Салишев Сергей Николаевич
аспирант
Кыргызский национальный университет им. Жусупа Баласагына
г. Бишкек, Республика Кыргызстан
Сеюбергенова Дидар Сламовна
докторант
Международный университет Кыргызстана
г. Бишкек, Республика Кыргызстан
Алияскарова Милана Урматбековна
аспирант
Кыргызско-Российский Славянский университет имени Б.Н. Ельцина
г. Бишкек, Республика Кыргызстан

ТЕОРЕТИКО-ПРАВОВЫЕ КОНЦЕПЦИИ И ПОДХОДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *настоящее исследование посвящено комплексному анализу концепций и подходов в сфере управления информационной безопасностью и регулирования информационных правоотношений в постиндустриальном обществе. В рамках статьи осуществляется детальное изучение методологических стратегий в исследовании информационной безопасности. Рассматриваются различные научные подходы, включая социологический, социально-психологический, социокультурный, гуманитарный и технологический. Особое внимание уделяется критическому осмыслению теоретических основ и практических аспектов информационной безопасности, а также их корреляции с современными вызовами и тенденциями в данной области. Исследование предполагает интеграцию междисциплинарного подхода, что позволяет всесторонне оценить эффективность существующих механизмов защиты информации в условиях глобального процесса информатизации и выявить перспективы их дальнейшего совершенствования. Подчеркивается, что информационная безопасность – это не только техническая, но и социальная, политическая и правовая проблема.*

Делается вывод о необходимости комплексного подхода и междисциплинарных исследований для разработки эффективных стратегий обеспечения информационной безопасности.

Ключевые слова: *постиндустриальное общество, информационные технологии, информационное общество, информационная безопасность, телекоммуникационные технологии, информационные ресурсы, информационная культура, информатизация, кибербезопасность, информационная инфраструктура.*

Информация является фундаментальным элементом общественной жизни, пронизывая все социальные процессы и оказывая значительное влияние на поведение индивидов. С углублением и усложнением общественных отношений возрастает значение информационных правоотношений, что в свою очередь приводит к увеличению количества нормативных актов, регулирующих данную сферу. Управление информационной безопасностью приобретает особую актуальность, поскольку оно направлено на минимизацию рисков, связанных с утечкой, искажением или несанкционированным доступом к информации. В современном мире, где информации становится все больше, а ее значение для общества возрастает в геометрической прогрессии, защита данных выходит на первый план. Технологии и методы должны быть передовыми, особенно учитывая, как быстро развиваются новые виды информационных технологий и автоматизированные системы. А это требует создания новых комплексных мер по защите информации на всех этапах ее жизненного цикла.

Данное исследование направлено на анализ концепций и философских подходов в области управления информационной безопасностью и регулирования информационных правоотношений, в нем рассматриваются технологические решения и методологические стратегии защиты информации.

Информационная безопасность представляется в науке как защита информации от целенаправленных или случайных воздействий, которые могут быть естественными или искусственными и способны нанести значительный ущерб всем участникам информационных отношений, включая владельцев и

пользователей информации [1, с. 108]. В философской традиции информация рассматривается через призму категорий «отражение» и «разнообразие» [2, с. 36]. Категория отражения позволяет выявить сущностные свойства объектов познания, в то время как разнообразие служит инструментом для дифференциации этих свойств между различными объектами. Таким образом, информация представляется как структурированное разнообразие, проявляющееся в процессе отражения [2, с. 36]. А. Д. Урсул, выдающийся представитель современной философии, утверждает, что информация является универсальной характеристикой всех материальных систем, пронизывая все уровни мироздания и выступая как фундаментальное отражение многообразия [3, с. 27]. В свою очередь В.Г. Афанасьев трактует информацию как результат отражения многообразной действительности в форме сообщений и сведений, что подчеркивает ее эпистемологическую и коммуникативную природу [4, с. 12].

Современные подходы к понятию информации подчеркивают его взаимосвязь с теорией познания. Так, М.А. Петров определяет информацию как систему логически организованных высказываний и предложений, выраженных в языке и функционирующих в социальных системах и тем самым акцентирует внимание на социальной природе информации, ее зависимости от языковой и коммуникативной деятельности человека, а также ее роли в формировании и трансляции знаний в обществе [5].

