КИБЕРПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Горбатов В. С.[1], Эрдниев А. С.[2]

DOI: 10.21681/2311-3456-2024-5-95-104

Цель исследования: *изучить возможность и необходимость использования терминологического описания безопасности информационных технологий и систем.*

Методы исследования: *диалектический и полипарадигмальный подходы, системный анализ, синтез решений.*

Полученные результаты: *могут быть полезны специалистам по защите информации при создании и совершенствовании внутренней (локальной) нормативной базы, а также при создании учебно-методических материалов в сфере образовательных услуг в области информационной безопасности. Полученные результаты также можно рекомендовать потенциальным авторам научных публикаций в аспекте диалектического изложения своих научных достижений.*

Научная новизна: *уделено внимание обсуждению кибернетической сущности рассматриваемого феномена, имеющей с прагматической точки зрения относительно общий характер и определяющей более общее толкование различных понятий с приставкой кибер-..., в частности, взаимосвязь терминов информационная безопасность и кибербезопасность.*

Практическая ценность: *с практической точки зрения данное исследование рассматривается, как решение частной задачи в рамках общей проблемы совершенствования подготовки кадров для органов внутренних дел.*

Ключевые слова: *законы диалектики, информационная безопасность, кибернетика, кибербезопасность, критическая информационная инфраструктура, метапредметность, парадигма, понятийный аппарат, терминология.*

Введение

Всеобщая цифровизация жизнедеятельности российского общества не обходит стороной и органы внутренних дел (ОВД) как особой разновидности государственной службы. Преобразования в области ИТ-технологий последних лет позволили автоматизировать многие процессы оказания государственных услуг, обеспечить оцифровку реестров значимой информации, в том числе касающихся персональных данных граждан Российской Федерации. Происходит активное внедрение телекоммуникационных систем для обеспечения охраны общественного порядка и безопасности граждан.

Вместе с тем, очевидно, что активная цифровизация государственного управления требует наличия у представителей органов госвласти дополнительного набора профессиональных компетенций, что, в свою очередь, актуализирует проблему совершенствования процесса подготовки кадров, в том числе в интересах системы ОВД.

С целью определения возможных подходов разрешения этой проблемы было поставлено исследование этого актуального аспекта системы ведомственного образования[3], в частности, в рамках задачи, поставленной в [1].

Актуальность указанного исследования также поддерживается перспективой реформирования в ближайшие годы общей системы высшего образования, в том числе утверждения новых образовательных стандартов. В рамках проводимой реформы перед профессиональным научно-образовательным сообществом поставлена задача более основательного подхода к разработке новых квалификационных требований и компетенций на основе современных тенденций развития цифровых технологий.

Несмотря на уже существующую детальную формализацию образовательного процесса в интересах системы ОВД, в ней существует ряд позиций, изменение которых, на наш взгляд, позволит повысить уровень подготовки необходимых специалистов по вопросам безопасности используемых цифровых технологий. Например, изменение структуры и содержания требований к специальной профессиональной подготовке сотрудников ОВД с учетом современных тенденций позволит расширить рамки применяемых образовательных программ, а их содержательное наполнение под задачи профессиональной деятельности обеспечит впоследствии детальную проработку вариативной части соответствующего учебно-методического обеспечения.

1 Горбатов Виктор Сергеевич, кандидат технических наук, доцент, Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия, e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733

2 Эрдниев Александр Сергеевич, кандидат педагогических наук, Московский университет МВД России имени В. Я. Кикотя, г. Москва, Россия, e-mail: konfuci@inbox.ru, https://orcid.org/0009-0007-5363-8365

3 Научно-исследовательская работа проводится в рамках выполнения договора о взаимном сотрудничестве между НИЯУ МИФИ и Московским университетом МВД России имени В. Я. Кикотя от 12 июля 2023 г. № 394.

Выше уже упоминалась возможность решения одной из частных задач такого исследования применительно к вопросам обеспечения безопасности информационной инфраструктуры ОВД [1]. В настоящей работе в качестве логического продолжения рассмотрена еще одна частная задача, связанная с уточнением и конкретизацией используемого в будущем терминологического аппарата для дальнейшего общего анализа вопросов совершенствования подготовки кадров в исследуемой области в интересах ОВД.

