictions on the right to privacy in the face of cyberthreats. The risks of expanding digital surveillance, cross-border data exchange, and the use of mass monitoring technologies are analyzed.

Ключевые слова: кибербезопасность; право на приватность; международное право; защита персональных данных; цифровое наблюдение.

Keywords: cybersecurity; right to privacy; international law; personal data protection; digital surveillance.

Стремительная цифровизация общественных отношений, трансформация государственных функций в условиях электронного управления и глобальный характер

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

информационных потоков обусловили качественное изменение архитектуры международной безопасности. Рост трансграничных киберугроз, включая кибершпионаж, атаки на критическую инфраструктуру и массовые утечки персональных данных, усиливает потребность государств в разработке эффективных механизмов киберзащиты. Одновременно расширение инструментов цифрового мониторинга и анализа данных порождает риски чрезмерного вмешательства в частную жизнь и ограничения фундаментальных прав человека.

В научной литературе подчеркивается, что современное регулирование киберпространства находится на стыке международного публичного права, права прав человека и национальных режимов информационной безопасности [1, 2].

Исследователи отмечают, что формирование международного режима кибербезопасности неизбежно сопряжено с необходимостью соблюдения универсальных стандартов защиты приватности [3, 4].

Ключевая научная проблема заключается в выявлении допустимых пределов ограничения права на приватность в целях обеспечения кибербезопасности. С одной стороны, государства обязаны защищать национальную и международную безопасность, предотвращая киберпреступность и кибератаки. С другой стороны, международные стандарты прав человека требуют соблюдения принципов законности, необходимости и пропорциональности при любом вмешательстве в сферу частной жизни [5, 11].

Конфликт между этими двумя векторами усиливается в условиях трансграничной передачи данных и развития механизмов международного сотрудничества в сфере киберпреступности (International data transfers and cybersecurity, n.d.). Проблема приобретает особую сложность в контексте цифрового наблюдения и алгоритмических систем анализа данных [6].

Проблематика баланса кибербезопасности и приватности получила развитие в зарубежной и отечественной доктрине. Вопросы правовой природы киберрегулирования рассматриваются в рамках экспертного анализа применения международного права к кибероперациям [7, 8].

В современных исследованиях акцент делается на правозащитном измерении цифровой безопасности, а также на международно-правовых аспектах защиты прав человека в цифровой среде. Вместе с тем сохраняется фрагментарность исследований: большинство работ анализируют либо вопросы кибербезопасности, либо защиту приватности, не формируя комплексной модели их согласования [9].

Целью настоящего исследования является формирование комплексного международно-правового подхода к обеспечению баланса между кибербезопасностью и правом на приватность.

В международно-правовой доктрине кибербезопасность рассматривается как совокупность правовых, организационных и технических мер, направленных на обеспечение устойчивости информационных систем, защиту критической инфраструктуры и предотвращение трансграничных киберугроз. Несмотря на отсутствие универсально закрепленного определения, формирование международного подхода к кибербезопасности происходит в рамках деятельности государств и международных организаций, а также через развитие доктринальных источников. Вопросы применения норм международного права к кибероперациям получили системное отражение, где киберпространство анализируется через призму существующих норм международного гуманитарного права, принципов суверенитета и невмешательства. При этом подчеркивается, что киберпространство не является «внеправовой зоной», а подлежит регулированию на основе общепризнанных норм международного права. Исследователи отмечают, что развитие международного

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

регулирования кибербезопасности тесно связано с вопросами трансграничной юрисдикции и международного сотрудничества [5].

