ISSN: 2181-9416
4-SON, 2026

YURIST AXBOROTNOMASI

ВЕСТНИК ЮРИСТА * LAWYER HERALD

HUQUQIY, IJTIMOIY, ILMIY-AMALIY JURNAL

iD g doi crossref CYBERLENINKA НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU

ISSN 2181-9416
DOI JURNAL: 10.34920/2181-9416/2026/4

YURIST AXBOROTNOMASI

4-SON

ВЕСТНИК ЮРИСТА

НОМЕР 4

LAWYER HERALD

ISSUE 4

Toshkent — 2026

БАХРИДДИНОВА Бехруза Бахриддиновна
Самостоятельный соискатель Института законодательства и правовой политики при Президенте Республики Узбекистан
E-mail: bexruza.baxriddinova@mail.ru

ИНСТИТУЦИОНАЛЬНО-ПРАВОВАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Для цитирования (iqtibos keltirish uchun, for citation): БАХРИДДИНОВА Б.Б. Институционально-правовая модель обеспечения информационной безопасности в условиях развития информационного общества // Yurist axborotnomasi – Вестник юриста – Lawyer herald. № 4 (2026) С. 147-157.

4 (2026) DOI https://doi.org/10.34920/2181-9416/2026/4-016

АННОТАЦИЯ

В статье исследуется институционально-правовая модель обеспечения информационной безопасности в условиях развития информационного общества сквозь призму согласования интересов личности, общества и государства. Цель статьи заключается в обосновании информационной безопасности как комплексного правового института, обеспечивающего реализацию информационных прав человека, цифровую устойчивость общества и защиту легитимных интересов государства. Использованы формально-юридический, системно-структурный, сравнительно-правовой, институциональный и функциональный методы, а также аналитическая апробация модели на актуальных данных о киберинцидентах, рисках третьих сторон и межведомственной интеграции персональных данных. Проанализированы законодательство Республики Узбекистан, Стратегия кибербезопасности на 2026–2030 годы, международные стандарты и зарубежные исследования 2024–2026 годов. В качестве научной новизны предложена трехконтурная модель, объединяющая контур прав личности, контур общественной устойчивости и контур государственной устойчивости, а также пятиэтапный тест баланса. Определены механизмы интеграции модели в деятельность действующих институтов государственного управления, пакет нормативно-правовых мер и трехэтапная схема ее реализации до 2030 года. Обосновано введение оценки воздействия проектов нормативно-правовых актов и государственных информационных систем на цифровые права и информационную безопасность.

Ключевые слова: информационное общество, информационная безопасность, институционально-правовая модель, цифровые права, неприкосновенность частной жизни, общественная устойчивость, государственный суверенитет, соразмерность, кибербезопасность, институциональная подотчетность, оценка воздействия.

BAXRIDDINOVA Bexruza Baxriddinovna
O'zbekiston Respublikasi Prezidenti huzuridagi
Qonunchilik va huquqiy siyosat instituti mustaqil izlanuvchisi
E-mail: bexruza.baxriddinova@mail.ru

AXBOROT JAMIYATINI RIVOJLANTIRISH SHAROITIDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING INSTITUTSIONAL-HUQUQIY MODELI

ANNOTATSIYA

Maqolada axborot jamiyati rivojlanishi sharoitida axborot xavfsizligini ta'minlashning institutsional-huquqiy modeli shaxs, jamiyat va davlat manfaatlarini muvozanatlashtirish nuqtayi nazaridan tadqiq etilgan. Maqolaning maqsadi axborot xavfsizligini insonning axborot huquqlari, jamiyatning raqamli barqarorligi va davlatning legitim xavfsizlik manfaatlarini uyg'unlashtiruvchi kompleks huquqiy institut sifatida asoslashdan iborat. Formal-yuridik, tizimli-tuzilmaviy, qiyosiy-huquqiy, institutsional va funksional tahlil usullari, shuningdek kiberhodisalar, uchinchi tomon xavflari va shaxsga doir ma'lumotlarning idoralararo integratsiyasiga oid dolzarb ma'lumotlar asosida modelning tahliliy aprobatsiyasi qo'llanildi. O'zbekiston qonunchiligi, 2026–2030-yillarga mo'ljallangan Kiberxavfsizlik strategiyasi, xalqaro standartlar hamda 2024–2026-yillardagi xorijiy tadqiqotlar tahlil qilindi. Ilmiy yangilik sifatida uch konturli model va besh bosqichli muvozanat testi taklif etildi. Modelni amaldagi davlat boshqaruvi institutlari faoliyatiga integratsiya qilish mexanizmlari, normativ-huquqiy choralar paketi hamda 2030-yilgacha uch bosqichli joriy etish sxemasi belgilandi. Normativ-huquqiy hujjatlar va davlat axborot tizimlarining raqamli huquqlar hamda axborot xavfsizligiga ta'sirini oldindan baholash zarurati asoslandi.

