***Салишев Сергей Николаевич.***

***Сеюбергенова Дидар Сламовна***

***Исманов Таалайбек Кадырович***

*DOI 10.31483/r-149586*

# МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА

***Аннотация**: в главе рассматривается вопрос уголовно-правовой защиты информационной безопасности на международном уровне. Основное внимание уделяется национальному законодательству США, Великобритании, Франции и Германии в этой сфере. Анализируются основные нормативно-правовые акты, направленные на обеспечение кибербезопасности, механизмы ответственности за нарушения в области информационной безопасности. Рассматриваются различные аспекты защиты информационных ресурсов, включая защиту государственной тайны, частной жизни и критически важных объектов информационной инфраструктуры.*

*Анализ международного опыта противодействия преступлениям в сфере информационной безопасности выявил ключевые проблемы: сложности с идентификацией злоумышленников, трудности в расследовании и раскрытии преступлений. Предлагается создать международную конвенцию по информационной безопасности под эгидой ООН. Делается вывод, что регионализация актов может привести к росту атак из стран, не подписавших соглашения. Важно регулировать ответственность за запись непубличных разговоров, распространение преступно полученных данных и мошенничество для доступа к охраняемой информации.*

***Ключевые слова**: информационная безопасность, уголовно-правовая защита, кибербезопасность, национальное законодательство, ответственность за нарушения, защита информационных ресурсов.*

***Abstract**: the chapter considers the issue of criminal-legal protection of information security at the international level. The main attention is paid to the*

*national legislation of the USA, Great Britain, France and Germany in this area. The main regulatory legal acts aimed at ensuring cybersecurity, as well as liability mechanisms for violations in the field of information security are analyzed. Various aspects of information resource protection are considered, including the protection of state secrets, privacy and critical information infrastructure facilities.*

*An analysis of international experience in countering crimes in the field of information security revealed key problems: difficulties in identifying intruders, difficulties in investigating and solving crimes. It is proposed to create an international convention on information security under the auspices of the UN. It is concluded that the regionalization of acts can lead to an increase in attacks from countries that have not signed the agreement. It is important to regulate liability for recording non-public conversations, dissemination of criminally obtained data and fraudulent access to protected information.*

***Keywords**: information security, criminal law protection, cybersecurity, national legislation, liability for violations, protection of information resources.*

В настоящее время уголовно-правовая защита информационной безопасности на международном уровне находится в стадии формирования. Отсутствие единого нормативно-правового акта обусловлено сложностью и многоаспектностью проблемы, а также различиями в правовых системах государств. Тем не менее отдельные аспекты этой проблематики уже регулируются национальным законодательством многих стран, что свидетельствует о признании важности защиты информационных ресурсов на глобальном уровне.

На национальном уровне государства принимают специальные законы и подзаконные акты для защиты информации. Например, *американская уголовно-правовая доктрина* уделяет значительное внимание противодействию кибертерроризму, определяя его как незаконные компьютерные атаки на государственные информационные системы с целью запугивания или принуждения к действиям, направленным на достижение политических или социальных целей.

Киберпространство рассматривается как средство совершения террористических атак, нарушающих неприкосновенность цифровой собственности.

У. Лакёр отмечает, что развитие технологий в эпоху электронных коммуникаций создало условия для возникновения кибертерроризма, который ранее существовал лишь в фантастических произведениях. Сочетание технологий и терроризма, считает автор, представляет серьезную угрозу для будущего [1, p. 254].

М. Конвей, классифицируя деяния в сети «Интернет» на правомерные и неправомерные, отмечает, что «правомерное использование включает общение, коммуникацию, выражение идей и использование электронной почты. Неправомерное использование охватывает нарушение неприкосновенности информационных ресурсов, взлом веб-сайтов, хакерство, DoS-атаки, а также оскорбительное использование, связанное с повреждением компьютерной информации и кражей персональных данных» [2]. Кибертерроризм М. Конвей определяет как «умышленную атаку, направленную на насилие или причинение серьезного экономического ущерба» [2].