Существенное значение в этом контексте имеет деятельность международных организаций по формированию стандартов противодействия киберпреступности и защите прав человека. Таким образом, кибербезопасность в международном праве формируется как междисциплинарный и комплексный правовой режим, сочетающий элементы безопасности и правозащитного регулирования. Право на приватность является одним из фундаментальных прав человека, закрепленных в универсальных и региональных международных актах. Оно включает защиту личной жизни, корреспонденции, персональных данных и иных аспектов частной сферы. В условиях цифровизации содержание данного права существенно расширяется, охватывая цифровые следы, метаданные и автоматизированную обработку информации. Современные исследования подчеркивают, что цифровая среда создает новые формы вмешательства в частную жизнь, включая массовое наблюдение и алгоритмический анализ поведения. В европейском правовом пространстве особое внимание уделяется защите конфиденциальности коммуникаций и персональных данных как составным элементам права на приватность [7].

Отечественная и зарубежная доктрина указывает на необходимость адаптации международных стандартов к цифровым реалиям [5, 8].

Право на приватность в современном понимании выступает не только как индивидуальная гарантия, но и как структурный элемент демократического правопорядка, обеспечивающий доверие к цифровым институтам и международному сотрудничеству. Международное право допускает ограничение отдельных прав человека при наличии легитимной цели, включая обеспечение национальной безопасности и общественного порядка. Однако такие ограничения должны соответствовать принципам законности, необходимости и пропорциональности. Принцип законности предполагает наличие четкой правовой основы для вмешательства в сферу частной жизни. Принцип необходимости требует доказательства того, что вмешательство является действительно необходимым для достижения легитимной цели. Принцип пропорциональности обязывает соразмерять применяемые меры с масштабом угрозы и минимизировать негативное воздействие на права человека. В условиях противодействия киберугрозам данные принципы приобретают особую значимость, поскольку цифровые инструменты мониторинга обладают высокой степенью инвазивности. В доктрине отмечается, что отсутствие четких критериев пропорциональности может привести к расширению практики массового наблюдения и подрыву доверия к международным механизмам киберрегулирования [4].

Соблюдение указанных принципов выступает ключевым условием легитимности мер кибербезопасности в международном правовом пространстве.

Концепция «цифрового суверенитета» отражает стремление государств установить контроль над информационными потоками, цифровой инфраструктурой и данными, находящимися в пределах их юрисдикции. Данная тенденция усиливается в условиях геополитической напряженности и роста киберугроз. С точки зрения международного права, цифровой суверенитет является развитием традиционного принципа государственного суверенитета в киберпространстве [8].

Однако чрезмерная интерпретация данного принципа может привести к фрагментации глобального цифрового пространства и ослаблению универсальных стандартов защиты прав человека [9].

Проблема особенно остро проявляется в сфере трансграничной передачи данных и международного сотрудничества по вопросам кибербезопасности. Усиление национального

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

контроля над цифровыми ресурсами нередко сопровождается расширением механизмов наблюдения, что требует дополнительного правового контроля в целях соблюдения баланса между государственными интересами и индивидуальными правами.

Современные технологические вызовы, включая использование искусственного интеллекта и автоматизированных систем анализа данных, дополнительно усложняют поиск оптимального соотношения между суверенитетом, безопасностью и приватностью [2]. В этой связи формирование международных стандартов, способных обеспечить согласование интересов государств и защиту фундаментальных прав человека, приобретает первостепенное значение.

ООН играет ключевую роль в формировании универсальных подходов к регулированию киберпространства. В рамках Генеральной Ассамблеи и профильных экспертных групп вырабатываются рекомендации по ответственному поведению государств в информационном пространстве. Концептуально подход ООН основывается на признании применимости действующего международного права к киберпространству, включая принципы суверенитета, невмешательства и мирного разрешения споров [3].

Особое значение имеет деятельность Управления ООН по наркотикам и преступности, разрабатывающего практические механизмы противодействия киберпреступности с учетом стандартов прав человека. В данных документах подчеркивается необходимость соблюдения принципов законности и пропорциональности при применении мер цифрового мониторинга. Таким образом, ООН формирует рамочную нормативную архитектуру, в которой кибербезопасность рассматривается не изолированно, а в тесной связи с международной системой защиты прав человека.