Kalit so'zlar: axborot jamiyati, axborot xavfsizligi, institutsional-huquqiy model, raqamli huquqlar, shaxsiy hayot daxlsizligi, ijtimoiy barqarorlik, davlat suvereniteti, mutanosiblik, kiberxavfsizlik, institutsional hisobdorlik, ta'sirni baholash.

BEKHRUZA Bakhriddinovna
Independent researcher at the Institute of
Legislation and Legal Policy under the
President of the Republic of Uzbekistan
E-mail: bexruza.baxriddinova@mail.ru

AN INSTITUTIONAL AND LEGAL MODEL FOR ENSURING INFORMATION SECURITY IN THE DEVELOPMENT OF THE INFORMATION SOCIETY

ANNOTATION

The article examines an institutional and legal model for ensuring information security in the development of the information society through the reconciliation of the interests of the individual, society and the state. The article conceptualises information security as a comprehensive legal institution enabling the exercise of human information rights, societal digital resilience and the protection of the state's legitimate security interests. Formal legal, systemic-structural, comparative legal, institutional and functional methods were applied, together with an analytical validation of the model using current data on cyber incidents, third-party risks and inter-agency integration of personal data. The legislation of the Republic of Uzbekistan, the Cybersecurity Strategy for 2026–2030, international standards and foreign research published in 2024–2026 were analysed. The article proposes a three-circuit model and a five-stage balancing test. It specifies mechanisms for integrating the model into existing public administration institutions, a package of legal measures and a three-stage implementation pathway through 2030. The

study substantiates the introduction of an impact assessment for draft legal acts and public information systems in relation to digital rights and information security.

Keywords: information society, information security, institutional and legal model, digital rights, privacy, societal resilience, state sovereignty, proportionality, cybersecurity, institutional accountability, impact assessment.

Цифровая трансформация изменила не только способы производства, коммуникации и оказания государственных услуг, но и саму юридическую природу информационной среды. Информация из самостоятельного экономического ресурса превратилась в инфраструктурное условие осуществления конституционных прав, функционирования публичной власти и устойчивости базовых социальных систем. Электронные государственные услуги, цифровые финансовые инструменты, медицинские информационные системы, дистанционное образование и платформенные коммуникации расширяют возможности человека, одновременно создавая риски незаконного оборота персональных данных, нарушения непрерывности критической инфраструктуры, киберпреступности, дискриминации на основе автоматизированных решений и манипулятивного воздействия на общественное сознание. В этих условиях информационная безопасность перестает быть исключительно технической категорией и приобретает качество комплексного конституционно-правового института.

Конституция Республики Узбекистан закрепляет неприкосновенность частной жизни, тайну переписки и электронных сообщений, право на защиту персональных данных, а также свободу искать, получать и распространять информацию. Одновременно конституционное регулирование требует, чтобы применяемые государственными органами меры правового воздействия основывались на законе, преследовали конституционно значимую цель и были соразмерны характеру охраняемого интереса [1]. Из этого следует, что информационная безопасность не может формироваться как автономный режим, находящийся вне системы основных прав. Напротив, ее содержание должно определяться двойной функцией: защитой цифровой инфраструктуры и созданием условий для реального осуществления прав и свобод.

На уровне отраслевого законодательства безопасность в информационной сфере определяется через защищенность интересов личности, общества и государства [2]. Законодательство о кибербезопасности конкретизирует требования к защите информационных систем и ресурсов, а законодательство о персональных данных формирует самостоятельный режим правомерной обработки и охраны сведений о человеке [3; 4]. Принятие Стратегии кибербезопасности Республики Узбекистан на 2026–2030 годы усилило стратегическое планирование, межведомственную координацию и персональную ответственность руководителей государственных органов и организаций [5]. Вместе с тем наличие специальных правовых режимов еще не означает их концептуальной согласованности.

В современной доктрине прослеживаются две крайние позиции. Первая отождествляет безопасность преимущественно с государственным суверенитетом и защищенностью инфраструктуры, вследствие чего права личности и общественный контроль воспринимаются как внешние ограничения эффективности. Вторая абсолютизирует информационную свободу и недооценивает позитивную обязанность государства предупреждать киберриски, обеспечивать непрерывность жизненно важных услуг и защищать граждан от неправомерного использования их данных. Обе позиции методологически уязвимы, поскольку исходят из предположения о неизбежной конкуренции безопасности и свободы.

Б.А.Ахмедов, рассматривая институциональные основы информационной безопасности, выделяет в качестве ее субъектов личность, общество и государство и связывает эффективность системы с согласованностью государственной политики, нормативного регулирования, мониторинга, координации и подготовки кадров [6, С. 9–12]. Развивая данную позицию применительно к современному информационному обществу, необходимо перейти от описания

совокупности субъектов к построению юридической архитектуры, которая определяет не только полномочия, но и пределы вмешательства, гарантии прав, процедуры согласования интересов и критерии результативности.

