Доверие и безопасность в информационном обществе

ИНФОРМАЦИОННАЯ САФИТОЛОГИЯ – НАУКА ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Колин Константин Константинович

Доктор технических наук, профессор, заслуженный деятель науки РФ
Федеральный исследовательский центр «Информатика и Управление» РАН, главный научный сотрудник
Научно-аналитический журнал «Информационное общество», член редакционного совета
Москва, Российская Федерация
kolinkk@mail.ru

Аннотация

Излагаются концептуальные основы формирования науки об информационной безопасности, которую предлагается назвать Информационной сафитологией. Показана актуальность и стратегическая важность этого направления научных исследований для обеспечения информационной безопасности человека, общества и биосферы в целом в условиях информационной революции XXI века. Рассмотрена структура предметной области этой науки, ее основные задачи, методы и перспективы развития. Показан научно-методологический потенциал России, который должен быть использован для решения этой комплексной проблемы. Определены приоритетные задачи исследований на ближайший период времени для определения мер адекватного противодействия внешним и внутренним информационным угрозам и формирования в обществе императива информационной безопасности.

Ключевые слова (используйте стиль «Ключевые слова»)

информационная безопасность, информационные вызовы и угрозы, императив безопасности, национальная безопасность

Введение

Научные исследования показывают, что доминирующей тенденцией развития мировой цивилизации в веке является глобальная и все более глубокая информатизация. Новые средства информатики и информационных технологий все более широко используются практически во всех сферах жизнедеятельности общества и уже стали атрибутами нашей культуры. Их использование радикальным образом изменяет организацию общественного производства, способы общения между людьми, а также их традиционные представления о качестве жизни, пространстве и времени. Информационная сфера становится новой средой обитания человека, в которой он проводит значительную часть времени [1].

Интенсивность информационных процессов в окружении человека многократно возросла, и это оказывает существенное влияние на самого человека, его психику, социальное поведение и физиологические процессы организма. Исследования показывают, что эти изменения далеко не всегда являются позитивными. Многие из них опасны, так как представляют угрозу для здоровья и жизнедеятельности людей, других живых организмов, включая бактерии и вирусы, а также для биосферы в целом.

Кроме того, благодаря развитию методов наблюдения за экономическим и социальными процессами, появились новые возможности манипулятивного воздействия на сознание и подсознание людей. Эти возможности уже широко используются для геополитической, экономической и корпоративной конкуренции, а также с террористическими и криминальными целями [2]. Именно поэтому одной из важных проблем современности становится обеспечение

https://doi.org/10.52605/16059921_2026_03_123

информационной безопасности человека, общества и государства. С этой целью во многих странах приняты и осуществляются национальные программы информационной безопасности [3].

Однако, этого недостаточно, так как проблема является многоаспектной и комплексной, и многие возможные последствия ее дальнейшего развития еще недостаточно изучены. Нам представляется, что для комплексного изучения этой актуальной и стратегически важной проблемы необходима наука об информационной безопасности, которую предлагается назвать *Информационной сафитологией*.

В настоящее время эта наука еще не сформирована, хотя изучение различных аспектов проблемы информационной безопасности ведется во многих странах, включая Россию, уже достаточно продолжительное время.

Целью настоящей работы является обоснование актуальности этого комплексного научного направления, а также определение его места в структуре современной науки, содержания предметной области и задач для научных исследований на ближайший период времени в интересах обеспечения национальной безопасности нашей страны.

1 Место информационной сафитологии в перспективной структуре научного познания

В России начало формироваться новое комплексное научное направление, в рамках которого должны системно изучаться проблемы безопасности. В работе [3] этому направлению дано название *Сафитология* (от англ. safety - безопасность). При этом содержание термина *безопасность* рассматривается в широком плане, с учетом нарастания комплекса угроз для безопасности в различных сферах - природной, социальной и гуманитарной.