С кибернетической точки зрения информация рассматривается как объективная субстанция, тесно связанная с содержанием, поступающим из окружающего мира. Н. Винер, один из основателей кибернетики, утверждал, что информация не является энергией или материей в традиционном смысле, а представляет собой содержание, способствующее адаптации систем к внешней среде [6, с. 201]. В.М. Глушков, выдающийся советский ученый, предложил более комплексное определение, рассматривая информацию как меру неоднородности материи и энергии, а также как количественную характеристику изменений, сопровождающих все природные процессы [7, с. 45].

Несмотря на разность подходов, все исследователи сходятся в одном: информация как атрибут объективного мира является ключевым фактором устойчивости и развития систем, обеспечивая функционирование и взаимодействие в обществе. Для защиты от угроз информационной безопасности необходимы правовые нормы, включая законодательные акты, которые оперируют понятиями «конфиденциальная информация», «персональные данные» и «тайна». Однако до сих пор не существует единого подхода к пониманию института персональных данных в правовой доктрине и законодательстве. В правовой доктрине конфиденциальная информация рассматривается как родовое понятие для всех видов тайн [8, с. 9]. Е.А. Палехова определяет конфиденциальность как требование не допускать распространения информации без согласия ее обладателя [9, с. 40], а М.В. Бундин – как информацию ограниченного доступа, которая не должна передаваться третьим лицам [10, с. 11]. Таким образом, в российской правовой доктрине конфиденциальность представляет собой качественную характеристику информации, к которой установлен специальный правовой режим, ограничивающий ее свободный обмен на основании федерального законодательства.

Постиндустриальное общество и информационные технологии: социально-философский взгляд. В современном индустриальном обществе ключевую роль играют машинные технологии, тогда как постиндустриальная парадигма характеризуется доминированием информационно-интеллектуальных технологий. Специфика постиндустриального социума заключается в акценте на процессах обмена информацией, осуществляемых посредством информационных и телекоммуникационных систем.

Концепция постиндустриального общества была впервые сформулирована американским социологом Дэниэлом Беллом, который заложил ее методологические основы. Впоследствии значительный вклад в развитие данной теории внесли такие выдающиеся исследователи, как Элвин Тоффлер, Герман Кан, Уильям Дайзард, Ален Турен, Теодор Стоуньер и Йошиа Масуда. Й. Масуда дал исчерпывающую характеристику нового типа общества, основанного на информационных ценностях [11]. Мануэль Кастельс определяет эту эпоху как

«информациональную», подчеркивая ее глубокое влияние на мировую культуру, социальную структуру и экономику [12, с. 25].

Исследователи сходятся во мнении, что современный этап развития цивилизации характеризуется значительными изменениями в общественной жизни, технологическом укладе и культурной парадигме. Они также отмечают тенденцию к постоянному росту технического потенциала, оказывающего существенное воздействие на социальные процессы. В своей работе «Социальные рамки информационного общества» Д. Белл конкретизировал эту концепцию, подчеркнув решающую роль телекоммуникационных технологий в повседневной жизни человека [13, с. 330].

Теоретики постиндустриализма рассматривают информацию и знания как стратегические ресурсы и ключевые факторы трансформации общества. Так, английский ученый Теодор Стоуньер в своем фундаментальном труде «Информационное богатство: профиль постиндустриальной экономики» проводит глубокий анализ и сравнительный анализ информации с традиционными природными ресурсами, такими как полезные ископаемые. Он утверждает, что в современном постиндустриальном мире информация стала важнейшим стратегическим ресурсом и ее значение можно сравнить с ролью сырья в эпоху индустриализации. Т. Стоуньер подчеркивает, что в современном мире доступ к качественной информации становится ключевым фактором в геополитической борьбе между странами. В условиях глобализации и стремительной цифровизации экономики государства, владеющие большими объемами данных и передовыми технологиями их обработки, получают значительное преимущество. Это преимущество проявляется в различных сферах, включая научные исследования, инновационные разработки, образовательные системы и управленческие практики [14, с. 393].

Элвин Тоффлер в труде «Третья волна» обращает внимание на ведущую роль новых информационных технологий в развитии информационного общества, которое, по его мнению, откроет неограниченные возможности и интенсифицирует процессы информационного обмена [15].