Право на приватность закреплено в универсальных и региональных международных договорах, включая Международный пакт о гражданских и политических правах (МПГПП) и региональные конвенции. Хотя данные акты были приняты до цифровой эпохи, их положения подлежат расширительному толкованию в условиях цифровизации. Современная доктрина подчеркивает, что право на неприкосновенность частной жизни охватывает не только физическую, но и цифровую сферу. Европейская практика развивает стандарты защиты коммуникационной конфиденциальности и персональных данных как составных элементов права на приватность [7].

В научной литературе отмечается, что международные договоры выполняют функцию «нормативного противовеса» расширяющимся полномочиям государств в сфере цифровой безопасности. Таким образом, международные акты по правам человека формируют юридические пределы вмешательства в частную жизнь при реализации мер кибербезопасности. Будапештская конвенция 2001 года стала первым международным договором, комплексно регулирующим вопросы киберпреступности и трансграничного сотрудничества. Ее значение заключается в гармонизации уголовно-правовых норм, создании механизмов взаимной правовой помощи и стандартизации процедур сбора электронных доказательств. Конвенция способствует унификации подходов к расследованию киберпреступлений, однако одновременно вызывает дискуссии относительно баланса между эффективностью правоохранительных мер и защитой прав человека. Вопросы трансграничной передачи данных и доступа к информации остаются наиболее чувствительными с точки зрения соблюдения права на приватность [12].

Таким образом, Будапештская конвенция представляет собой пример институционализированного механизма международного сотрудничества, который одновременно усиливает кибербезопасность и требует строгого соблюдения правозащитных стандартов.

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

Европейский союз сформировал одну из наиболее развитых моделей правового регулирования в сфере цифровой безопасности и защиты персональных данных. Регулятивная модель ЕС основана на комплексном подходе, сочетающем требования к киберустойчивости инфраструктуры с жесткими стандартами обработки персональных данных. Исследователи отмечают, что европейский подход демонстрирует пример институционального баланса между безопасностью и правами личности [4]. Особое значение имеет защита конфиденциальности коммуникаций и развитие механизмов трансграничной передачи данных с учетом гарантий приватности [6].

Современные вызовы, включая внедрение систем искусственного интеллекта, усиливают потребность в адаптации нормативной базы к новым технологическим рискам [3].

В результате формируется модель «регулируемой цифровой среды», в которой кибербезопасность не противопоставляется правам человека, а интегрируется в их правовую структуру.

Таблица 1

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕЖДУНАРОДНЫХ МЕХАНИЗМОВ

Механизм	*Основная цель*	*Инструменты регулирования*	*Влияние на право на приватность*
United Nations	Формирование универсальных принципов кибербезопасности	Резолюции, экспертные группы, рекомендации	Устанавливает рамочные стандарты с учетом прав человека
МПГПП и региональные конвенции	Защита фундаментальных прав	Договорные нормы и судебная практика	Ограничивают вмешательство через принципы законности и пропорциональности
Budapest Convention	Борьба с киберпреступностью	Гармонизация уголовного права, взаимная правовая помощь	Требует соблюдения правозащитных гарантий при расследовании
European Union	Интегративное цифровое регулирование	Регламенты, директивы, механизмы надзора	Формирует высокий стандарт защиты данных и конфиденциальности

Практика обеспечения кибербезопасности на уровне государств все чаще опирается на цифровое наблюдение как инструмент предупреждения угроз, выявления киберпреступности и защиты критической инфраструктуры. Однако именно в этой сфере наиболее ярко проявляется конфликт между императивами безопасности и правом на приватность. В доктрине подчеркивается, что цифровые инструменты наблюдения обладают высокой степенью вторжения (доступ к коммуникациям, метаданным, геолокации), а потому требуют строгих юридических ограничителей и независимого контроля [8].

С точки зрения международных стандартов, вмешательство в частную жизнь допустимо лишь при одновременном соблюдении требований законности, необходимости и пропорциональности, а также при наличии процедурных гарантий (судебного или иного независимого контроля). Эти стандарты прямо учитываются в правоприменительных подходах в сфере противодействия киберпреступности, где подчеркивается необходимость согласования оперативных мер с правами человека. В противном случае меры киберзащиты могут трансформироваться в перманентное наблюдение, подрывающее доверие к государству и международному сотрудничеству в цифровой сфере [2].