Закон «Об управлении информационной безопасностью» (Federal Information Security Management Act, FISMA), принятый Конгрессом США в 2002 году [3], является фундаментальным нормативным актом, направленным на обеспечение кибербезопасности в федеральных агентствах и организациях, обрабатывающих государственные данные. Его основная цель заключается в защите информационных систем и ресурсов от киберугроз, несанкционированного доступа и утечек конфиденциальной информации. FISMA определяет информационную безопасность как многоуровневую систему превентивных и реактивных мер, направленных на защиту информационных ресурсов и информационных систем от несанкционированного доступа, неправомерного использования, несанкционированного раскрытия, модификации или уничтожения [3]. В рамках данной парадигмы особое внимание уделяется обеспечению целостности, аутентичности и конфиденциальности данных, включая как личные, так и имущественные сведения. Для достижения поставленных целей FISMA предписывает разработку и внедрение комплексных программ управления рисками,

направленных на идентификацию уязвимостей, оценку потенциальных угроз и минимизацию их воздействия. Закон также требует создания и регулярного обновления планов обеспечения информационной безопасности, проведения всесторонней оценки эффективности реализуемых мер защиты, тестирования на проникновение, аудитов и мониторинга инцидентов информационной безопасности. Особое внимание уделяется вопросам повышения осведомленности сотрудников о потенциальных киберугрозах и формированию культуры безопасности в организации.

FISMA устанавливает четкую систему ответственности и подотчетности за обеспечение информационной безопасности, предусматривая распределение обязанностей между участниками процесса и создание механизмов отчетности на всех уровнях. Для практической реализации положений закона используются стандарты и руководства, разработанные и опубликованные Национальным институтом стандартов и технологий (NIST). Эти документы содержат детальные рекомендации по управлению информационной безопасностью, оценке рисков и защите данных [4]. Также NIST разрабатывает минимальные требования безопасности и меры контроля, необходимые для соответствия FISMA. В частности, документ NIST SP 800–53 Rev. 5 определяет средства контроля безопасности и конфиденциальности для информационных систем и организаций, необходимые для выполнения требований FISMA [4].

В 2014 году в рамках реализации FISMA была создана система совместного надзора за федеральными программами кибербезопасности, в которой участвуют Административно-бюджетное управление и Агентство кибербезопасности и инфраструктуры Министерства внутренней безопасности. В 2023 году было предложено обновление FISMA, которое предусматривало требования к регулярному информированию обо всех инцидентах, связанных с кибербезопасностью, и выполнению стандартизированных действий в этой области. Однако данное обновление не было принято Конгрессом.

Согласно FISMA, генеральные инспекторы по информационным технологиям (CIO) и другие ответственные лица обязаны проводить ежегодные проверки

программ информационной безопасности своих агентств и информировать об этом Административно-бюджетное управление, которое, в свою очередь, выпускает ежегодный руководящий документ, известный как «Руководство по федеральной информационной безопасности и управлению конфиденциальностью на 2024 финансовый год». В этом документе содержатся требования к отчетности агентств по вопросам кибербезопасности. Также существует дополнительный документ под названием «Показатели ИТ-директоров FISMA на 2024 финансовый год», в котором изложены вопросы, на которые агентства должны отвечать в рамках FISMA [5].

В *Великобритании* уголовное законодательство, регулирующее ответственность за преступления против информационной безопасности, связано с национальными нормативно-правовыми актами. Закон о телекоммуникационной безопасности 2021 года обязывает операторов связи выявлять и предотвращать киберугрозы, а также исполнять предписания государственных органов. ответственность за преступления в сфере информационной безопасности регулируется Законом о связи от 17 июля 2003 года. Статья 404 этого закона предусматривает уголовную ответственность для юридических лиц в случае, если преступление совершено с согласия или попустительства должностных лиц, таких как директор, менеджер, секретарь или иное лицо, действовавшее в таком качестве. В таких случаях ответственность может быть наложена на основании судебного решения [6].

В 2016 году был принят Закон «О следственных полномочиях» (The Investigatory Powers Act»), который ввел дополнительные меры по борьбе с киберпреступностью. Статья 3 этого закона устанавливает уголовную ответственность за перехват сообщений, передаваемых через телекоммуникационные системы, и предусматривает наказание в виде штрафа или лишения свободы на срок до двух лет. Под перехватом понимается доступ к сообщению лицом, не являющимся его отправителем или получателем и не имеющим законных оснований для такого доступа [7].

Законодательство *Франции* в области информационной безопасности акцентирует внимание на защите частной жизни, национальной обороны и критически важных объектов информационной инфраструктуры. Нарушение конфиденциальности частной жизни включает перехват, запись, передачу или фиксацию без согласия человека его конфиденциальных высказываний или изображений в приватном месте, что влечет уголовную ответственность, включая обнародование информации или потворство таким действиям.