Уильям Дайзард в своем исследовании представил сценарный анализ процесса перехода общества в информационное состояние и обозначил потенциальные риски, связанные с обеспечением информационной безопасности [16, с. 345]. Он указал на угрозы вторжения в личную и общественную жизнь через базы данных, содержащие конфиденциальную информацию о здоровье, профессиональной деятельности и финансовых операциях. У. Дайзард подчеркивает необходимость внедрения согласованных подходов и методов контроля на государственном уровне для минимизации этих рисков [16, с. 345].

Йошиа Масуда акцентировал внимание на возможности использования информационных технологий для влияния на духовно-моральные ценности индивидов и социальных групп. Он предложил комплекс мер по защите граждан, включая развитие демократических институтов и предотвращение преступных действий в виртуальной среде [11].

Среди российских исследователей И.С. Мелюхин провел всесторонний анализ информационного общества, подчеркнув необходимость разработки государственной концепции для гармоничного интеграции в мировое информационное пространство, отмечая при этом важность создания института «электронного правительства» как ключевого элемента на пути к информатизации [17, с. 156]. И.С. Мелюхин подчеркнул важность ключевой роли социальной преемственности и государственного регулирования в процессе интеграции и эффективного использования информационных технологий, подчеркивая при этом, что без системной координации и согласованности на всех уровнях управления невозможно раскрыть весь потенциал этих технологий и достичь значимых результатов в различных сферах общественной жизни [17, с. 197].

Таким образом, развитие информационного общества требует комплексного подхода к обеспечению информационной безопасности и разработки государственной политики, направленной на безопасное внедрение информационных технологий.

Подходы к исследованию информационной безопасности в современном обществе. Модель сетевого общества, разработанная Мануэлем Кастельсом,

является продуктом информационно-технологической революции и отличается доминированием глобальных и сетевых структур в социальных процессах [18]. Ядром этого общества является не просто информация, а ее применение и направление. В рамках этой парадигмы возникают сети, такие как Интернет, которые объединяют людей, гражданские институты, государственные органы и организации. М. Кастельс подчеркивает, что компьютерные технологии оказывают значительное влияние на властные отношения и культурные трансформации в обществе [18, с. 39]. Анализ подходов зарубежных исследователей к формированию информационного общества и вопросам информационной безопасности в контексте информационно-коммуникативных технологий показывает, что ранние концепции, представленные Дэниелом Беллом и Теодором Стоуньером, были оптимистичны в отношении технократической власти и прогресса в науке и технике. Д. Белл в своей концепции постиндустриального общества выделял знания и информацию как ключевые факторы экономического и социального прогресса, а Т. Стоуньер в свою очередь подчеркивал, что информация становится новым видом богатства, способным трансформировать структуру экономики и общества [14, с. 392–409; 19]. Однако более поздние теории М. Кастельса и Т. Росзака, охватывали более широкий спектр проблем, связанных с развитием информационного общества. Так, М. Кастельс уделял особое внимание сетевым структурам и их влиянию на социальные, экономические и политические процессы. Он подчеркивал ведущую роль сетевых взаимодействий в формировании новых форм общественного устройства и управления [18], в то время как Т. Росзак, напротив, рассматривал информационные технологии не только как средство улучшения жизни, но и как источник новых вызовов, поэтому на первый план выдвигал вопросы конфиденциальности, манипуляции информацией и их влияние на психическое здоровье. Т. Росзак также считал важным развитие новых форм культуры и образования, способных адаптироваться к стремительно меняющемуся информационному миру [21].

Таким образом, современный этап информационного развития характеризуется возрастающей ролью информации и знаний как ведущих факторов

общественного прогресса, а также значимостью технологических достижений в сфере информационных технологий и телекоммуникаций. Эти факторы оказывают существенное влияние на социально-экономические и политические трансформации.

Сложности формирования единого определения информационной безопасности. Информационная безопасность представляет собой комплексное и многогранное явление, которое трудно формализовать из-за объективного и динамичного характера информатизации. Чаще всего информационная безопасность рассматривается с позиций права, психологии, социологии и технического обеспечения, что порождает многообразие подходов и усложняет формирование единого определения.