Пример практической коллизии: применение широких режимов data retention» (обязательное хранение данных связи) или массового перехвата трафика в целях безопасности

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

нередко сталкивается с вопросом: является ли такое вмешательство минимально необходимым и насколько оно соразмерно реальной угрозе [1, 5].

Трансграничная передача данных — один из центральных узлов конфликта безопасности и приватности, поскольку киберугрозы по своей природе не ограничены национальными границами, а расследование киберпреступлений требует оперативного доступа к данным, которые часто хранятся в другой юрисдикции. Это порождает конкуренцию правопорядков и коллизию требований: государство-инициатор запроса стремится к эффективности расследования, а государство-хранитель данных — к соблюдению стандартов приватности и собственных регулятивных ограничений [7].

В таких условиях на практике формируется многоуровневый режим: взаимная правовая помощь, прямые запросы к провайдерам, экстренные процедуры сохранения данных. Однако, чем «быстрее» механизм, тем выше риск недостаточного правового контроля и снижения гарантий приватности. В научной литературе подчеркивается, что именно трансграничная передача данных становится полем для выработки компромиссных решений: процедурной прозрачности, минимизации собираемых данных и закрепления стандартов конфиденциальности коммуникаций [8].

Пример практической коллизии: запрос одного государства на доступ к данным пользователя, размещенным на серверах в другой стране, может вступать в противоречие с национальными/региональными стандартами защиты данных и конфиденциальности связи, что приводит к спору о применимом праве и допустимых пределах экстерриториального доступа. Атрибуция кибератак (установление субъекта, которому может быть юридически вменено деяние) является одной из наиболее сложных правоприменительных проблем в международном праве. Даже при наличии технических индикаторов компрометации вопрос юридической атрибуции требует доказательственной базы и обоснования связи между действиями конкретных акторов и государством. Это усложняет применение норм об ответственности государств и затрудняет реализацию мер реагирования, включая контрмеры и международно-правовые претензии [3].

В доктринальных источниках подчеркивается, что киберпространство не исключает действие общих принципов международного права, однако его специфика (анонимность, распределенная инфраструктура, использование прокси-актеров) приводит к «разрыву» между техническим установлением происхождения атаки и юридическим установлением ответственности. В результате государства на практике чаще опираются на политико-дипломатические форматы обвинения, санкционные подходы и коалиционные заявления, чем на строгие юридические процедуры [10].

Пример практической коллизии: государство может заявить о причастности другого государства к атаке на критическую инфраструктуру, но отсутствие раскрываемых доказательств атрибуции ограничивает возможности правовой защиты и ведет к доминированию политической логики над юридической [9].

Современные практики кибербезопасности все чаще включают автоматизированные системы анализа данных, поведенческого моделирования, прогнозирования угроз и фильтрации контента. Эти технологии повышают эффективность защиты, но одновременно усиливают риск системного вмешательства в приватность. Проблема заключается не только в сборе больших массивов данных, но и в их последующем алгоритмическом «прочтении»: профилировании, выявлении социальных связей, прогнозировании намерений, что выходит за рамки традиционных представлений о приватности [1].

Особую сложность создают решения на базе искусственного интеллекта, когда правоприменительная логика заменяется статистической: индивид может стать объектом

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

повышенного контроля не из-за совершенного деяния, а из-за вероятностной модели. В исследованиях, посвященных регулятивным вызовам новых технологий, подчеркивается необходимость юридической «встраиваемости» гарантий приватности в архитектуру цифровой безопасности. При отсутствии таких гарантий меры киберзащиты могут приводить к эффекту «перманентного наблюдения» и нормализации масштабного контроля [2].