Во французском праве используется термин «тайны национальной обороны». В соответствии с частью 1 статьи 413–9 Уголовного кодекса Франции тайны национальной обороны охватывают сведения, технологии, документы и данные, связанные с национальной обороной и подлежащие защите [8]. Отнесение информации к этой категории также регламентируется декретом Государственного совета. Преступления, связанные с нарушением этих тайн, включают изъятие, копирование, уничтожение таких сведений, ознакомление с ними посторонних лиц или передачу их иностранным государствам, организациям или предприятиям, что может нанести ущерб национальным интересам. Уголовная ответственность предусмотрена за попустительство таким действиям и за несанкционированное получение информации.

Французское законодательство также защищает критически важные объекты информационной инфраструктуры. Уголовный кодекс устанавливает ответственность за атаки на автоматизированные системы обработки данных и за контрабанду специального технического оборудования или программного обеспечения, которые могут быть использованы для таких преступлений [8]. Наказания включают штрафы и лишение свободы. Преступления, направленные против критически важных объектов информационной инфраструктуры, характеризуются умышленной формой вины и включают ответственность за нарушение тайны переписки, а также посягательство на личную и семейную жизнь. В рамках французского уголовного права данные преступления рассматриваются как особо тяжкие, которые могут привести к значительным негативным последствиям для общества и государства в целом.

Уголовное законодательство *Федеративной Республики Германии* (ФРГ) детально регулирует вопросы охраны государственной тайны. В Уголовном кодексе ФРГ предусмотрены пять статей, касающихся посягательств на государственную тайну: шпионаж (ст. 94), разглашение государственной тайны (ст. 95), овладение государственной тайной с целью выдачи или разглашения (ст. 96), шпионская агентурная деятельность (ст. 98) и выдача нелегальных тайн (ст. 97a). В последней статье предусмотрена ответственность за разглашение сведений о нарушениях свободного демократического строя или межгосударственных соглашений об ограничении вооружения, которые остаются тайной от партнеров ФРГ [9].

Определение государственной тайны содержится в статье 93 Уголовного кодекса ФРГ, где указано, что это «факты, предметы или сведения, доступные ограниченному кругу лиц и предназначенные для предотвращения опасности причинения тяжкого вреда внешней безопасности Германии».

В 2021 году в Германии был принят Закон о модернизации телекоммуникаций (Telecommunications Modernization Act – TKMG), а также действует Закон О защите данных телекоммуникаций и телемедиа (Telecommunications Telemedia Data Protection Act – TTDSG), регулирующий защиту данных в телекоммуникациях. Однако уголовная ответственность за деяния, аналогичные статье 274 УК РФ (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей), в этой сфере не предусмотрена.

Уголовное законодательство ФРГ охватывает широкий спектр деяний, направленных на обеспечение информационной безопасности. В частности, раздел 15 УК Германии посвящен посягательствам на неприкосновенность частной жизни и частной тайны. Статья 201 кодекса устанавливает ответственность за противоправную запись непубличных разговоров, не предназначенных для третьих лиц, и их последующее воспроизведение, если это противоречит интересам потерпевшего [9].

Статьи 202a и 202b предусматривают ответственность за противоправное получение доступа к особо защищенным данным и перехват данных пользователей с использованием специальных технических средств соответственно. Статья 202d устанавливает наказание за распространение данных, полученных преступным путем и не являющихся общедоступными, с целью личного обогащения или выгоды третьих лиц [9].

Особое внимание в уголовном законодательстве ФРГ уделяется защите права на тайну связи, которая является составляющей права на неприкосновенность частной жизни. В отличие от некоторых других стран, в Германии нарушение тайны переговоров и телефонных разговоров рассматривается как преступление против общественного порядка. В Испании и Эстонии также предусмотрены нормы, направленные на защиту права на тайну сообщений, но они отличаются от немецкого подхода.

Уголовный кодекс *Австрии* также содержит нормы, регулирующие вопросы коммерческой и производственной тайны, а также разглашение государственной тайны. В Австрии понятие государственной тайны определено в статье 255 УК, и под ней понимаются сведения, доступные ограниченному кругу лиц и предназначенные для предотвращения угрозы безопасности государства или его отношений с другими странами [10].