Отличительной особенностью предлагаемой концепции изучения проблем безопасности является учет двойственности смыслового содержания термина « *безопасность*» в русском языке. Исследования показали, что при изучении проблем безопасности необходимо помнить, что термин «*безопасность*» в русском языке имеет два основных значения. Первое из них обозначает *отсутствие какой-либо опасности* для некоторого объекта, процесса или явления со стороны внешних или внутренних источников или же его *состояние защищенности* от их негативного воздействия. В этом смысле мы употребляем такие словосочетания как *личная безопасность*, *общественная безопасность, национальная безопасность* и т. п.

Второе значение термина «*безопасность*» используется для обозначения свойства самих объектов, процессов или явлений *не причинять вреда или ущерба* другим объектам или процессам в результате своей деятельности. Характерными примерами здесь могут служить такие понятия как *безопасный транспорт*, *безопасная пища*, *безопасная бритва*.

Понимание и учет этой двойственности является очень важным при определении источников и причин опасностей или угроз. Так, например, источником опасности может быть человек, который нарушает законы природы и общества, а также некоторые социальные структуры, например, преступные сообщества или же террористические организации.

Источником опасности может быть и государство, если оно проводит агрессивную внешнюю или репрессивную внутреннюю политику.

Отметим, что определение некоторых важных терминов в области безопасности приведено в ряде директивных документов нашей страны по этой проблематике. Однако, во всех этих документах основное внимание уделяется, главным образом, проблематике *обеспечения защищенности* объектов безопасности от внешних угроз. А этого явно недостаточно, так как проблема безопасности является многоаспектной, и поэтому для получения целостных знаний нужно учитывать все аспекты этой проблемы.

Все изложенное выше в полной мере относится и к проблеме информационной безопасности, которая является важной составной частью более общей проблемы - проблемы безопасности.

Поэтому *информационную сафитологию,* изучающую проблематику информационной безопасности, необходимо рассматривать как составную часть науки о безопасности – *сафитологии*.

2 Определение содержания термина «информационная безопасность»

При проведении исследований проблемы информационной безопасности мы предлагает использовать следующие два определения содержания этого термина:

1. ***Информационная безопасность*** – это такое *состояние* некоторого компонента реальности (субъекта, объекта, системы или процесса в природе и обществе), при котором он не испытывает внешних или внутренних деструктивных информационных воздействий, способных нарушить процессы его существования или функционирования.
2. ***Информационная безопасность*** – это *свойство* некоторого компонента реальности (субъекта, объекта, системы или процесса в природе и обществе) не оказывать деструктивных информационных воздействий на другие компоненты реальности в процессе его существования или функционирования.

3 Комплексный характер проблемы информационной безопасности

Исследования показали, что проблема информационной безопасности является многоаспектной. Она включает в себя большое количество разнообразных факторов технологического, социально-экономического, психологического, информационного, биологического и гуманитарного характера. Поэтому для глубокого системного изучения этой проблемы необходимо обеспечить проведение междисциплинарных исследований с привлечением специалистов во многих областях современной науки.

В работе [3] показана целесообразность различать следующие уровни объектов реальности при изучении проблемы безопасности:

- дальний и ближний космос,
- планета Земля,
- неживая природа,
- биосфера планеты,
- человеческое общество,
- национальные государства и их объединения,
- корпоративные организационные структуры общества,
- семья,
- человек.

В качестве критерия для определения уровней этой структуры было принято проявление угроз для безопасности, которые сегодня наблюдаются для объектов или процессов, находящихся на различных уровнях структуры современного мира как сложной иерархической системы. Поскольку деятельность современной цивилизации проявляется на всех этих уровнях, то и проблематику изучения информационной безопасности следует ориентировать соответственно этим уровням.

При этом необходимо обязательно рассматривать оба аспекта проблемы безопасности, которые были указаны ранее. Так, например, при изучении проблемы безопасности для объектов и процессов космического уровня, нужно рассматривать не только угрозы и опасности, исходящие из космического пространства, но также и проблемы обеспечения информационной безопасности самого этого пространства, в котором уже сегодня работают очень важные для обеспечения нашей жизнедеятельности информационные системы навигации, передачи данных и космического мониторинга. Это пространство нуждается в очистке от «космического мусора», который становится одной из новых угроз для деятельности человека в космосе и на Земле.