Социологический подход к информационной безопасности акцентирует внимание на информационном противоборстве, проявляющемся в масс-медиа и электронных средствах массовой информации, и оценивает его последствия через общественное мнение. Социально-психологический подход, разработанный Е.П. Белинской, Ю.Д. Бабаевой и другими, анализирует эффективность информационного воздействия на индивида, учитывая установки и уровень доверия к информации в обществе [22; 23]. А.Е. Войскунский в свою очередь рассматривает кибербезопасность как важный аспект информационной безопасности [24, с. 49].

Социокультурный подход, предложенный Э.К. Наберушкиной, интерпретирует информационную культуру как неотъемлемую часть общечеловеческой культуры и акцентирует внимание на сохранении социальных ценностей и противодействии их подмене [25]. Данный подход подчеркивает значимость безопасного развития личности в информационном обществе и необходимость защиты от деструктивного информационного воздействия.

Особое внимание уделяется их отношению к вопросам кибербезопасности и влиянию социальных сетей на распространение информации. Психологическая составляющая рассматривает когнитивные процессы, решения в условиях угроз и эмоциональное восприятие рисков. Правовые аспекты касаются

законодательных норм, регулирующих защиту данных, и международных соглашений по кибербезопасности. Педагогическое направление направлено на обучение и повышение осведомленности о рисках и способах защиты информации. Технические аспекты включают разработку и внедрение технологий для обеспечения безопасности. Экономические исследования анализируют влияние кибербезопасности на бизнес и экономику.

Многие научные работы не стремятся к четкому определению понятий, что ограничивает их вклад в систематизацию знаний. Отсутствие единого мнения о термине «информационная безопасность» мешает интеграции различных методологических подходов и концепций, что затрудняет создание общетеоретической базы и приводит к фрагментации знаний. Разночтения в понимании термина «информационная безопасность» осложняют взаимодействие специалистов, снижая эффективность их совместных усилий.

Для более глубокого понимания феномена информационной безопасности предлагается междисциплинарный подход, который интегрирует достижения различных научных областей и выходит за рамки узкодисциплинарных методологий. Это особенно важно в условиях глобального процесса информатизации и формирования информационного общества.

Подходы, применяемые в междисциплинарных направлениях. Информационная безопасность представляет собой междисциплинарную область, требующую комплексного и системного подхода к исследованию. Существующие научные труды в данной сфере преимущественно фокусируются на технологических и организационных аспектах, освещая вопросы систематизации и структурирования мер по обеспечению безопасности на национальном и корпоративном уровнях [19].

Гуманитарный подход к информационной безопасности акцентирует внимание на необходимости духовной трансформации общества, соблюдении прав и свобод граждан в информационном пространстве, а также на разработке методологических основ и правовой регламентации [24, с. 50; 26]. Этот подход также направлен на выявление значимости информационной безопасности в контексте

современных общественных процессов и обеспечение безопасности сознания на различных уровнях.

В российском обществе сформировался нормативно-правовой подход к информационной безопасности, закрепленный в Законе Российской Федерации от 28 декабря 2010 года №390-ФЗ «О безопасности» [27] и Доктрине информационной безопасности Российской Федерации от 5 декабря 2016 года №646 [28]. Эти документы определяют информационную безопасность как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, включая угрозы международного характера.

Исследователи, придерживающиеся технологического подхода, акцентируют внимание на защите информации и информационной инфраструктуры от естественных и искусственных угроз [29, с. 6; 30, с. 15]. Информационная инфраструктура включает организационные структуры, технические средства, аппаратное и программное обеспечение, обеспечивающее сбор, хранение, передачу и использование информации. Устойчивая работа этой инфраструктуры является ключевым фактором для реализации конституционных прав граждан, экономической деятельности, государственного управления и социального обеспечения.

Информационная коммуникация осуществляется через информационную инфраструктуру, и ее нарушение может привести к дестабилизации общественных институтов. Технологический подход подчеркивает необходимость защиты информации как продукта информационных технологий, что требует применения правовых, организационных и технических мер. Защита информации включает предотвращение утечки, несанкционированного доступа и воздействия на информацию, а также ликвидацию последствий информационных угроз и хакерских атак. Защита от утечки информации направлена на предотвращение несанкционированного распространения конфиденциальных данных, а защита от несанкционированного доступа – на исключение доступа к информации без соответствующих прав. Для этого используются организационные, технические и программные средства, включая криптографические методы.