Актуальность поставленной задачи определяется тем, что такое многомерное явление как информационная безопасность (ИБ) находит свое отражение применительно к различным областям научного познания и, следовательно, современный феномен цифровой информации с прагматической точки зрения требует внимания к вопросам унификации соответствующего понятийного аппарата научной и/или образовательной деятельности, в том числе в области обеспечения безопасности информационных систем. При этом, как правило, предполагается возможность решения указанной проблемы по однозначному пониманию и описанию сложно формализуемых задач данной области с последующей единообразной их технологической реализации в различных приложениях. Прагматичная мотивация подобного подхода сводится к очевидной необходимости создания общепринятой понятийной основы для повышения эффективности коммуникативного взаимодействия специалистов различного профиля в условиях «взрывного» характера развития информационных технологий. Не умаляя научной и практической значимости такой методологии, отметим, однако, что в соответствии с законами диалектики указанный подход имеет и серьезные ограничения в аспекте его применения к анализу фундаментальных проблем образовательной деятельности. Попытки «жесткой» унификации (стандартизации) определений (дефиниций) основных понятий сложной предметной области, в частности, обеспечения информационной безопасности, только на основе «хороших практик», без учета диалектики развития содержания и сущности таких понятий, может привести к их «омертвлению» в аспекте совершенствования образовательных программ, что является характерным следствием метафизической методологии познания.

В настоящей работе показаны возможность и необходимость использования для терминологического описания такой предметной области исследования, как безопасность информационных технологий и систем, полипарадигмального подхода, учитывающего диалектику развития языковых и речевых явлений, терминов и понятий [2].

При этом обеспечивается «взрывной» характер развития указанных технологий даже при наличии относительной неопределенности терминологического базиса.

Трудно не согласиться с авторами указанной выше работы [2, с. 1], которые утверждают, что «... сущность языкового явления раскрывается только путем обнаружения его связей и отношений с другими явлениями на основе выделения единичного, особенного и всеобщего». При этом важнейшим условием является применение основных законов диалектики. Далее утверждается, что «...современная функциональная лингвистика провозглашает новый подход к изучению языковых явлений: не от формы к значению и функции...», а в точности до наоборот. Постулирование необходимости полипарадигмального подхода к изучению языковых и речевых явлений позволяет изучать их со всех сторон: системно-структурной, функциональной, коммуникативной и прагматической.

Как показано ниже такая лингвистическая методология хорошо подтверждается контент-анализом различных исследований искомого понятия ИБ, которое рассматривается в качестве объекта или предмета научного познания не только в естественных и технических отраслях наук [1, 3, 7 и др.]., но и гуманитарного профиля: философии, правоведения, социологии, политологии, педагогики и т.д. [4, 5, 6 и др.].

И, естественно, с точки зрения методологического преломления понятие ИБ приобретает неоднозначные сущностные парадигмы. Так в базовом законе[4] правовое содержание ИБ раскрывается через понятия «защита информации» (ст. 16), «ограничение доступа к информации и распространения сведений, имеющих свойство конфиденциальности» (ст. 5 ч. 3; ст. 6). В ГОСТ[5] приводится наиболее распространенное в сфере оказания дополнительных образовательных услуг определение ИБ (п. 3.28) как безопасность информации, определяемое по трем основным критериям: доступности (ст. 3.7), целостности (п. 3.36) и конфиденциальности (п. 3.10). И далее дополняется критериями подлинности (п.3.6), неотказуемости (п. 3.48) и достоверности (п. 3.55).

В кредитно-финансовой сфере принята своя формулировка парадигмы ИБ[6], целью которой является необходимость обеспечения непрерывности бизнеса.

4 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5 Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. N 392-ст).

6 Стандарт ЦБР СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (принят и введен в действие распоряжением ЦБР от 21 июня 2010 г. № Р-705).

Таким образом, без необходимого уточнения понятия ИБ применительно к сфере профессиональной деятельности ОВД дальнейший анализ образовательных аспектов в интересах данной структуры государственной службы будет содержать существенные недостатки системного характера.

Одной из существенных новаций терминологического характера последних лет в исследуемой области, связанной с научно-образовательной деятельностью, является нормативная легализация применения понятия «кибербезопасность» [3]. Введена новая научная специальность – кибербезопасность – наряду с традиционной – информационная безопасность, методы и средства защиты информации, в Российской академии наук создано новое подразделение.