Традиционное понимание информационной безопасности строится вокруг состояния защищенности информации и поддерживающей ее инфраструктуры. Оно сохраняет нормативную ценность, поскольку фиксирует цель охранительного воздействия. Однако цифровые риски отличаются изменчивостью, трансграничным характером и способностью вызывать каскадные последствия. Защита одного элемента системы может одновременно создать новые риски для другого: например, расширение массивов данных для профилактики угроз повышает ценность таких массивов для злоумышленников и усиливает последствия возможной утечки.

ОЭСР предлагает рассматривать цифровую безопасность как управление экономическими и социальными рисками цифровой среды, а не как максимизацию технической защиты независимо от ее цены и воздействия на другие ценности. Меры безопасности должны соответствовать целям деятельности, вероятности и масштабу вреда, не устраняя при этом преимущества цифровизации, инновации и основные права [7, С. 10–15]. NIST CSF 2.0 включает управление в число самостоятельных функций и выстраивает цикл из шести элементов: **управление (Govern), идентификация (Identify), защита (Protect), обнаружение (Detect), реагирование (Respond) и восстановление (Recover)** [8, С. 3–8]. Общим для этих подходов является переход от разовой защиты к непрерывному управлению.

Зарубежная научная литература 2024–2026 годов демонстрирует переход от узкого технико-охранительного понимания кибербезопасности к правоориентированной и социотехнической модели управления. П.Г. Кьяра обосновывает формирование нормативных предпосылок права на кибербезопасность и ставит вопрос о доступных человеку средствах правовой защиты при неисполнении обязанностей субъектами цифровой безопасности [16]. М. Кандиль показывает, что конституционные гарантии должны толковаться с учетом цифровой среды и сопровождаться процедурами судебного контроля и осторожным подходом к новым ограничениям цифровых прав [18]. Обзор А. Поулсена и соавторов подтверждает, что игнорирование цифровых прав при проектировании цифровых сервисов способно усиливать уже существующие неравенства и требует специальных стандартов их предварительного учета [19].

Одновременно исследования в области публичного управления указывают на разрыв между стратегическими документами и измеримой организационной практикой. Систематический обзор Л. Магнуссона и соавторов, в котором из первоначально выявленных 1496 публикаций были отобраны и проанализированы 41 работа, выявил фрагментарность технологических решений, недостаток показателей результативности, устойчивых моделей риска и регулярного аудита в публичном секторе [17]. Т. Синожич и Ю. Янель подчеркивают необходимость оценки новых технологий через категорию безопасности человека, включающую частную жизнь, недискриминацию и благополучие [20]. Б. Котта и М.С. Ригеттини рассматривают эффективную политику кибербезопасности как сочетание информационных, властно-регулятивных, финансовых и организационных инструментов [21], а Ф. Тейхманн показывает, что принцип «кибербезопасность на этапе проектирования» реализуется только тогда, когда он становится устойчивой практикой инженеров, руководителей, регуляторов и пользователей на протяжении всего жизненного цикла цифровой системы [22]. Эти выводы подтверждают необходимость не только концептуальной, но и процедурной интеграции предлагаемой модели.

На основании проведенного анализа предлагается понимать информационную безопасность как конституционно обусловленную управляемую устойчивость информационной среды, при которой права личности, общественно значимые коммуникации и легитимные интересы государства обеспечиваются посредством законного, риск-ориентированного, соразмерного и подотчетного управления. Термин «управляемая устойчивость» подчеркивает отсутствие абсолютной безопасности, но одновременно закрепляет позитивную обязанность государства и

иных ответственных субъектов предупреждать риски, минимизировать ущерб, восстанавливать нарушенные права и извлекать институциональные выводы из каждого значимого инцидента.

Предлагаемая дефиниция позволяет разграничить информационную безопасность и кибербезопасность. Кибербезопасность представляет технологико-инфраструктурный сегмент, ориентированный на защиту систем, сетей, ресурсов и процессов от угроз в киберпространстве. Информационная безопасность шире: она включает свободу информации, защиту персональных данных, достоверность публичной коммуникации, устойчивость общественных институтов, информационный суверенитет и гарантии от незаконного вмешательства. Развитая система киберзащиты является необходимым, но недостаточным условием безопасного информационного общества.

Баланс интересов нередко понимается как поиск средней точки между тремя заранее заданными величинами. Такое представление не учитывает контекстуальный характер правовой оценки. Значимость интереса зависит от вероятности и тяжести вреда, природы защищаемого объекта, масштаба вмешательства, продолжительности меры и наличия менее ограничительных альтернатив. При атаке на медицинскую или энергетическую систему приоритет приобретают оперативность и непрерывность услуг. При массовом наблюдении за коммуникациями повышенные требования предъявляются к законности, конкретности оснований, срокам, независимому разрешению и последующему контролю.