Уголовные кодексы стран бывшего СССР демонстрируют внимание к преступлениям против информационной безопасности. В Казахстане, Азербайджане, Беларуси, Таджикистане, Узбекистане, Кыргызстане, Туркменистане и Молдове были приняты специализированные законы, направленные на борьбу с киберпреступностью. В этих странах киберпреступления рассматриваются как часть более широкой категории преступлений против информационной безопасности.

Анализ уголовных законодательств *стран СНГ* выявляет общие тенденции в криминализации преступлений в сфере компьютерной информации. Одной из ключевых закономерностей является наличие универсального объекта преступлений, что обусловлено влиянием положений Модельного уголовного кодекса

стран СНГ. Это позволяет говорить о наличии единой концептуальной базы для регулирования вопросов кибербезопасности в рамках постсоветского пространства. Так, Уголовный кодекс Республики Беларусь является примером унифицированного подхода к криминализации преступлений в сфере информационной безопасности. Глава 31 кодекса посвящена преступлениям против информационной безопасности, включая такие составы, как несанкционированный доступ к компьютерной информации, разработка, использование или распространение вредоносных программ, нарушение правил эксплуатации компьютерных систем или сетей и другие. Следует отметить, что Уголовный кодекс Беларуси также дифференцирует ответственность за разглашение государственной тайны в зависимости от формы вины [11], что позволяет более точно определять степень общественной опасности деяния и назначать справедливое наказание.

Законодательство других стран ближнего зарубежья содержит интересные положения, направленные на защиту информации. Так, в Уголовном кодексе Республики Узбекистан предусмотрена ответственность за создание, внедрение и эксплуатацию информационных систем, причинивших вред, в том числе государственным интересам [12]. Как видим, узбекский законодатель признает важность защиты информационной инфраструктуры и предотвращения ущерба, который может быть нанесен в результате кибератак. Уголовный кодекс Туркменистана включает главу 33 «Преступления в сфере компьютерной информации», состоящую из статей 333, 334 и 335. Статья 333 устанавливает ответственность за нарушение законодательства о правовой охране алгоритмов, программ для ЭВМ, баз данных и топологий интегральных микросхем [13]. Такой подход ориентирован в основном на защиту интеллектуальной собственности в сфере информационных технологий. Уголовный кодекс Азербайджанской Республики содержит главу 30 «Киберпреступления», включающую статьи 271, 272, 273 и 273–1. Статья 271 предусматривает ответственность за неправомерный доступ к компьютерной системе [14], что позволяет предотвращать несанкционированное вмешательство в работу информационных систем и защищать данные пользователей

Наконец, Уголовный кодекс Республики Казахстан включает главу 7 «Уголовные правонарушения в сфере информатизации и связи», содержащую статьи 205, 206, 207, 208, 209, 210, 211 и 212. Эти статьи направлены на борьбу с неправомерным доступом к информации, уничтожением или модификацией данных, а также с распространением вредоносных программ [15].

Уголовный кодекс Кыргызской Республики, принятый в 2021 году, также включает новую главу, регулирующую ответственность за преступления в сфере кибербезопасности. В статьях 319–322 этой главы рассматриваются различные правонарушения, такие как несанкционированный доступ к компьютерным системам, создание и распространение вредоносного программного продукта, киберсаботаж и массовый спам [16].

Уголовный кодекс Российской Федерации, принятый в 1996 году, также содержит нормы, направленные на борьбу с преступлениями в сфере компьютерной информации. В главе 28 УК РФ (статьи 272–274.2) предусмотрены меры ответственности за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, а также нарушение правил эксплуатации информационных систем. Статья 159.6 УК РФ охватывает мошенничество в сфере компьютерной информации, подчеркивая важность защиты экономических интересов в цифровом пространстве [17]. В уголовных кодексах других стран СНГ такой нормы нет. В условиях роста киберпреступлений, которые используют информационные технологии для мошенничества и обмана с целью кражи денег и имущества граждан, эта норма представляется нам крайне важной. Она поможет лучше защищать экономические интересы людей и компаний в цифровую эпоху.

Таким образом, анализ подходов различных государств показывает, что обеспечение безопасности в информационной сфере является приоритетной задачей для всех стран. Важным является гармонизация национальных законодательств с международными стандартами и нормами, что позволит создать более эффективную систему защиты информации и обеспечить безопасность пользователей в цифровом пространстве.

В завершение обсуждения подведем краткие итоги и сформулируем ряд предложений.