Эта легализация сопровождается активной разработкой различных проектов соответствующих организационно-распорядительных и методических документов в сфере высшего образования[7]. В Российской академии наук создана организационная структура государственного характера с данным наименованием.

Поэтому в соответствии с обсужденной выше методологией научного познания необходим анализ введения и такой новации применительно к сфере деятельности ОВД и на этой основе выявление характерных ее особенностей для соответствующей подготовки необходимых специалистов.

Таким образом, задается цель данной работы – определение терминологической сущности и содержания основных понятий: ИБ и кибербезопасности, применительно к системе ОВД. Результаты решения этой задачи будут использованы для дальнейшей проработки предложений по совершенствованию учебно-методической базы подготовки кадров в интересах ОВД, хотя в методологическом плане могут быть полезны специалистам и других сфер общественной деятельности.

1. Метапредметное свойство ИБ

На нынешнем этапе подготовка специалистов в исследуемой области в интересах ОВД осуществляется в рамках обучения по укрупненной группе специальностей и направлений подготовки (УГСНП) – информационная безопасность – в соответствии с нормативными требованиями, заданными федеральными образовательными стандартами высшего образования (ФГОС ВО), в частности по специальности 10.05.05[8] с ведомственными процедурными уточнениями[9]. Терминологическую основу данных ФГОС составляет уже устоявшаяся, хотя и не без дискуссионных моментов, обширная понятийная база естественных и технических наук. В то же время практически отсутствуют компетенции, связанные с гуманитарными аспектами ИБ. Поэтому в рамках задачи, поставленной в настоящей работе целесообразно провести анализ различных полипарадигмальных подходов, исходя из понятийной базы наук гуманитарного профиля, как необходимого этапа достижения сформулированной выше цели исследования метапредметного свойства (сущности) феномена ИБ.

1.1. Философский подход

Осмысление проблемы на уровне философской методологии предполагает применение диалектического подхода [4], по которому термин ИБ тесно связано с понятиями «информационная свобода» и «информационное насилие». В этом случае феномен ИБ может определяться с одной стороны метафизическим состоянием свободы, как противоположностью детерминированности, с другой в социально-политическом смысле, как отсутствием ограничений. Генезис безопасности в информационной пространстве связывается не только с наиболее традиционным представлением как защита информации ограниченного доступа, но и с «защитой от нежелательной информации». Отсюда следует что, любое вмешательство третьих лиц в добровольное и свободное информационное взаимодействие, приводящее к нарушению данного фактора, является «информационным насилием». В этом случае допустимо применить так называемый либертарианский подход к осмыслению феномена ИБ, по которому свобода рассматривается с точки зрения отсутствия инициированного насилия. Таким образом, ИБ можно рассматривать в качестве некоторого состояния защищенности информационного пространства от нежелательных воздействий. Эта конструкция используется в первой и второй версиях Доктрины информационной безопасности Российской Федерации[10].

В то же время развитие толкования понятия ИБ тесно связывается с четвертой промышленной революцией и одной из рамочных характеристик выступает понятия «информационная цивилизация» в контексте информационной реальности [5]. Рассмотрение информационной реальности на основе метафизического и диалектического подходов предполагает выделение ряда свойств ИБ:

7 Портал федеральных государственных образовательных стандартов высшего образования // URL: https://fgosvo.ru/ (дата обращения: 24.05.2024).

8 Приказ Минобрнауки РФ от 26.11.2020 № 1461 «Об утверждении федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере» (Зарегистрировано в Минюсте РФ 22.12.2020 № 61703).

9 Приказ МВД России от 2 февраля 2024 г. № 44 «Об утверждении Порядка организации подготовки кадров для замещения должностей в органах внутренних дел Российской Федерации» (Зарегистрировано в Минюсте РФ 12.03.2024 № 77488).

10 Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

- развитие потенциала социальной коммуникации за счет внедрения информационных технологий;
- угроза информационной защищенности благодаря выделению таких институтов, как информационная война, информационный терроризм, нейролингвистическое программирование, отчуждение личности в виртуальной компьютерной реальности (метавселенная);
- отрицательная энтропия, основанная на системности, организованности, упорядоченности информации, отсюда информационная реальность выступает в качестве силы, противодействующей хаосу и дезорганизации.