Защита от несанкционированного воздействия направлена на предотвращение искажения, уничтожения, блокирования или утраты информации, а защита от непреднамеренного воздействия – на минимизацию рисков, связанных с ошибками пользователей или сбоями в работе программно-аппаратных средств.

Анализ научной литературы показывает, что технологический аспект информационной безопасности более разработан по сравнению с гуманитарным. Оптимальным определением информационной безопасности является подход, предложенный М. В. Арсентьевым, который рассматривает ее как ситуацию снятия информационной неопределенности относительно потенциальных и реальных угроз, а также наличия возможностей и средств для их отражения [31, с. 49].

Информационная безопасность должна рассматриваться как комплексное явление, соответствующее тенденциям развития информационного общества. Для обеспечения безопасной информационной среды необходимо анализировать применение информационных технологий, выявлять опасные тенденции и их последствия, а также устранять причины их возникновения.

Таким образом, постиндустриальное общество отличается от индустриального тем, что в нем доминируют информационно-интеллектуальные технологии. В индустриальном обществе ключевую роль играют машинные технологии, которые определяют характер производства и образ жизни людей. В постиндустриальном обществе информация и знания становятся стратегическими ресурсами и ключевыми факторами трансформации общества. Они влияют на все сферы жизни, включая экономику, культуру и социальные отношения.

Информационная безопасность – это комплексное и многогранное явление, которое требует междисциплинарного подхода к исследованию, поскольку играет ключевую роль в формировании национальной безопасности на государственном уровне. Это связано с тем, что информация и информационные системы становятся все более важными для функционирования государственных институтов, экономики и общества в целом.

Существующие научные труды в сфере информационной безопасности преимущественно фокусируются на технологических и организационных аспектах,

рассматривая вопросы защиты информации в компьютерных системах, сетях и других информационных инфраструктурах. Однако информационная безопасность – это не только техническая проблема, но и социальная, политическая и правовая.

В российском обществе сформировался нормативно-правовой подход к информационной безопасности, закрепленный в соответствующих федеральных законах и доктринах. Этот подход предполагает разработку и реализацию комплекса мер, направленных на защиту информации и информационных систем от различных угроз. Технологический подход подчеркивает необходимость защиты информации как продукта информационных технологий, что требует применения правовых, организационных и технических мер.

Таким образом, информационная безопасность является важной составляющей национальной безопасности и требует комплексного подхода, включающего технические, организационные, правовые и гуманитарные аспекты, что лишний раз подчеркивает необходимость междисциплинарных исследований и сотрудничества между специалистами разных областей для разработки эффективных стратегий и мер по обеспечению информационной безопасности.

Список литературы

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: Форум, 2018. – 256 с.

2. Украинцев Б.С. Информация и отражение / Б.С. Украинцев // Вопросы философии. – 1963. – №2. – С. 26–38.

3. Урсул А.Д. Информация и глобальные процессы: междисциплинарные исследования / А.Д. Урсул // Знание. Понимание. Умение. – 2013. – №3. – С. 26–33. EDN RBOVID

4. Афанасьев В.Г. Социальная информация: монография / В.Г. Афанасьев. – М.: Наука, 1994. – 199 с.

5. Петров М.А. Информационно-знаниевая сущность познавательного процесса / М.А. Петров // Вестник Иркутского государственного университета. –

2010. – №26 (2). – URL: https://nbisu.moy.su/_ld/8/887_...?ysclid=mbet1eltns280815125 (дата обращения: 20.05.2025).

6. Винер Н. Кибернетика, или Управление и связь в животном и машине / Н. Виннер; пер. с англ.; предисл. Г.Н. Поварова. – 2-е изд. – М.: Советское радио, 1968. – 326 с.

7. Глушков В.М. Алгебра. Языки. Программирование / В.М. Глушков, Г.Е. Цейтлин, Е.Л. Ющенко; АН УССР, Ин-т кибернетики им. В.М. Глушкова. – 3-е изд., перераб., доп. – Киев: Наукова думка, 1989. – 376 с.

8. Туманова Л.В. Обеспечение и защита права на информацию / Л.В. Туманова, А.А. Снытников. – М.: Городец-издат, 2001. – 339 с.