Человекоцентричный подход рассматривает сети и цифровые платформы как инфраструктуру реализации современных прав и поэтому не ограничивает безопасность территориальным суверенитетом [14, С. 411–424]. Одновременно государство в цифровой сфере выполняет несколько ролей: регулирует, предоставляет услуги, поддерживает общественную устойчивость, участвует в партнерстве, производит знания и само способно создавать риски для прав [15, С. 37–59]. Следовательно, модель должна одновременно обеспечивать действенность публичной власти и юридические пределы ее усмотрения.

Предлагаемая модель включает три взаимосвязанных контура. Контур прав личности охватывает свободу искать, получать и распространять информацию, неприкосновенность частной жизни, контроль над персональными данными, защиту от дискриминационных автоматизированных решений, справедливую процедуру и эффективные средства правовой защиты. Контур общественной устойчивости включает непрерывность общественно значимых услуг, информационный плюрализм, цифровую инклюзию, медиаграмотность, доверие к официальной коммуникации и участие гражданского общества. Контур государственной устойчивости объединяет суверенитет, конституционный строй, критическую информационную инфраструктуру, непрерывность публичного управления, правопорядок и международное сотрудничество.

Связь между контурами обеспечивается четырьмя процессуальными механизмами: законностью и правовой определенностью; риск-ориентированной необходимостью и соразмерностью; четким распределением полномочий и ответственности; независимым контролем, обжалованием и пересмотром. Отсутствие любого из этих механизмов превращает формулу баланса в декларацию. Например, законная цель без точных пределов полномочий создает риск произвольного вмешательства; технически эффективная мера без возможности обжалования лишает заинтересованное лицо реальной защиты.

Таким образом, баланс представляет собой не статическое равновесие и не арифметическое равенство интересов, а юридически организованный процесс их контекстуального согласования. Его результатом должно быть решение, которое обеспечивает достаточный уровень защиты при минимально необходимом ограничении прав и открытости информационной среды.

Институциональную модель нельзя сводить к наличию единственного компетентного органа. Информационная безопасность охватывает стратегическое управление, техническую защиту, персональные данные, свободу информации, правоохранительную деятельность, судебную

защиту, образование, научную экспертизу и частную инфраструктуру. Централизация необходима для формирования единой политики, минимальных стандартов, категорирования критических объектов, совместимости систем и обмена сведениями об инцидентах. Однако концентрация всех оперативных решений и информационных массивов в одном центре способна породить конфликт интересов, единые точки отказа и ослабление контроля.

В связи с этим обосновывается формула «централизованные стандарты – распределенная ответственность – независимый контроль». На стратегическом уровне определяются национальные приоритеты, минимальные требования, правила межведомственного взаимодействия и индикаторы результативности. На отраслевом уровне каждый государственный орган, субъект критической информационной инфраструктуры и крупный оператор данных выступает владельцем риска, возникающего в пределах его деятельности. На контрольном уровне суд, парламентские механизмы, прокурорский надзор, институты защиты персональных данных и общественный контроль оценивают законность и соразмерность вмешательства.

Стратегия кибербезопасности на 2026–2030 годы создала основу для стратегической координации, персональной ответственности руководителей и деятельности Координационного национального совета [5]. Следующий этап должен заключаться не в механическом увеличении числа органов, а в процессуальной интеграции кибербезопасности с институтами свободы информации, защиты персональных данных, электронного правительства и прав человека. Для этого необходимы обязательные консультации при подготовке решений, единый протокол уведомления об инцидентах, правила устранения конфликта компетенций, совместная оценка рисков и четкое разграничение оперативной, регулятивной и контрольной функций.

Международные модели подтверждают многокомпонентный характер институциональной зрелости. Глобальный индекс кибербезопасности МСЭ оценивает государства по правовым, техническим, организационным мерам, развитию потенциала и сотрудничеству [9]. Директива NIS 2 объединяет ответственность руководства, управление рисками, уведомление об инцидентах, надзор и взаимодействие [13]. Следовательно, институциональная эффективность определяется не объемом полномочий отдельного органа, а качеством согласованных обязанностей, информационных потоков и механизмов ответственности.

Отдельное значение имеет государственно-частное сотрудничество. Значительная часть цифровой инфраструктуры и данных находится у негосударственных операторов, поэтому исключительно административная модель не способна обеспечить необходимую устойчивость. Правовое регулирование должно определять стандарты ответственного раскрытия уязвимостей, сроки уведомления об инцидентах, условия обмена технической информацией, совместные учения и гарантии сохранения коммерческой тайны и персональных данных. Партнерство не должно означать передачу публичных функций без соответствующей подотчетности.