С позиции метафизического подхода ИБ выступает в качестве произвольно конструируемой системы, в основе которой лежит технологический прогресс. В этом случае ИБ обладает определенными динамическими свойствами, своего рода энергетическим потенциалом, для которых выступают потребности информационного общества. Диалектический подход к толкованию ИБ возлагает на это понятие свойство противодействия деструктивным информационным проявлениям.

Динамика социально-политических явлений как внутреннего, так и международного характера последних нескольких лет предполагает рассмотрение понятия ИБ через призму прокси-войн и военной безопасности российской цивилизации [6]. Именно через призму такого противоборства в так называемом киберпространстве как части сферы военного противостояния и часто рассматривается легализируемый ныне термин кибербезопасность [7].

Применение междисциплинарной методологии и системного подхода к осмыслению ИБ как составляющей военной безопасности Российской Федерации также определяет актуальность ее учета во всех сферах общественных отношений. Причем деструктивному воздействию подвергаются как социальные общности, так и отдельные индивиды. С точки зрения состояния защищенности ИБ не разделяет обеспеченность защитой отдельного индивида или социума в целом, а лишь расширяет или сужает объекты информационного воздействия. ИБ выступает в качестве «состояния репрезентативной практики социума, регистрирующей ее качественную способность реагировать на предотвращение различного вида опасностей материальным и духовным ценностям».

Таким образом, философское осмысление понятия ИБ позволяет определить этот феномен и как статичное состояние материального и духовного объекта, так и представить в качестве динамического процесса, направленного на обеспечение интересов общества и индивида, в том числе в рамках охраны общественного порядка.

1.2. Социологический подход

Социологический подход к определению понятия информационной безопасности предполагает выделение трех ключевых элементов в структуре информационной безопасности [8]. Среди них:

1) Информационно-правовое или нормативное правовое регулирование, обеспечивающее защиту интересов различных субъектов в сфере информационной безопасности.
2) Информационно-техническое или обеспечение защищенности информации путем технических и программных средств защиты.
3) Информационно-психологического защита личности от деструктивного информационного контента.

При этом ключевой проблемой [8, с. 12] в вопросе трактовки понятия ИБ автор видит в «смешении подходов естественнонаучных и гуманитарных дисциплин». При этом отмечено, что гуманитарный подход обладает избыточной абстракцией в конкретизации терминологии. Такой социологический подход позволяет позиционировать ИБ в качестве составляющей социологии безопасности. Указанные условия определяют ИБ, как «сложное системное, многоуровневое явление современного социума, представляющее собой стабильное, равновесное существование информационно-коммуникационной подсистемы общества, выражающееся в отсутствии дезорганизационно-дисфункциональных индикаторов (маркеров) в ее функционировании».

Проще говоря, ИБ есть отрицание (и преодоление) информационной опасности, проявляющейся в любых масштабах. Опасности и угрозы ИБ определяют содержание деятельности по ее обеспечению. «Обеспечение ИБ представляет собой защиту от опасностей и угроз инфосферы общества, а также предполагает позитивное развитие информационной реальности, порождающее отсутствие негативных эффектов от процесса информатизации».

1.3. Политологический аспект ИБ

Глубина политологических исследований направлена на анализ технологий, средств и методов обеспечения ИБ. Современная геополитическая ситуация определяет интерес к исследованию феномена ИБ в контексте политических процессов и «мягкой» методологии их организации [9]. Политологическая ориентация определения понятия ИБ предлагает следующую трактовку: «состояние защищенности всех сфер общественной жизни, общественного сознания от негативного воздействия информацией, обеспечиваемое государством и гражданским обществом и являющееся ключевым условием модернизации и демократизации общества и государства и их готовности к защите национальных интересов страны на международной арене». Подобная трактовка

позволяет определить нетрадиционную форму понятия ИБ, как «состояние защищенности от информации», в качестве альтернативно предложенного ранее определению «защищенности информации и информационного пространства».

То есть ИБ, как социально-политический феномен, связывается с развитием гражданского общества, в этом случае объективно безрамочное информационное пространство ограничивается интересами отдельной социальной общности. Информация переходит из категории идеального в материальный объект, обеспечивающий артикулированность интересов отдельного индивида и социальных структур. В этом случае концепция информационной безопасности выделяет в качестве объекта охраны национальную идентичность. Векторами обеспечения национальной ИБ выступают: идеологическая целостность национального информационного пространства и защита от внешних деструктивных информационных акторов.