Пример практической коллизии: использование систем автоматического выявления угроз в сетевом трафике может требовать глубокой инспекции пакетов и анализа метаданных, что влечет системное вмешательство в конфиденциальность коммуникаций и требует особенно строгого теста пропорциональности [7].

Таблица 2

КОНФЛИКТ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ В ПРАКТИКЕ: ТИПОВЫЕ СИТУАЦИИ И ПРАВОВЫЕ РИСКИ

Практика	*Цель безопасности*	*Потенциальное вмешательство в приватность*	*Ключевой международно-правовой «тест»*
Массовое цифровое наблюдение	Предупреждение угроз, выявление киберпреступности	Перехват/анализ коммуникаций и метаданных	Законность + необходимость + пропорциональность + независимый контроль
Трансграничные запросы данных	Расследование инцидентов, сбор e-evidence	Экстерриториальный доступ к данным, коллизия режимов защиты	Юрисдикция + процедурные гарантии + минимизация данных
Атрибуция и ответственность	Реакция на кибератаки, претензии/контрмеры	Риск ошибок атрибуции, политизация доказательств	Доказательственность + критерии вменения государству
Алгоритмический контроль/ИИ	Прогнозирование и автоматизация защиты	Профилирование, автоматизированные решения, расширение мониторинга	Прозрачность + минимизация + контроль вмешательства

Развитие искусственного интеллекта (ИИ) и автоматизированных систем безопасности радикально меняет практику противодействия киберугрозам: от реактивных мер (фиксация инцидента) государства и частные операторы переходят к прогнозно-аналитическим моделям (поведенческая аналитика, обнаружение аномалий, автоматическое реагирование). Однако правовая проблема заключается в том, что алгоритмические решения усиливают «невидимость» вмешательства в приватность: мониторинг становится постоянным, а оценка рисков — вероятностной, что затрудняет применение традиционных критериев необходимости и пропорциональности [1].

В европейском контексте отмечается, что новые технологии требуют одновременного регулирования ответственности, приватности и кибербезопасности как взаимосвязанных сфер, поскольку автоматизация безопасности нередко означает расширение доступа к массивам данных, включая метаданные коммуникаций и данные поведения пользователя [2]. Следовательно, международное регулирование должно учитывать не только «техническую эффективность» ИИ, но и встраивание правовых гарантий в архитектуру цифровой безопасности (privacy-by-design, accountability-by-design), что соответствует общей логике правозащитного подхода [7].

Пример вызова: системы поведенческого скоринга в киберзащите могут классифицировать пользователей как «подозрительных» на основе статистических

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

корреляций. Это порождает риск необоснованного усиления контроля без процессуальной возможности оспаривания, что проблематично с точки зрения международных стандартов прав человека [6].

Трансграничный характер киберугроз делает международное сотрудничество системообразующим условием эффективной кибербезопасности. На практике сотрудничество реализуется через обмен информацией, взаимную правовую помощь, совместные расследования, а также через унификацию подходов к сбору электронных доказательств. В то же время эффективность сотрудничества ограничивается различиями правовых режимов приватности, процедур доступа к данным и подходов к цифровому суверенитету. В доктрине подчеркивается, что стабильная международная модель возможна лишь при формировании «минимальных универсальных стандартов» защиты прав человека в цифровой среде, которые должны быть признаны базовой рамкой любой киберполитики [11]. Практические руководства, разрабатываемые в системе ООН, также фиксируют, что сотрудничество по киберпреступности должно осуществляться с учетом прав человека и процессуальных гарантий.

Пример вызова: в рамках трансграничных запросов к данным государства стремятся к ускоренным каналам доступа, однако упрощение процедур неизбежно повышает риск несоразмерного вмешательства в приватность, особенно если отсутствуют единые стандарты конфиденциальности коммуникаций [7].

Перспективы развития международного регулирования напрямую связаны с формированием сбалансированной модели, в которой кибербезопасность не противопоставляется правам человека, а выступает частью правовой экосистемы. Такая модель должна включать три взаимосвязанных уровня: 1. Нормативный (четкие юридические основания вмешательства); 2. Процедурный (контроль, надзор, прозрачность и способы обжалования); 3. Технологический (минимизация данных, ограничение целей обработки, встроенные механизмы защиты приватности).