Аналогичным образом при комплексном исследовании проблем *информационной безопасности личности*, должны рассматриваться не только проблемы защищенности человека от различного рода внешних и внутренних негативных информационных факторов, но также и проблемы формирования *информационно безопасной личности*. При этом необходимо создавать такие условия образования и воспитания, при которых человек не будет являться источником информационных угроз опасности для других людей и окружающей его природы, а также - для самого себя.

Исследования показывают, что именно эта гуманитарная проблема и является в настоящее время ключевой проблемой информационной безопасности дальнейшего развития мировой цивилизации, а ее решение - необходимое условие выживания человечества в современном мире.

4 Предмет и задачи информационной сафитологии

Главными задачами информационной сафитологии должны стать следующие:

1. *Философское осмысление* проблемы информационной безопасности и ее места в стратегии дальнейшего развития мировой цивилизации, а также формирование *системы понятийных знаний* в этой области.
2. *Прогнозирование угроз* для информационной безопасности в различных сферах жизнедеятельности человека и общества, их источников, причин и возможных последствий.
3. *Определение допустимых пределов* негативного информационного воздействия на различные объекты, системы и процессы в природе, техносфере и обществе, то есть, определение тех «красных линий», превышение которых ведет к особо опасным последствиям.
4. Определение адекватных *мер противодействия информационным вызовам и угрозам* для безопасности природы, человека и общества, а также разработка рекомендаций по их реализации на персональном, корпоративном, национальном или международном уровнях.
5. Формирование научно обоснованного *императива информационной безопасности* и принципов его реализации в системе образования и воспитания.
6. Формирование в обществе *культуры информационной безопасности*.
7. *Популяризация передовых достижений* в области обеспечения информационной безопасности.

Предметная область этой науки должна содержать исследования в следующих основных сферах:

- естественная *неживая природа*, включая недра Земли и окружающее ее космическое пространство;
- *биосфера*, включая животный и растительный мир, бактерии и вирусы;
- *техносфера*, включая информационную технику и технологии;
- *общество*, во всем многообразии его жизнедеятельности;
- *человек*, как объект обеспечения информационной безопасности и источник информационных угроз для других людей, государства и общества.

Приведенная структура является весьма широкой, что обусловлено междисциплинарным характером науки об информационной безопасности. Ее формирование является необходимым условием выживания человечества в стремительно изменяющемся и все более опасном мире.

5 Информационная безопасность как глобальная проблема

В современных геополитических условиях проблема информационной безопасности становится глобальной и приобретает новое содержание, в котором большую значимость приобретают геополитические и гуманитарные аспекты этой комплексной проблемы.

По оценкам экспертов, в период 2030–2040 годов может быть сформировано глобальное информационное общество, которое станет принципиально новым этапом развития цивилизации – ***информационной цивилизацией*** [4]**.** Ее особенностью станет преобладание информации и знаний во всех сферах деятельности, а также глубокое воздействие на эти сферы информационных технологий, которые станут катализаторами и главными движущими факторами цивилизационного развития [5].

Глобальная проблема развития мировой цивилизации в XXI веке заключается в том, что культура общества и общественное сознание существенным образом отстают от темпов научно-технологического развития информационной сферы, а новые информационные технологии, в которых все более широко применяются средства и методы искусственного интеллекта, становятся сложными для их понимания.

Информационная сфера является *внешней памятью человечества,* которая в последние годы стремительно развивается. О масштабах и динамике этого процесса свидетельствует тот факт, что созданные в США информационные центры сегодня потребляют около 30% всей энергетики этой страны. Но ведь память – это важнейший функциональный компонент интеллекта. Поэтому, передавая внешним информационным системам значительную часть содержания своей биологической памяти, человечество интеллектуально деградирует. И этот процесс быстро нарастает и становится новой глобальной угрозой для мировой цивилизации. А сам человек все больше становится не творцом и хозяином созданной им глобальной информационной системы, а ее придатком.