Ключевым акцентом политологического рассмотрения понятия ИБ является отношение к таким понятиям как целостность и доступность информации. Целостность обеспечивается свободой распространения взглядов любыми социальными субъектами, равенство доступа к информации. Доступность наделяет информационное пространство такой характеристикой, как защита от сокрытия информации от потребителя.

1.4. Право и ИБ

Связь ИБ с гражданским обществом определяет потребность изучения контекста данного понятия через призму юридических наук. Связь ИБ с правами человека обуславливает анализ теоретико-правовой значимости этого понятия [10]. В данном контексте справедливо применение аксиологического подхода в осмыслении понятия ИБ в связи с теорией государства и права. Определение ИБ в качестве правовой категории выделяет такие понятия, как информационный патернализм, цифровая идентичность и свобода информации в рамках национального права.

Формальный антагонизм между информационной свободой и информационной безопасностью преодолевается путем определения взаимозависимостей между двумя категориями как правовыми ценностями нового времени. Отсюда следует, что правовая природа ИБ определяется, как «состояние защищенности прав человека в информационной сфере». Обеспечение ИБ личности реализуется путем дополнения правовых средств защиты техническими нормами. При этом важнейшим композитом достижения баланса интересов личности и государства выступает принцип правовой соразмерности.

Систематизация нормативно-правовых оснований, определяющих сущность ИБ в национальном законодательстве, выделяет потребность в унификации терминологического аппарата [11, с. 165]. В качестве обоснования представлены дефиниции отдельных смысловых конструкций, не имеющих однозначной трактовки, например «информационные ресурсы» (ИР). Универсальная с точки зрения права и науки трактовка понятия ИР позволит преодолевать нарушения правовой логики при формализации общественных отношений.

2. Формализация метапредметности ИБ

Проведенный краткий и даже в некотором роде поверхностный анализ толкований понятия ИБ с позиций гуманитарных наук дает обоснование закрепить его метапредметное свойство как особенную характеристику, определяющую его полипарадигмальную (многоаспектную) сущность и не позволяющую в полной мере осуществить возможный таксонометрический подход.

На рис. 1 представлена сущностная характеристика ИБ с точки зрения совокупности научных гуманитарных знаний, ее определяющих. Так философский подход позволяет дать статичные и динамические свойства ИБ, социологический подход наделяет ИБ потенциалом отрицания и преодоления информационной опасности, политологический подход наделяет ИБ характеристиками целостности и доступности, аксиологическое основание через призму юридического подхода определяет ИБ, как состояние защищенности прав человека в информационной сфере.

Нормативная правовая регламентация ИБ применительно к органам внутренних дел обоснованно затрагивает и уголовно-правовые аспекты [12]. Уголовно-правовое содержание ИБ тесно связано с такими понятиями, как: конфиденциальность (тайны) информации, безопасность обращения с компьютерной информацией, права граждан на получение информации. В рассматриваемом контексте ИБ представляется в виде совокупности «общественных отношений, регулируемых системой правовых норм, направленных на обеспечение национальных интересов государства, интересов общества, на обеспечение законных интересов личности и субъектов хозяйствования в информационной сфере». Ключевой характеристикой в призме уголовно-правового регулирования является защита компьютерной информации от несанкционированного доступа, уничтожения, блокирования, модификации, копирования и неправомерного использования».

В этом смысле ассоциативное соотнесение системы ОВД с институтом принуждения приводит к однобокой трактовке понятия ИБ применительно возможной тематике соответствующих образовательных программ. Нормативный правовой контекст указанного понятия в искомом институте государственной

власти связывает ИБ только с защитой информации [13].

Сформулированная ранее сущность ИБ позволяет сделать вывод о том, что интерпретация искомого понятия в контексте ОВД исключает ряд значимых характеристик, к которым относится: обеспечение доступности информации, отрицание и преодоление информационной опасности, активное противодействие информационному насилию. Исключения приводят к нивелированию всех динамических свойств понятия ИБ, сводя его только в состояние защищенности ограниченного информационного пространства. При таком прочтении ИБ в контексте деятельности ОВД приобретает окрас как некий объект охраны без активного противоборства, что значительно сужает содержание образовательной подготовки в интересах ОВД по направлению ИБ.