В исследованиях по правовым и этическим аспектам цифровой безопасности подчеркивается, что «баланс» не может сводиться к декларации — он требует институциональных механизмов подотчетности и доказуемости необходимости вмешательства [5]. Параллельно отмечается, что демократическое управление в сфере кибербезопасности предполагает наличие внешнего контроля над силовыми и технологическими инструментами, иначе возникает риск нормализации массового мониторинга [2].

Системный подход подтверждается и доктринальными источниками, применяющими нормы международного права к кибероперациям: даже при высокой угрозе безопасности государства обязаны действовать в границах международных принципов и правозащитных стандартов [8].

Пример инструмента баланса: закрепление обязательного независимого контроля (судебного/квазисудебного), публичных критериев пропорциональности и ограничения сроков хранения данных как условий допустимости вмешательства в приватность при киберугрозах [9].

Дискуссия о создании универсальной международной конвенции по кибербезопасности (или киберпреступности) отражает стремление преодолеть фрагментарность регулирования и несоответствие национальных режимов. На сегодняшний день наиболее институционально оформленным договорным механизмом остается Будапештская конвенция, однако ее восприятие не является универсальным, что ограничивает глобальную гармонизацию. Перспектива универсальной конвенции связана с двумя ключевыми условиями: Признание

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

базовых правозащитных стандартов как «ядра» регулирования (приватность, конфиденциальность коммуникаций, процессуальные гарантии); Разработка единых процедур международного сотрудничества по электронным доказательствам и трансграничному доступу к данным при сохранении теста пропорциональности.

С точки зрения международного права важен также вопрос применимости общих принципов (суверенитет, невмешательство, должная осмотрительность) к киберпространству — именно эти элементы должны быть встроены в будущую договорную рамку, чтобы конвенция не противоречила существующему международному правопорядку. Пример возможной архитектуры конвенции: «двухконтурная» модель, где первый контур фиксирует стандарты прав человека и пределы вмешательства, а второй — процедурные механизмы сотрудничества (запросы данных, сохранение электронных доказательств, экстренные процедуры), причем второй контур действует только при соблюдении первого.

Таблица 3

КЛЮЧЕВЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ МЕЖДУНАРОДНОГО РЕГУЛИРОВАНИЯ

Направление	*Вызов*	*Риск для приватности*	*Перспективное решение*
ИИ и автоматизация безопасности	Алгоритмическая непрозрачность решений	Профилирование, постоянный мониторинг, ошибочные «подозрения»	Accountability, прозрачность, встроенные гарантии privacy-by-design
Международное сотрудничество	Различие режимов приватности и доступа к данным	Экстерриториальный доступ, ослабление контроля	Унификация минимальных стандартов и процедур
Сбалансированная модель	Дисбаланс «безопасность > права»	Нормализация наблюдения	Трехуровневая модель: нормы + процедуры + технологии
Универсальная конвенция	Фрагментарность и политическая поляризация	Размывание правозащитных гарантий	Двухконтурная конвенция: права человека + сотрудничество

Проведённый анализ показал, что проблема соотношения кибербезопасности и права на приватность является одной из центральных в современном международном праве. Цифровизация общественных отношений и трансграничный характер киберугроз объективно усиливают роль государств в обеспечении информационной безопасности. Вместе с тем расширение цифрового мониторинга, трансграничного обмена данными и автоматизированных систем анализа информации создаёт риски чрезмерного вмешательства в частную жизнь и подрыва фундаментальных прав человека [1, 4].

Международные механизмы регулирования, включая деятельность системы ООН, договорные режимы противодействия киберпреступности и правозащитные стандарты, демонстрируют стремление к формированию баланса между безопасностью и приватностью. Однако существующая нормативная архитектура остаётся фрагментарной и неоднородной. Проблемы атрибуции кибератак, трансграничной юрисдикции и алгоритмического контроля подтверждают необходимость системного подхода к регулированию киберпространства.