1. Анализ международно-правовых и зарубежных аспектов проблемы противодействия преступлениям в сфере информационной безопасности выявил несколько ключевых тенденций и проблем. Большинство государств, активно участвующих в борьбе с такими преступлениями, имеют сформированную уголовно-правовую базу, основанную на национальном административном законодательстве. Основные криминализованные деяния включают неправомерный доступ к охраняемой информации, воздействие на объекты критической информационной инфраструктуры и нарушения в сети.

2. Проблемы уголовной ответственности за преступления против информационной безопасности в основном связаны с раскрытием и расследованием, особенно с идентификацией лиц, совершивших преступления, из-за трудностей с определением их IP-адресов. В связи с этим предлагается консолидация усилий на уровне ООН для принятия международной Всеобъемлющей конвенции по международной информационной безопасности.

3. Регионализация международных актов в этой области может привести к тому, что злоумышленники будут действовать из стран, не подписавших такие соглашения, против целей в странах-участницах. Сравнительно-правовое исследование зарубежного уголовного законодательства указывает на перспективность решения вопросов ответственности за запись непубличных разговоров и их последующую передачу третьим лицам, особенно если это привело к тяжким последствиям. Также важно установить ответственность за распространение сведений, полученных преступным путем, и за использование мошенничества как способа доступа к охраняемой информации через обман и злоупотребление доверием.

***Список литературы***

1. Walter Laqueur. The New Terrorism: Fanaticism and the Arms of Mass Destruction. Oxford: Oxford University Press, 1999. – 312 p.

2. Cyberterrorism: Hype and Reality Maura Conway Dublin City University. 2007 [Электронный ресурс]. – Режим доступа: https://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf (дата обращения: 12.04.2025).

3. Federal Information Security Modernization Act (FISMA) [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzZoZ (дата обращения: 14.04.2025).

4. NIST SP 800–53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата обращения: 14.04.2025).

5. Fiscal Year 2024 Senior Agency Official for Privacy Federal Information Security Modernization Act of 2014 Reporting Metrics v1.0, August, 2024 [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzZpH (дата обращения: 12.04.2025).

6. Закон о связи Великобритании от 17 июля 2003 года [Электронный ресурс]. – Режим доступа: https://www.legislation.gov.uk/ukpga/2003/21/section/404 (дата обращения: 10.04.2025).

7. Закон о следственных полномочиях Великобритании от 29 ноября 2016 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzZpu (дата обращения: 10.04.2025).

8. Уголовный кодекс Французской Республики [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzZqW (дата обращения: 16.04.2025).

9. Уголовное уложение Федеративной Республики Германия (Strafgesetzbuch (StGB) [Электронный ресурс]. – Режим доступа: https://www.uni-potsdam.de/fileadmin/projects/lshellmann/ (дата обращения: 16.04.2025).

10. Уголовный кодекс Австрии / пер. с нем. А.В. Серебренниковой. – М.: ИКД «Зерцало М», 2001.

11. Уголовный кодекс Республики Беларусь от 9 июля 1999 года №275-З // Национальный реестр правовых актов Республики Беларусь. 1999. №76, 2/50.

12. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года №2012-XII (в ред. от 21 февраля 2024 года) [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=30421110 (дата обращения: 20.04.2025).

13. Уголовный кодекс Туркменистана от 12 июня 1997 года №222-I (в ред. от 12 апреля 2025 года) [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=31295286 (дата обращения: 23.04.2025).

14. Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 года №787-IQ (В ред. от 27 декабря 2024 года) [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=30420353 (дата обращения: 20.04.2025).

15. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V ЗРК [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 23.04.2025).

16. Уголовный кодекс Кыргызской Республики от 28 октября 2021 года №127 // Эркин-Тоо. 2021. 16 ноября.

17. Уголовный кодекс Российской Федерации от 13 июня 1996 года №63-ФЗ (В ред. 21 апреля 2025 года №102-ФЗ) [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzZsy (дата обращения: 22.04.2025).

---

**Салишев Сергей Николаевич –** аспирант Отдела аспиратуры и докторантуры, Кыргызский национальный университет им. Жусупа Баласагына, Бишкек, Республика Кыргызстан.

**Сеюбергенова Дидар Сламовна –** докторант PhD / по юриспруденции, Международный университет Кыргызстана, Бишкек, Республика Кыргызстан.

**Исманов Таалайбек Кадырович –** руководитель направления докторанты PhD / по юриспруденции, Международный университет Кыргызстана, Бишкек, Республика Кыргызстан.

---