Возможные решения противоречий основываются на конкретизации и системной структуризации образовательной подготовки в ведомственных ООВО. ИБ, как ключевое определение направлений подготовки не должно основываться на «таксономическом» представлении понятия, как обеспечения безопасности отдельных видовых объектов [14, с. 139]. А рассматриваться с точки зрения состояния защищенности собственного информационного пространства и защищенности от деструктивной информации. Подобная целевая установка позволяет расширить образовательный потенциал ведомственной подготовки кадров, увеличивая спектр возможных компетенций.

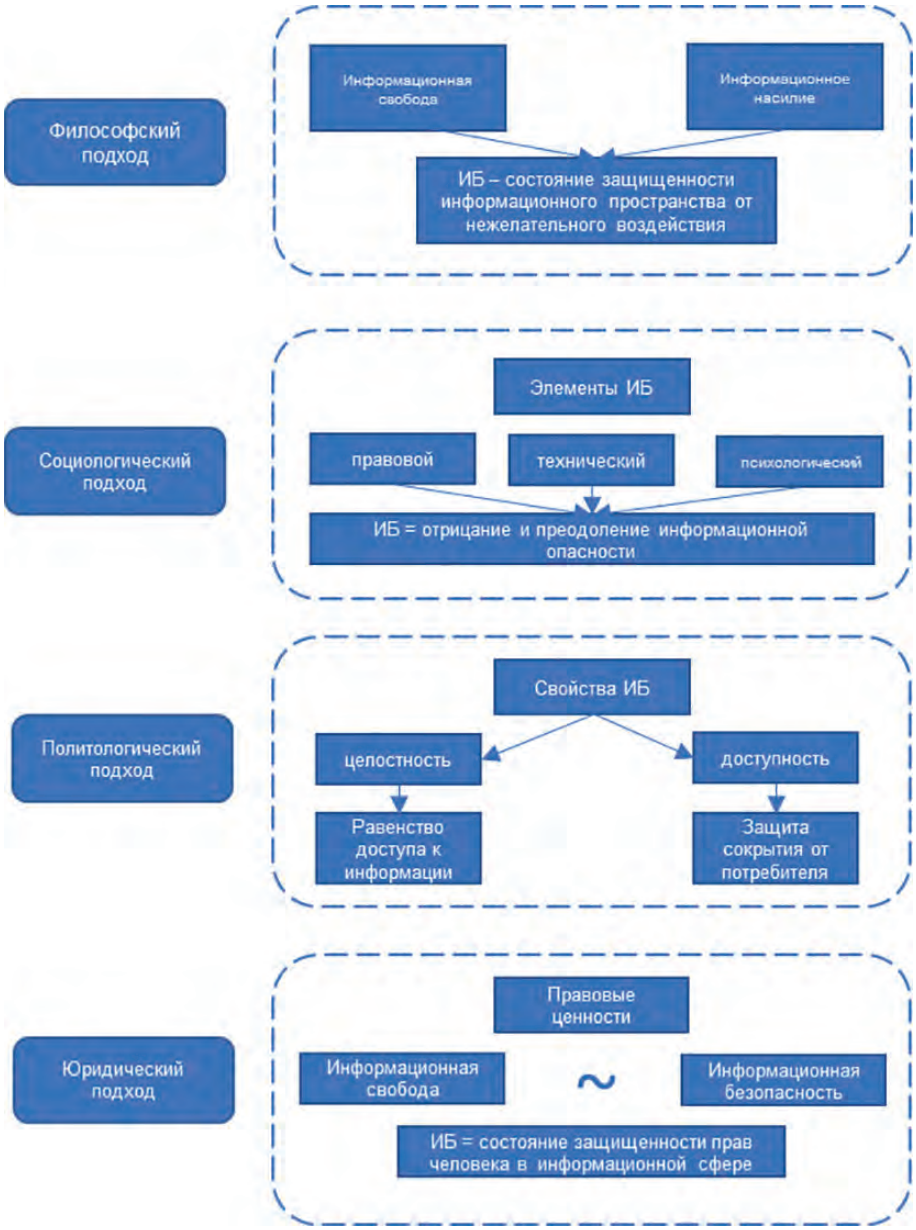

Рис. 1. Сущность понятия ИБ как метапредметной категории

3. Кибернетическая сущность ИБ

Описанное выше с позиций наук гуманитарного профиля метапредметное свойство (сущность) исследуемой области в рамках поставленной задачи на наш взгляд целесообразно дополнить практически не встречающимся в научных публикациях представлением, названным нами киберпарадигмой ИБ. Выбор этого термина сделан по примеру повального применения в последнее время понятий с приставкой кибер-... (киберпространство, киберугрозы, кибератаки и т.д.). В этом же аспекте лежит упомянутая выше нормативная легализация понятия «кибербезопасность» в виде наименования альтернативы научной специальности – информационная безопасность, методы и средства защиты информации.

Информационный поиск «на просторах Интернета» показал, что данный термин не является новацией авторов настоящей работы. Так в YouTube уже существует канал молодого пытливого исследователя PardigM[11], используемый для «романтического» описания государства будущего, «всеобщее процветание» на основе «правильной» цифровизации общественных отношений. То есть за счет технологических достижений можно добиться коренного изменения социальных отношений. Не вдаваясь в дальнейшую дискуссию, отметим только в качестве существенного замечания используемое определение понятия кибер (CYBER) как «приставка, использующаяся для того, чтобы присвоить слову значение чего-то относящегося к эпохе компьютеров, Интернета и цифровых технологий». Довольно распространенное представление, генезис которого будет обсужден ниже.