Интеграция трехконтурной модели в национальную систему не требует создания **единого «мегарегулятора»** и может быть осуществлена посредством включения единой процедуры оценки в уже действующее распределение компетенций. *Координационный национальный совет по кибербезопасности* целесообразно определить площадкой утверждения методики, перечня высокорисковых проектов, межведомственных приоритетов и ежегодного сводного доклада. *Служба государственной безопасности* как уполномоченный государственный орган в области кибербезопасности должна формировать критерии киберриска, требования к категорированию объектов, уведомлению об инцидентах и реагированию [3; 5]. *Министерство цифровых технологий* может встроить оценку воздействия в обязательную экспертизу проектов и технической документации государственных информационных систем, их реестр, процедуру приемки и оценку деятельности заместителей руководителей по цифровизации [26]. *Государственный центр персонализации при Кабинете Министров* должен оценивать законность целей обработки, минимизацию и сроки хранения данных, разграничение доступа и гарантии прав субъектов персональных данных [27].

Министерству юстиции целесообразно поручить проверку правовой определенности оснований вмешательства, наличия менее ограничительных альтернатив, порядка обжалования и восстановления нарушенного права. *Каждый отраслевой государственный орган, оператор критической информационной инфраструктуры и владелец государственной информационной системы* должен выступать владельцем остаточного риска и утверждать план его обработки персонально ответственным руководителем. *Независимый контроль* обеспечивается не дублированием оперативных функций, а последующей проверкой судами, парламентскими механизмами, прокурорским надзором, Омбудсманом, общественными советами и внешним аудитом. Таким образом, трехконтурная модель превращается в сквозной процесс: инициатор проекта формирует карту данных и рисков; профильные органы дают функциональные заключения; уполномоченный руководитель принимает мотивированное решение об остаточном риске; независимые институты получают возможность проверить законность, соразмерность и результативность.

Наиболее сложной задачей является определение границы между законной мерой безопасности и неправомерным вмешательством в права. *Комитет ООН по правам человека* исходит из того, что ограничение свободы выражения и доступа к информации должно быть установлено законом, преследовать конкретную легитимную цель, отвечать требованиям необходимости и соразмерности, причем обязанность обосновать ограничение лежит на государстве [10, п. 18, 21–36]. *Резолюция Генеральной Ассамблеи ООН о праве на неприкосновенность частной жизни в цифровую эпоху* требует эффективных гарантий против незаконного или произвольного наблюдения, сбора и обработки данных [11]. *Конвенция 108+* закрепляет принципы законности, ограничения цели, пропорциональности данных, прозрачности и независимого надзора [12].

Для операционализации данных стандартов предлагается пятиэтапный тест баланса.

Первый этап – **законность и определенность**: содержание меры, компетенция органа, основания применения, срок, круг лиц и объем данных должны быть предусмотрены доступной и предсказуемой нормой.

Второй этап – **доказанный риск и легитимная цель**: вмешательство не может основываться на абстрактном предположении; риск должен подтверждаться проверяемыми данными, а цель — иметь конституционное основание.

Третий этап – **необходимость**: устанавливается, существует ли менее ограничительное, но сопоставимо эффективное средство достижения цели.

Четвертый этап – **соразмерность в узком смысле**: ожидаемая польза для безопасности сопоставляется с прямым и косвенным ущербом правам, общественной открытости, инновациям и экономической деятельности.

Пятый этап – **подотчетность и пересмотр**: должны быть обеспечены независимое разрешение или контроль, фиксация мотивов решения, право на обжалование, ограничение срока, удаление избыточных данных, компенсация вреда и последующая оценка эффективности.

Тест исключает восприятие свободы и безопасности как отношений с нулевой суммой. Шифрование, надежная аутентификация, минимизация данных и защита, встроенная в архитектуру системы, одновременно повышают ее устойчивость и гарантируют частную жизнь. Напротив, неопределенные полномочия и избыточный сбор данных могут кратковременно расширить возможности контроля, но в долгосрочной перспективе увеличивают масштаб потенциального ущерба, создают условия для злоупотреблений и подрывают доверие. Юридически качественная мера безопасности должна не максимизировать вмешательство, а минимизировать совокупный риск для всех трех контуров.

Полученные результаты показывают ограниченность схемы «личность против государства». Права человека не могут полноценно осуществляться без безопасной инфраструктуры, устойчивых государственных услуг и защиты от преступного использования данных. В то же время политика безопасности без правовых границ, открытости и доверия не обладает достаточной легитимностью и способна воспроизводить новые угрозы. Общество в данной системе не является пассивным

посредником: оно обладает самостоятельными интересами в информационном плюрализме, надежности коммуникаций, непрерывности услуг, цифровой инклюзии и сохранении общественного доверия.

В национальном исследовании институциональных основ информационной безопасности ранее была обоснована необходимость координации, мониторинга, единых стандартов и подготовки профессиональных кадров [6, С. 66–82]. Современное законодательное развитие свидетельствует о последовательном укреплении данных элементов. Однако внедрение больших данных, биометрической идентификации, межведомственной интеграции и систем искусственного интеллекта смещает центральную проблему: от согласования технических подразделений – к согласованию прав, полномочий, ответственности и алгоритмических последствий.