Современный человек все больше ощущает себя винтиком гигантского информационно-технологического монстра, который подавляет его индивидуальность и начинает функционировать по собственным законам и в своих интересах.

Похоже, что современное общество быстро приближается к той ситуации, которая была описана в научно-фантастическом романе А. А. Зиновьева «Глобальный человейник» [6]. Он был впервые опубликован в нашей стране, а также в Италии в 1997 г. и затем переиздан в 2019 г.

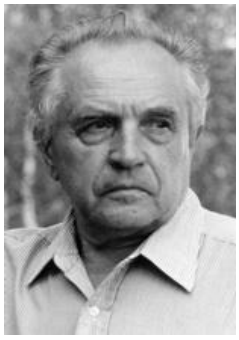
В этом романе образно и наглядно представлена картина жизни человека в XXI веке, когда на всей нашей планете установятся традиции и базовые ценности стран Запада. Автором показано, что их доминирование приведет к тому, что в обществе установится обстановка вседозволенности, развращенного секса и насилия. Будет разрушен институт традиционной семьи, отношения между родственниками утратят свою душевную теплоту, а дети станут для многих людей дорогой и бесполезной обузой.

Этот прогноз российского философа, сделанный им 20 лет назад и казавшийся тогда фантастическим, сбывается на наших глазах. Разве не такую ситуацию мы наблюдаем сегодня в США и странах Западной Европы?

Второй прогноз автора этой книги относится к динамике социально-экономической сферы информационного общества. По его оценке, социальное расслоение в этом обществе существенным образом усилится. При этом безработица станет массовым явлением, так как многие функции общественного производства будут выполнять роботы. Поэтому в обществе появится много «лишних людей», которые будут никому не нужны. И этот прогноз также может оправдаться.

Однако самая большая угроза для человека в таком обществе состоит в его *интеллектуальной деградации,* которая обусловлена развитием и широким использованием средств и технологий искусственного интеллекта. И этот процесс мы также наблюдаем в современном обществе. Он является вполне закономерным. В живой природе существует один из важных законов эволюции. Он утверждает, что все то, что не используется, обязательно деградирует и отмирает.

Поэтому когда мы передаем выполнение своих интеллектуальных функций по решению сложных задач искусственному интеллекту, нужно понимать, что в результате этого мы снижаем уровень своего собственного интеллектуального потенциала. И это очень опасно, так как будущее готовит нам целый комплекс сложнейших проблем, которых решать будет некому. Эта угроза была особо отмечена в монографии известного российского математика и философа Александра Зиновьева [7]. Однако путей эффективного противодействия этой новой глобальной угрозе пока не найдено, хотя она уже начинает осознаваться не только учеными, но и некоторыми политическими лидерами.



*Александр Александрович Зиновьев (*1922–2006 *гг.)*

6 Информационная безопасность как международная проблема

Актуальность проблемы обеспечения информационной безопасности на международном уровне начала осознаваться в самом конце XX века, когда стала понятной неизбежность становления глобального информационного общества и связанных с этим новых вызовов и угроз развитию цивилизации в информационной сфере.

Эта проблема была впервые включена в повестку дня деятельности ООН в 1998 г. по инициативе России. 23 сентября 1998 г. наша страна направила Генеральному секретарю ООН специальное Послание, в котором предлагался проект резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». В нем было указано на угрозу применения информационных технологий в военно-политических целях и давалось определение терминов «*информационное оружие*» и «*информационная война*». Кроме того, указывалось на необходимость запрещения такого оружия, а также на сопоставимость результатов его возможного применения с воздействием оружия массового поражения.