Применительно к сфере общественной безопасности данный термин по умолчанию, без определения, используется в публикации[12]. Но опять суть приставки понятен из контекста статьи и в целом совпадает с указанным выше представлением.

Недостаток таких представлений, несомненно, имеющих «право на жизнь», состоит в том, что они сильно сужают области возможного применения, так как авторы в своих рассуждениях используют критикуемый лингвистами подход от формы к значению и функции.

В отличие от этих публикаций в данной работе применительно к термину киберпарадигма будет обсуждаться его сущность, исходя из определения общего функционала систем обеспечения ИБ, то есть путем перехода от их функционала к форме понятия. Такой функционал определяется на основе кибернетического подхода, определяемого как «...наука об управлении, изучающая ... общие законы получения, хранения, передачи и преобразования информации в сложных управляющих системах»[13] независимо от формы их представления в материальном мире (см. рис. 2).

Рассматриваемая в данной работе взаимосвязь кибернетики и проблематики ИБ, правда по отношению к понятию «защита информации», была представлена еще в конце прошлого века профессором Герасименко В.А. в работе [15]. Суть такой взаимосвязи автор рассматривал через, введя очевидное, но практически, не используемое, понятие «качество информации», то есть условия, очевидно необходимое для эффективных управленческих процессов. В свою очередь, оно раскрывается через традиционное толкование информационной безопасности (защиты информации), в соответствии с упомянутым выше «гостовским» подходом: доступности, целостности и конфиденциальности.

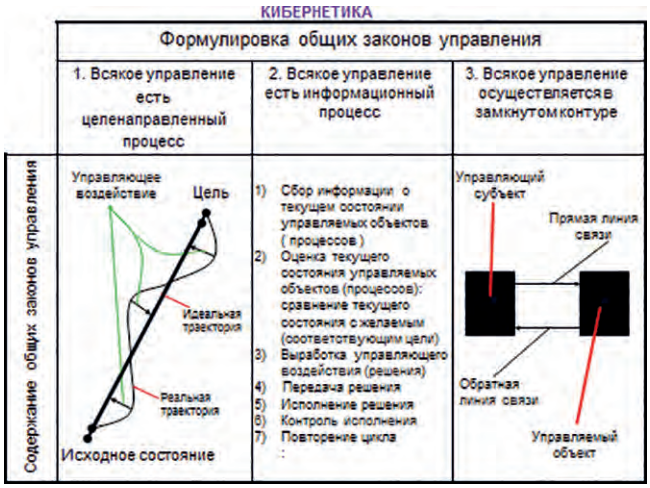

Рис. 2. Функционал кибернетического подхода [15]

Второй новацией рассматриваемой работы, связанной, в общем-то, с важной, но достаточно традиционной проблемой – повышением информационной грамотности, это представление уровня развития информации применительно к разным видам систем объектного (материального мира) (см. рис. 3).