Практическая ценность трехконтурной модели проявляется в том, что она требует до принятия решения идентифицировать все затрагиваемые интересы. Например, интеграция государственных баз данных может сократить административные издержки и предотвратить мошенничество. Одновременно она увеличивает концентрацию информации, расширяет круг доступа и способна влиять на решения в отношении человека. Поэтому проект должен оцениваться по объему и категориям данных, целям обработки, срокам хранения, разграничению доступа, последствиям автоматизированных решений, киберустойчивости и доступности механизма обжалования.

В этой связи предлагается ввести оценку воздействия на цифровые права и информационную безопасность для проектов нормативно-правовых актов, государственных информационных систем, интеграционных платформ и высокорисковых технологий. Такая оценка шире традиционной экспертизы кибербезопасности. Она должна включать: карту данных и заинтересованных субъектов; анализ воздействия на права и общественные услуги; модель угроз; сравнение альтернатив; минимизацию данных; встроенные технические и организационные гарантии; независимый контроль; средства восстановления права; измеримые индикаторы результата.

Нормативно-правовое обеспечение модели предполагает взаимосвязанный пакет решений.

Во-первых, в законодательстве о нормативно-правовых актах, электронном правительстве, информатизации, кибербезопасности и персональных данных следует закрепить обязательную оценку воздействия на цифровые права и информационную безопасность для высокорисковых проектов. К таким проектам относятся массовая межведомственная интеграция данных, биометрическая идентификация, автоматизированное принятие юридически значимых решений, обработка специальных категорий данных, создание объектов критической информационной инфраструктуры и системы, отказ которых способен нарушить предоставление жизненно важных услуг.

Во-вторых, к техническому заданию, бюджетной заявке, заключению обязательной экспертизы и акту ввода системы в эксплуатацию должен прилагаться «паспорт цифрового воздействия», содержащий цели и правовые основания обработки, карту потоков данных, модель угроз, альтернативы, гарантии по каждому контуру, остаточный риск и измеримые показатели.

В-третьих, совместным нормативным актом заинтересованных органов необходимо утвердить единую методику, шкалу риска, типовые формы заключений, сроки согласования и правила устранения разногласий.

В-четвертых, следует установить обязательность уведомления о существенных инцидентах, фиксации управленческих решений, периодического аудита, повторной оценки после существенного изменения системы и публикации обезличенных агрегированных результатов.

Поэтапная реализация должна быть синхронизирована со сроками Стратегии кибербезопасности на 2026–2030 годы. На первом этапе (2026–2027 годы) целесообразно разработать методику и провести пилотную апробацию в трех сферах с различным профилем риска: электронные государственные услуги, здравоохранение и налоговое администрирование. На втором этапе (2028 год) оценка становится обязательной для всех высокорисковых нормативных и цифровых проектов и включается в бюджетирование, государственные закупки, экспертизу и

ввод в эксплуатацию. На третьем этапе (2029–2030 годы) вводятся независимый аудит, публичная агрегированная отчетность, анализ извлеченных из инцидентов уроков и регулярный пересмотр методики. Переход к следующему этапу должен зависеть не только от календарного срока, но и от достижения критериев готовности: наличия обученных специалистов, работающего обмена сведениями, завершенных пилотов, утвержденных индикаторов и проверенных механизмов обжалования.

Степень открытости оценки должна соотноситься с режимом охраняемой информации. Технические уязвимости и сведения, составляющие государственную тайну, не подлежат необоснованному раскрытию. Вместе с тем правовое основание решения, его цель, общая категория риска, примененные гарантии и агрегированные показатели результативности могут быть представлены общественности в доступной форме. Открытость в данном случае выступает не противоположностью безопасности, а механизмом обнаружения ошибок, использования распределенных знаний и укрепления институционального доверия.

Оценка эффективности также не должна ограничиваться числом предотвращенных атак или зарегистрированных инцидентов. Рост числа выявленных событий может означать как ухудшение защищенности, так и повышение качества обнаружения. Поэтому индикаторы целесообразно формировать по трем контурам. Для личности – количество утечек, срок восстановления нарушенного права, результативность жалоб и доверие пользователей. Для общества – непрерывность критически важных услуг, цифровая доступность и устойчивость официальной коммуникации. Для государства – время обнаружения, локализации и восстановления, результаты аудита критических систем, качество межведомственных учений и соблюдение стандартов.

Для проверки применимости предложенной модели проведена аналитическая апробация на трех типах эмпирического материала: агрегированных данных о киберинцидентах, статистике нарушений с участием третьих сторон и конкретном национальном проекте межведомственной интеграции данных. Такая апробация не заменяет экспериментально-полевого пилота, однако позволяет проверить, выявляет ли модель одновременно риски для прав личности, непрерывности общественно значимых услуг и устойчивости государственного управления.