9. Палехова Е.И. Конфиденциальная информация и институт персональных данных в банковской деятельности / Е.И. Палехова // Предпринимательское право. – 2010. – №3. – С. 40–46. EDN MWGFVD

10. Бундин М.В. Персональные данные как информация ограниченного доступа / М.В. Бундин // Информационное право. – 2009. – №1. – С. 10–14. EDN KDMPQN

11. Masuda Y. The Information Society as Postindustrial Society. Wash.: World Future Soc., 1983. 299 p.

12. Кастельс М. Власть коммуникации / М. Кастельс, пер. с англ. Н.М. Тылевич; под науч. ред. А.И. Черных. – М.: Изд. дом Высшей школы экономики, 2016. – 564 с.

13. Белл Д. Социальные рамки информационного общества / Д. Белл // Новая технократическая волна на Западе. – М.: Прогресс, 1986. – С. 330–342.

14. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики / Т. Стоуньер // Новая технократическая волна на Западе / Под ред. П.С. Гуревича. – М.: Прогресс, 1986. – С. 392–409.

15. Тоффлер Э. Третья волна / Э. Тофлер. – М.: АСТ, 2004. – 345 с.

16. Дайзард У. Наступление информационного века / У. Дайзард // Новая технократическая волна на Западе / под ред. П.С. Гуревича. – М.: Прогресс, 1986. – С. 343–355.

17. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития / И.С. Мелюхин. – М.: Изд-во Моск. ун-та, 1999. – 206 с.

18. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – М.: ГУ ВШЭ, 2000. – 606 с.

19. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Д. Белл; пер. с англ. – 2-е изд., испр. и доп. – М.: Academia, 2004, CLXX. – 788 с. EDN QOCVVP

20. Стоуньер, Т. Информационное богатство: профиль постиндустриальной экономики / Т. Стоуньер // Новая технократическая волна на Западе / под ред. П.С. Гуревича. – М.: Прогресс, 1986. – С. 392–409.

21. Roszak T. The Cult of Information. The Folklore of computers and the True Art of Thinking. New York: Pantheon Books, Cop. 1986. XII, 238 p.

22. Белинская Е.П. Информационная социализация в поликультурном пространстве / Е.П. Белинская // Известия Саратовского университета. Новая серия. Серия Философия. Психология. Педагогика. – 2015. – Т. 3. №30. – С. 253–259.

23. Бабаева Ю.Д. Психологические последствия информатизации / Ю.Д. Бабаева, А.Е. Войскунский // Психологический журнал. – 1998. – Т. 19. №1. – С. 89–100

24. Войскунский А.Е. Информационная безопасность: психологические аспекты / А.Е. Войскунский // Национальный психологический журнал. – 2010. – Т. 1. №3. – С. 48–53. EDN NXUUVR

25. Наберушкина Э.К. Социокультурные аспекты информационной безопасности в сетевом обществе / Э.К. Наберушкина, Е.А. Бердник // Научные ведомости. Серия Философия. Социология. Право. – 2016. – №17 (238). – Вып. 37. – С. 90–98. EDN WZRGPT

26. Скворцов Л.В. Информационная культура и цельное знание / Л. В. Скворцов. – М.: Изд-во МБА, 2011. – 440 с. EDN QONAHJ

27. Закон Российской Федерации «О безопасности» от 28 декабря 2010 года №390-ФЗ. – URL: http://base.garant.ru/10136200/ (дата обращения: 20.05.2025).

28. Доктрина информационной безопасности Российской Федерации Утверждена Указом Президента Российской Федерации от 5 декабря 2016 года №646. – URL: https://www.mid.ru/ru/foreign_policy/official_documents/1539546/ (дата обращения: 20.05.2025).

29. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, С.Н. Погожин. – М.: Горячая линия-Телеком, 2001. – 144 с.

30. Галатенко В.А. Основы информационной безопасности. Курс лекций: учебное пособие / В.А. Галатенко; под ред. В.Б. Бетелина. – М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2006. – 208 с.

31. Арсентьев М.В. К вопросу о понятии «информационная безопасность» / М.В. Арсентьев // Информационное общество. – 1997. – №4–6. – С. 48–50.