Таким образом, баланс между кибербезопасностью и правом на приватность не может рассматриваться как статичное соотношение. Он представляет собой динамическую правовую конструкцию, требующую постоянной адаптации к технологическим изменениям и новым формам цифровых рисков. Теоретическая значимость исследования заключается в развитии интегративного подхода к анализу кибербезопасности и права на приватность как

Т. 12. №5 2026
https://doi.org/10.33619/2414-2948/126

взаимосвязанных элементов международного правопорядка. В отличие от традиционного разграничения сфер «безопасности» и «прав человека», в работе обоснована необходимость их концептуального объединения в рамках единой правовой модели, основанной на принципах законности, необходимости и пропорциональности [7].

Практическая значимость состоит в возможности использования предложенных выводов при разработке международных соглашений, совершенствовании национального законодательства и формировании механизмов международного сотрудничества в сфере кибербезопасности. Результаты исследования могут быть применены в правотворческой деятельности, при оценке допустимости цифрового наблюдения, а также в практике трансграничного обмена данными и расследования киберпреступлений.

Рекомендации по совершенствованию международного регулирования:

1. Закрепление универсальных минимальных стандартов защиты приватности в международных документах, регулирующих кибербезопасность, включая обязательное применение теста пропорциональности при ограничении прав человека;

2. Институционализация независимого контроля за мерами цифрового наблюдения на международном и национальном уровнях (судебный или квазисудебный надзор, прозрачные процедуры отчётности);

3. Унификация процедур трансграничного доступа к данным, обеспечивающая баланс между эффективностью расследования и защитой конфиденциальности коммуникаций;

4. Внедрение принципов privacy-by-design и accountability при использовании искусственного интеллекта и автоматизированных систем безопасности, что позволит минимизировать риски алгоритмического контроля;

5. Разработка универсальной международной договорной модели, в которой нормы о сотрудничестве в сфере кибербезопасности будут неразрывно связаны с правозащитными гарантиями, исключая их ослабление в интересах оперативности.

Перспективными направлениями дальнейших исследований представляются: Анализ правовой природы алгоритмических решений в сфере кибербезопасности и их соответствия международным стандартам прав человека; Сравнительное исследование региональных моделей регулирования (ЕС, Азия, ЕАЭС) в аспекте цифрового суверенитета и приватности; Разработка критериев международной атрибуции кибератак с учётом технических и юридических факторов; Исследование влияния квантовых технологий и новых криптографических инструментов на баланс безопасности и конфиденциальности; Формирование концепции «цифровой должной осмотрительности» государств в киберпространстве.

В целом дальнейшее развитие международного регулирования кибербезопасности должно строиться на признании того, что защита приватности не является препятствием для безопасности, а выступает её структурным элементом и условием легитимности международного правопорядка в цифровую эпоху.

Список литературы:

1. Allahrakha N. Balancing cyber-security and privacy: legal and ethical considerations in the digital age // Legal Issues in the digital Age. 2023. №2. P. 78-121. https://doi.org/10.17323/10.17323/2713-2749.2023.2.78.121

2. Buckland B. S., Schreier F., Winkler T. H. Democratic governance challenges of cyber security. Geneva: DCAF, 2010. V. 1. P. 12.

3. Danel'yan A. A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva //Obrazovanie i pravo. 2020. №1. P. 261-269.

4. Кикоть-Глуходедова Т. В. Конституционно-правовые основы обеспечения национальной безопасности современной России // Международный журнал конституционного и государственного права. 2018. №4. С. 38-42.

5. Kudriasova Z. Cryptologic Techniques and Associated Risks in Public and Private Security. An Italian and European Union Perspective with an Overview of the Current Legal Framework //arXiv preprint arXiv:2505.08650. 2025. https://doi.org/10.48550/arXiv.2505.08650

6. Lukings M., Lashkari A. H. Understanding cybersecurity law and digital privacy. Springer International Publishing, 2022.