Такая постановка проблемы была принципиально важной, так как она создавала основу для формирования системы международного контроля над развитием информационного оружия. Однако, предложения России в таком контексте не были приняты. В Резолюции ООН, которая была принята в декабре 1998 г. использовались совсем другие термины: «*несанкционированное вмешательство*» и «*неправомерное использование информационных и телекоммуникационных систем и информационных ресурсов*». И это было сделано по результатам замечаний со стороны представителей Великобритании и США в ООН.

Все последующие годы, вплоть до настоящего времени, наша страна продолжает настойчиво бороться за принятие эффективного международного соглашения по обеспечению информационной безопасности на глобальном уровне. Эта деятельность достаточно подробно освещения в монографии специалистов ИМЭМО РАН [8].

В ней также показано, что главным источником угроз в этой области являются США, где в 2018 г. была принята Национальная Киберстратегия. Ее цели и основные направления реализации кратко представлены ниже в Таблице 1.

Анализ их содержания показывает, что эта Стратегия имеет не оборонительный, а главным образом, наступательный характер, так как ее главной целью является *завоевание и удержание господства США в киберпространстве*. И это доминирование США используют не только в своих геополитических и экономических целях, но также и для навязывания другим странам своих базовых ценностей потребительского общества и американского образа жизни.

Нужно отметить, что кроме Национальной киберстратегии в США имеется еще и Киберстратегия Министерства обороны, а также Стратегия Объединенного киберкомандования вооруженных сил, которое включает более шести тысяч специально подготовленных сотрудников.

Таблица 1. Структура Национальной Киберстратегии США

№ пп	Основные задачи	Направления реализации киберстратегии
1	Защита американского народа, Америки и американского образа жизни	Безопасность федеральных сетей и информации. Безопасность критически важной инфраструктуры в киберпространстве. Борьба с киберпреступностью.
2	Обеспечение процветания Америки	Содействие динамичной и устойчивой цифровой экономике. Содействие развитию и защита изобретений в США. Развитие исключительных человеческих ресурсов, обеспечивающих кибербезопасность.
3	Сохранение мира силовыми методами	Повышение киберстабильности через нормы ответственного поведения государств. Атрибуция и сдерживание неприемлемого поведения в киберпространстве.

4	Продвижение американского влияния	Продвижение открытого, интероперабельного, надежного и безопасного Интернета. Создание международного киберпотенциала.

7 Современная структура угроз для информационной безопасности России

Для успешного решения проблем обеспечения информационной безопасности, необходимо, прежде всего, достаточно четко представлять себе структуру и содержание основных вызовов и угроз в данной области, а также определить те источники и причины, которые их порождают. Некоторые результаты наших исследований в данной области в сжатой форме представлены в Таблице 2. Источники и причины вызовов и угроз распределены в этой таблице по областям их проявления в современном обществе. При этом показан ряд новых вызовов и угроз, которые появились в последние годы и, весьма вероятно, станут социально значимыми в будущем.

Таблица 2. Структура основных вызовов и угроз для информационной безопасности России

№ пп	**Области проявления вызовов и угроз**	**Источники и причины вызовов и угроз**
1	Геополитика и международные отношения	Информационное противоборство в киберпространстве. Кибертерроризм. Глобальное информационное наблюдение. Нарушение информационного суверенитета государства.
2	Экономика и финансовая сфера	Монополизация банковских информационных и платежных систем со стороны США. Киберпреступность. Низкий уровень информационной компетенции специалистов.
3	Наука и технологии	Неадекватность международных рейтинговых систем оценки научной деятельности. Монополизация странами Запада производства информационной техники и технологий.
4	Национальное информационное пространство	Деформация традиционных устоев и базовых ценностей. Опасное содержание массовой информации. Недостаточная защищенность персональных данных и государственных информационной ресурсов.
5	Национальная информационная инфраструктура	Низкая безопасность национального сегмента сети Интернет. Недостаточная киберустойчивость критически важных объектов и государственных информационных систем.
6	Система образования	Неадекватность содержания образования новым условиям становления глобального информационного общества. Низкий уровень информационной компетенции специалистов.
7	Культура	Культурологическая и лингвистическая агрессия США и стран Запада. Отсутствие культуры информационной безопасности.