ENISA Threat Landscape 2024 основан на анализе более 11 тыс. инцидентов: публичное управление стало наиболее часто атакуемым сектором (19%), а DDoS-атаки и программы-вымогатели в совокупности составили более половины наблюдавшихся событий [23]. *В отчете Verizon DBIR 2025* проанализировано свыше 22 тыс. инцидентов, включая 12 195 подтвержденных утечек; участие третьих сторон удвоилось и достигло 30%, эксплуатация уязвимостей выросла на 34%, а программы-вымогатели присутствовали в 44% нарушений [24]. Эти данные показывают, что оценка только технической защищенности отдельного органа недостаточна: необходимо учитывать поставщиков, общие платформы, каскадные последствия отказов и влияние на доверие пользователей. В национальной практике показателен предусмотренный постановлением *Президента Республики Узбекистан от 15 июля 2026 года № ПП-265* механизм автоматического обновления с 1 октября 2026 года основных персональных данных граждан в государственных информационных системах через **Межведомственную интеграционную платформу** [25]. Он способен одновременно повысить точность реестров и удобство услуг, но требует журналирования источника изменения, уведомления гражданина, оперативного исправления ошибочных сведений, разграничения доступа и определения ответственности за каждую стадию передачи данных.

Ограничение исследования состоит в том, что проведенная апробация имеет аналитический, а не экспериментально-полевой характер и использует открытые агрегированные данные. Следующим этапом должна стать пилотная апробация в сферах электронных государственных услуг, здравоохранения и налогового администрирования с участием государственных органов, операторов критической инфраструктуры, судейского сообщества, специалистов по информационным технологиям, бизнеса и институтов гражданского общества. До начала пилота необходимо зафиксировать исходные показатели, а после его завершения сопоставить

время выявления и устранения рисков, количество предотвращенных нарушений, длительность восстановления услуг, результативность жалоб, число исправленных ошибок в данных и уровень доверия пользователей. Такая схема позволит проверить не только логическую согласованность, но и исполнимость процедур и измеримость предлагаемых индикаторов.

Проведенное исследование подтверждает, что информационная безопасность представляет собой не узкую сферу технической защиты и не самостоятельную привилегию публичной власти, а комплексный институционально-правовой механизм согласования прав личности, общественной устойчивости и легитимных интересов государства.

Во-первых, баланс интересов личности, общества и государства не является заранее установленной иерархией. Он имеет динамический характер и определяется реальностью риска, значимостью охраняемой ценности, интенсивностью вмешательства, наличием альтернатив и эффективностью правовых гарантий.

Во-вторых, предложена трехконтурная модель, включающая контур прав личности, контур общественной устойчивости и контур государственной устойчивости. Их согласование обеспечивается законностью, риск-ориентированной соразмерностью, распределением ответственности, независимым контролем и эффективным обжалованием.

В-третьих, институциональная архитектура должна основываться на формуле «централизованные стандарты – распределенная ответственность – независимый контроль». Такая конструкция позволяет совместить единство государственной политики с отраслевой ответственностью и предотвратить чрезмерную концентрацию полномочий.

В-четвертых, меры, затрагивающие информационные права, должны проходить пятиэтапный тест, включающий законность и определенность, доказанность риска и легитимность цели, необходимость, соразмерность, подотчетность и пересмотр.

В-пятых, целесообразно внедрить предварительную оценку воздействия на цифровые права и информационную безопасность применительно к проектам нормативно-правовых актов, государственным информационным системам, интеграции баз данных и высокорисковым цифровым технологиям.

В-шестых, предложен механизм институциональной интеграции модели без создания нового централизованного органа: стратегическая координация, киберэкспертиза, цифровая экспертиза, защита персональных данных, правовая экспертиза, отраслевое владение риском и независимый контроль объединяются общей процедурой и единым «паспортом цифрового воздействия».

В-седьмых, обоснована трехэтапная реализация модели до 2030 года – от разработки методики и пилотов к обязательному применению в высокорисковых проектах, а затем к независимому аудиту и ex post оценке. Аналитическая апробация на данных ENISA, Verizon и национальном кейсе межведомственного обновления персональных данных показала способность модели выявлять взаимосвязанные риски для всех трех контуров.

Правоориентированная информационная безопасность является не альтернативой свободе, а условием ее реального осуществления; права человека, открытость и подотчетность, в свою очередь, образуют основу легитимности и долгосрочной эффективности институтов безопасности.

СНОСКИ/IQTIBOSLAR/REFERENCES:

1. Конституция Республики Узбекистан. Принята на референдуме 30.04.2023. URL: https://lex.uz/docs/-6445145

2. Закон Республики Узбекистан «О принципах и гарантиях свободы информации» от 12.12.2002 № 439-II. URL: https://lex.uz/docs/-52268

3. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 № ЗРУ-764. URL: https://lex.uz/docs/-5960604

4. Закон Республики Узбекистан «О персональных данных» от 02.07.2019 № ЗРУ-547, с изменениями, внесенными Законом от 26.03.2026 № ЗРУ-1125. URL: https://lex.uz/ru/docs/4396428; https://lex.uz/docs/8104580

5. Указ Президента Республики Узбекистан «Об определении Стратегии кибербезопасности Республики Узбекистан и совершенствовании системы предупреждения киберпреступности» от 10.03.2026 № УП-38. URL: https://lex.uz/ru/docs/8079286

6. Ахмедов Б.А. Институциональные основы обеспечения информационной безопасности в Республике Узбекистан. – Ташкент: Высшая школа стратегического анализа и прогнозирования Республики Узбекистан, 2017. – 123 с. (Akhmedov B.A. Institutional Foundations for Ensuring Information Security in the Republic of Uzbekistan. – Tashkent, 2017. – 123 p.).