7. Novelli C., Casolari F., Hacker P., Spedicato G., Floridi L. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity // Computer Law & Security Review. 2024. V. 55. P. 106066.

8. Segura-Serrano A. Internet regulation and the role of international law // Max Planck Yearbook of United Nations Law Online. 2006. V. 10. №1. P. 191-272.

9. Schmitt M. N. (ed.). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press, 2017.

10. Canton H. United Nations Office on drugs and crime—UNODC //The Europa directory of international organizations 2021. Routledge, 2021. P. 240-244.

11. Walia I. K. Cyber surveillance and privacy issues vis-à-vis international law // Brawijaya Law Journal. 2023. V. 10. №2. P. 219-241. https://doi.org/10.1515/til-2019-0010

12. Zuiderveen Borgesius F. J., Steenbruggen W. The right to communications confidentiality in Europe: protecting privacy, freedom of expression, and trust // Theoretical Inquiries in Law. 2019. V. 20. №1. P. 291-322. https://doi.org/10.1515/til-2019-0010

References:

1. Allahrakha, N. (2023). Balancing cyber-security and privacy: legal and ethical considerations in the digital age. *Legal Issues in the digital Age*, (2), 78-121. https://doi.org/10.17323/10.17323/2713-2749.2023.2.78.121

2. Buckland, B. S., Schreier, F., Winkler, T. H., & Centre pour le contrôle démocratique des forces armées (Genève). (2010). *Democratic governance challenges of cyber security* (Vol. 1, p. 12). Geneva: DCAF.

3. Danel'yan, A. A. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstva. *Obrazovanie i pravo*, (1), 261-269. (in Russian).

4. Kikot′-Glukhodedova, T. V. (2018). Konstitutsionno-pravovye osnovy obespecheniya natsional′noj bezopasnosti sovremennoj Rossii. *Mezhdunarodnyj zhurnal konstitutsionnogo i gosudarstvennogo prava,* (4), 38-42. (in Russian).

5. Kudriasova, Z. (2025). Cryptologic Techniques and Associated Risks in Public and Private Security. An Italian and European Union Perspective with an Overview of the Current Legal Framework. *arXiv preprint arXiv:2505.08650*. https://doi.org/10.48550/arXiv.2505.08650

6. Lukings, M., & Lashkari, A. H. (2022). *Understanding cybersecurity law and digital privacy*. Springer International Publishing.

7. Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity. *Computer Law & Security Review*, *55*, 106066.

8. Segura-Serrano, A. (2006). Internet regulation and the role of international law. *Max Planck Yearbook of United Nations Law Online*, *10*(1), 191-272.

9. Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

10. Canton, H. (2021). United Nations Office on drugs and crime—UNODC. In *The Europa directory of international organizations 2021* (pp. 240-244). Routledge.

11. Walia, I. K. (2023). Cyber surveillance and privacy issues vis-à-vis international law. *Brawijaya Law Journal*, *10*(2), 219-241.

12. Zuiderveen Borgesius, F. J., & Steenbruggen, W. (2019). The right to communications confidentiality in Europe: protecting privacy, freedom of expression, and trust. *Theoretical Inquiries in Law*, *20*(1), 291-322. https://doi.org/10.1515/til-2019-0010

Поступила в редакцию
06.03.2026 г.

Принята к публикации
14.03.2026 г.

Ссылка для цитирования:

Чатак уулу А. Баланс между кибербезопасностью и правом на приватность в международном праве // Бюллетень науки и практики. 2026. Т. 12. №5. С. 482-493. https://doi.org/10.33619/2414-2948/126/59

Cite as (APA):

Chatak uulu, A. (2026). The Balance Between Cybersecurity and the Right to Privacy in International Law. *Bulletin of Science and Practice, 12*(5), 482-493. (in Russian). https://doi.org/10.33619/2414-2948/126/59