8 Основные направления обеспечения информационной безопасности России

Наши представления об основных направлениях обеспечения информационной безопасности России представлены в Таблице 3. При их определении учитывались те основные информационные вызовы и угрозы, которые были представлены выше.

Необходимо отметить, что Россия в настоящее время находится в эпицентре мировой информационной войны, которая активно ведется странами Запада против нашей страны и ее геополитических союзников. Исследования системных военных аналитиков показали [2,9], что средства и методы, которые применяются в этой войне, по своей эффективности сопоставимы с применением военной силы.

Мало того, они прогнозируют, что после нашего победного завершения СВО на Украине, многоплановое информационное воздействие Запада на Россию не ослабнет, а, наоборот, усилится. При этом наибольшее деструктивное информационное давление, вероятнее всего, будет испытывать гуманитарная сфера нашего общества. Попытки подорвать Россию изнутри будут настойчиво продолжаться, и поэтому к противодействию этим попыткам нужно готовиться заранее.

В связи с все более широким подходом к определению предметной области проблем информационной безопасности, в последние годы в ней появился ряд новых терминов. В их числе: *информационный суверенитет*, *интеллектуальная безопасность*, *когнитивная безопасность*, *лингвистическая безопасность*, а также *живучесть информационных структур* общества. Их содержание раскрывается в работах [9-11].

Все указанные выше новые проблемы информационной безопасности и связанные с ними термины, безусловно, должны найти свое отражение в научно-методологических материалах по этой проблематике.

Таблица 3. Направления обеспечения информационной безопасности России

№ пп	**Области проявления угроз**	**Меры противодействия угрозам**
1	Геополитика и международные отношения	Обеспечение информационного суверенитета государства. Противодействие внешней культурной и информационной экспансии, а также международному кибертерроризму. Информационный нейтралитет. Международная стратегия информационной безопасности.
2	Экономика и финансовая сфера общества	Создание национальных банковских информационных и платежных систем. Снижение уровня киберпреступности. Повышение информационной компетенции специалистов.
3	Наука и технологии	Создание национальных рейтинговых систем оценки научной деятельности. Интеллектуальная безопасность. Собственное производство информационной техники и технологий.
4	Национальное информационное пространство	Сохранение традиционных устоев и базовых ценностей. Безопасное содержание массовой информации. Высокая защищенность персональных данных и государственных информационной ресурсов.
5	Национальная информационная инфраструктура	Безопасность национального сегмента сети Интернет. Киберустойчивость и живучесть критически важных объектов и государственных информационных систем.
6	Система образования	Обеспечение адекватности содержания и методов образования новым возможностям, вызовам и угрозам глобального информационного общества. Повышение информационной компетентности педагогов.
7	Культура	Противодействие культурологической и лингвистической агрессии США и стран Запада. Формирование культуры информационной безопасности личности и общества.

Системные исследования проблем информационной безопасности проводятся в России уже более 30 лет. За этот период получен ряд важных научно-методологических результатов, которые могут стать научной основой для формирования стратегии комплексного противодействия

современным вызовам и угрозам в этой области, как на национальном, так и на глобальном уровне. Примерами здесь могут служить проблемы информационного неравенства, информационные аспекты качества жизни, а также исследования в области философии информации, информационной культурологии, информационной антропологии и информационных оснований эстетики [11,12].

Пришло время более эффективно использовать эти результаты на различных уровнях системы образования, повышения квалификации руководителей и специалистов, а также научных работников. Сегодня это можно осуществить на основе цифровых платформ, которые будут обеспечивать постоянное взаимодействие науки и образования, необходимость которого объективно возрастает.