7. OECD. OECD Policy Framework on Digital Security. – Paris: OECD Publishing, 2022. – 38 p. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

8. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. – Gaithersburg, 2024. – 32 p. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

9. International Telecommunication Union. Global Cybersecurity Index 2024. – Geneva: ITU, 2024. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

10. UN Human Rights Committee. General Comment No. 34: Article 19 — Freedoms of Opinion and Expression. CCPR/C/GC/34. – Geneva, 2011. URL: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

11. United Nations General Assembly. The Right to Privacy in the Digital Age. Resolution A/RES/77/211, adopted on 15 December 2022. – New York: United Nations, 2023. – 10 p. URL: https://digitallibrary.un.org/record/3999709

12. Council of Europe. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). – Strasbourg, 2018. – 35 p. URL: https://edoc.coe.int/en/international-law/7729-convention-108-convention-for-the-protection-of-individuals-with-regard-to-the-processing-of-personal-data.html

13. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) // Official Journal of the European Union. – 2022. – L 333. – P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

14. Deibert R.J. Toward a Human-Centric Approach to Cybersecurity // Ethics & International Affairs. – 2018. – Vol. 32, No. 4. – P. 411–424. DOI: https://doi.org/10.1017/S0892679418000618

15. Dunn Cavelty M., Egloff F.J. The Politics of Cybersecurity: Balancing Different Roles of the State // St Antony's International Review. – 2019. – Vol. 15, No. 1. – P. 37–59. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf

16. Chiara P.G. Towards a Right to Cybersecurity in EU Law? The Challenges Ahead // Computer Law & Security Review. – 2024. – Vol. 53. – Article 105961. DOI: https://doi.org/10.1016/j.clsr.2024.105961.

17. Magnusson L., Iqbal S., Elm P., Dalipi F. Information Security Governance in the Public Sector: Investigations, Approaches, Measures, and Trends // International Journal of Information Security. – 2025. – Vol. 24. – Article 177. DOI: https://doi.org/10.1007/s10207-025-01097-x.

18. Qandeel M. Understanding Constitutional Principles for the Advancement of Digital Rights in Palestine // Middle East Law and Governance. – 2024. – Vol. 16, No. 3. – P. 400–429. DOI: https://doi.org/10.1163/18763375-20241444.

19. Poulsen A., Song Y.J.C., Fosch-Villaronga E., et al. Digital Rights and Mobile Health in Southeast Asia: A Scoping Review // Digital Health. – 2024. – Vol. 10. – Article 20552076241257058. DOI: https://doi.org/10.1177/20552076241257058.

20. Sinozic T., Jahnel J. Technology Assessment for Human Security: Aligning Security Cultures with Human Security in AI Innovation // TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis. – 2024. – Vol. 33, No. 2. – P. 16–21. DOI: https://doi.org/10.14512/tatup.33.2.16.

21. Cotta B., Righettini M.S. Governing Cybersecurity in the Digital Age: Mapping Comprehensive Policy Mixes with the Nodality–Authority–Treasure–Organization Lens // Review of Policy Research. – 2026. – Vol. 43, No. 4. – Article e70113. DOI: https://doi.org/10.1111/ropr.70113.

22. Teichmann F.M.J. Platform Governance under NIS2 and the Cyber Resilience Act: Cybersecurity by Design as Social Practice // Information, Communication & Society. – Published online 06.01.2026. DOI: https://doi.org/10.1080/1369118X.2025.2609780.

23. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. – Athens: ENISA, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

24. Verizon. 2025 Data Breach Investigations Report. – 2025. URL: https://www.verizon.com/business/resources/reports/dbir/.

25. Министерство цифровых технологий Республики Узбекистан. Количество услуг на my.gov.uz будет расширено: информация о постановлении Президента Республики Узбекистан от 15.07.2026 № ПП-265. URL: https://gov.uz/ru/digital/news/view/194413.

26. Министерство цифровых технологий Республики Узбекистан. Задачи и функции. URL: https://www.digital.gov.uz/ru/digital/pages/tasks_and_functions.

27. Министерство цифровых технологий Республики Узбекистан. О персональных данных. URL: https://www.digital.gov.uz/ru/advice/61/document/2116.

YURIST AXBOROTNOMASI

4-SON

ВЕСТНИК ЮРИСТА

НОМЕР 4

LAWYER HERALD

ISSUE 4

ISSN 2181-9416

DOI JURNAL: 10.34920/2181-9416/2026/4

2026-YIL