9 Доктрина и Стратегия информационной безопасности России

Для эффективного противодействия новым информационным вызовам и угрозам для национальной безопасности России необходимо внести соответствующие коррективы в Доктрину информационной безопасности РФ. Ее вторая редакция была принята в 2016 г. и поэтому не учитывает некоторых новых вызовов и угроз, которые появились в последующие годы. Кроме того, необходимо также разработать и утвердить Стратегию информационной безопасности России на период до 2030 года и дальнейшую перспективу. В настоящее время эта работа ведется, но еще не закончена.

Учитывая нарастание комплекса угроз в информационной сфере в современной геополитической ситуации, необходимо также:

- создать *Министерство информационной политики РФ* как централизованный орган управления внешней и внутренней информационной политикой нашей страны;
- разработать *Стратегию информационной безопасности стран БРИКС и ШОС* на период до 2030 года;
- планомерно и настойчиво расширять зарубежное русскоязычное информационное пространство, наполняя его позитивным содержанием о достижениях отечественной науки, технологий, образования и культуры.

Заключение

В настоящее время мировая цивилизация находится на переломном этапе своей истории. Предстоит сделать выбор, который определит дальнейшую судьбу человечества. Необходима новая стратегия развития общества и обеспечения его глобальной безопасности. При этом очень важно обеспечить информационную безопасность, в широком понимании содержания этого термина. Российская академия наук уже около 30 лет осуществляет комплексные исследования проблем безопасности. Они проводятся в виде специальной Программы Президиума РАН «*Безопасность России*» (научный руководитель – член-корр. РАН Н. А. Махутов).

Результаты этих исследований публикуются в виде серии монографий. Издано 75 таких монографий по различным аспектам проблемы безопасности [13, 14]. Очередная монография посвящена проблематике обеспечения информационной безопасности. В ее подготовке участвует и автор настоящей статьи, который надеется, что ее содержание может стать основой для формирования науки об информационной безопасности – информационной сафитологии.

Создание и развитие этой науки позволит вывести дальнейшие исследования проблем информационной безопасности на новый научно-методологический уровень. Результаты этих исследований можно будет использовать не только в России, но и в других странах, прежде всего, в тех, которые являются союзниками России [15].

Литература

1. Ершова Т.В. В центре цифрового мира - человек. //Информационное общество, 2026, № 2. С. 1.
2. Барташ А. А. Мировая гибридная война. М.: Горячая линия-Телеком, 2023. 544 с.
3. Колин К. К. Проектирование будущего и наука о безопасности /Проектирование будущего и горизонты цифровой реальности: труды Восьмой международной беларусско-

российской научно-практической конференции (29-30 мая 2025 г., г. Минск). Минск: Четыре четверти, 2025. 294 с. С. 86-95.

4. Кастельс М. Информационная эпоха: Экономика, общество и культура. М.: ВШЭ, 2017. 606 с.
5. Шваб К. Четвертая промышленная революция. М.: Изд-во "Э", 2017. 208 с.
6. Зиновьев А. А. Глобальный человейник. М.: Эксмо, 1977. 448 с.
7. Зиновьев А. А. Фактор понимания. М.: Алгоритм, 2006. 528 с.
8. Ромашкина Н. П., Марков А. С., Стефанович Д. В. Международная безопасность, стратегическая стабильность и информационные технологии. М.: ИМЭМО РАН, 2020. 98 с.
9. Ильницкий И.М. Ментальная война России. //Военная мысль, 2021, № 8. С. 19-33.
10. Быстров И.И. Живучесть автоматизированных организаций. М.: Майор: Осипенко, 2016. 506 с.
11. Колин К. К. Информационная безопасность: новое содержание комплексной проблемы. //Стратегические приоритеты, 2018, № 4. С. 51-63.
12. Романова А.С. Философские проблемы киборгизации мозга. //Информационное общество, 2025, № 2. С. 56-63.
13. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Анализ вызовов национальной безопасности. М.: Знание, 2024. 700 с.
14. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Системная инженерия в проблемах национальной безопасности. М.: Знание, 2025. 904 с.
15. Особенности политики государств-участников БРИКС в сфере развития ИКТ, обеспечения национальной и международной информационной безопасности. М.: Национальная Ассоциация международной информационной безопасности, 2024. 407 с.

INFORMATION SAFETOLOGY IS THE SCIENCE OF INFORMATION SAFETY

Kolin, Konstantin Konstantinovich

Doctor of technical sciences, professor; Honored worker of science of theRussian Federation
Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, chief researcher
Research and analytical journal "Information Society", member of the Editorial board
Moscow, Russian Federation
Kolinkk@mail.ru

Abstract

The article presents the conceptual foundations of the formation of the science of information security, which is proposed to be called Information Safitology. The relevance and strategic importance of this area of scientific research for ensuring the information security of individuals, society, and the biosphere as a whole in the context of the information revolution of the 21st century are demonstrated. The structure of the subject area of this science, its main objectives, methods, and development prospects are examined. The scientific and methodological potential of Russia, which should be utilized to address this complex issue, is highlighted. Priority research tasks have been identified for the near future in order to determine adequate measures to counter external and internal information threats and to establish the imperative of information security in society

Keywords

information security, information challenges and threats, security imperative, national security

References

1. Ershova T.V. V centre cifrovogo mira – chelovek. //Informacionnoe obshhestvo, 2026, № 2. S. 1.
2. Bartash A. A. Mirovaya gibridnaya vojna. M.: Goryachaya liniya-Telekom, 2023. 544 s.
3. Kolin K. K. Proektirovanie budushchego i nauka o bezopasnosti /Proektirovanie budushchego i gorizonty cifrovoj real'nosti: trudy Vos'moj mezhdunarodnoj belarussko-rossijskoj nauchno-prakticheskoj konferencii (29-30 maya 2025 g., g. Minsk). Minsk: Chetyre chetverti, 2025. 294 s. S. 86-95.
4. Kastel`s M. Informacionnaya e`poxa: E`konomika, obshhestvo i kul`tura. M.: VShE`, 2017. 606 s.
5. Shvab K. Chetvertaya promy`shlennaya revolyuciya. M.: Izd-vo "E`", 2017. 208 s.
6. Zinov'ev A. A. Faktor ponimaniya. M.: Algoritm, 2006. 528 s.
7. Zinov'ev A. A. Global'nyj chelovejnik. M.: Eksmo, 1977. 448 s.
8. Romashkina N. P., Markov A. S., Stefanovich D. V. Mezhdunarodnaya bezopasnost', strategicheskaya stabil'nost' i informacionnye tekhnologii. M.: IMEMO RAN, 2020. 98 s.
9. Il`niczkij I.M. Mental`naya vojna Rossii. //Voennaya my`sl`, 2021, № 8. S. 19-33.
10. Bystrov I. I. Zhivuchest` avtomatizirovanny`x organizacij. M.: Major: Osipenko, 2016. 506 s.
11. Kolin K. K. Informacionnaya bezopasnost': novoe soderzhanie kompleksnoj problemy. //Strategicheskie prioritety, 2018, № 4. S. 51-63.
12. Romanova A.S. Filosofskie problemy` kiborgizacii mozga. //Informacionnoe obshhestvo, 2025, № 2. S. 56-63.
13. Bezopasnost' Rossii. Pravovye, social'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Analiz vyzovov nacional'noj bezopasnosti. M.: Znanie, 2024. 700 s.
14. Bezopasnost' Rossii. Pravovye, social'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Sistemnaya inzheneriya v problemah nacional'noj bezopasnosti. M.: Znanie, 2025. 904 s.
15. Osobennosti politiki gosudarstv-uchastnikov BRIKS v sfere razvitiya IKT, obespecheniya nacional'noj i mezhdunarodnoj informacionnoj bezopasnosti. M.: Nacional'naya Associaciya mezhdunarodnoj informacionnoj bezopasnosti, 2024. 407 s.