Такое представление послужило толчком для дальнейшего расширения толкования киберпарадигмы ИБ с использованием сущности понятия «информационные ресурсы» (ИР). Оно имело легальное представление в недействующем с 2006 г. базовом законе «Об информации, информатизации и защите информации». Но, с методологической точки зрения, в рамках данной работы имеет смысл привести полностью определение функционала данного понятия:

11 [Философия] Основа киберпарадигмы. URL: https://www.youtube.com/watch?v=PjLbC_P-qoc (дата обращения: 24.05.2024).

12 Кибер-парадигма и общественная безопасность - действительно ли мы готовы. URL: https://safecity.by/index.php?route=revolution/revblog_blog&revblog_id=12 (дата обращения: 24.05.2024).

13 Кибернетика. Большая Советская энциклопедия. URL:https://bigenc.ru/c/kibernetika-979287 (дата обращения: 24.05.2024).

Рис. 3. Взаимосвязь видов информации и видов материального мира

«Глава 2., Статья 4. Основы правового режима ИР:

1. *Информационные ресурсы* являются объектами отношений физических, юридических лиц, государства, составляют ИР России и защищаются законом наряду с другими ресурсами.

Статья. 5 Документирование информации

1. *Документирование информации* является обязательным условием включения информации в ИР».

Не вдаваясь в обсуждение очевидной прагматической сущности понятия ИР как документированной информации, приведем возможную формулировку киберпарадигмы ИБ, определяющей известную риск-ориентированную или «бизнес»-процессную методологию обеспечения ИБ, применимую не только к предпринимательской деятельности, но и к государственной службе.

«Информационная безопасность – необходимое условие и цель деятельности в виде одного из показателей эффективности управления любой сложной системы управления. Управление невозможно без ИР (активов), защищаемых законом. Документирование – необходимое условие включения информации в ИР».

При таком киберпредставлении сложное описание сущности ИБ сводится к ее тривиальному прагматическому представлению как обеспечение безопасности делопроизводства и документооборота, в том числе в аналоговом (бумажном) виде с известными технологиями архивной деятельности. Недаром в указанном выше «гостовском» определении ИБ к трем основным критериям добавлены дополнительные: подлинности (п. 3.6), неотказуемости (п. 3.48) и достоверности (п. 3.55), что свидетельствует об интуитивном понимании прагматической сущности ИБ.

В то же время такое достаточно тривиальное представление не отменяет, а, скорее поясняет в современных условиях цифровизации общественной деятельности, многообразие системно-структурной сути («ниш») понятия ИБ. В частности, в отечественном законодательстве выделены: ограничение к государственной и профессиональным тайнам, ограничение распространения сведений, имеющих свойство конфиденциальности, защита персональных данных, в том числе общедоступного характера, безопасность электронного документооборота, обеспечение устойчивости критической информационной инфраструктуры, с разнообразными сложными механизмами и процедурами правового регулирования.

Очевидно разнообразие и прагматической сущности феномена ИБ. Любая система управления, рассматриваемая через призму технологий делопроизводства и документооборота, тем более в аспекте государственной службы, имеет свою специфику, исходя из назначения и функционала объекта управления. Это будет учитываться в дальнейшем уточнении профессиональных компетенций работников ОВД и вариативной части соответствующих образовательных программ.

Несмотря на указанную относительную общность предлагаемого толкования парадигмы ИБ на основе кибернетической сущности, необходимо в соответствии с законами диалектики также указать и на ограничение такого подхода.

Достаточно очевидно, что предлагаемая формулировка отражает лишь технологическую сущность феномена ИБ. Ее толкование, например, в рамках рассмотренного выше метапредметного свойства в аспекте гуманитарных наук достаточно затруднительно, хотя законы кибернетики по достаточно общепринятому представлению можно распространить и на процессы социального характера. Но такая пока неочевидная взаимосвязь кибернетики и ИБ требует дополнительного изучения представителями наук гуманитарного профиля.

Несколько слов о понятии «кибербезопасность» применительно к выводам данной работы. Его общее толкование, опирающееся на кибернетическую сущность феномена ИБ, по существу является его синонимом при указанном выше ограничении в аспекте гуманитарных подходов.

Но, исторически кибернетика наряду с другими научно-техническими достижениями давшая мощный импульс развитию компьютерных технологий, стала одной из фундаментальных основ так называемых «computer science» в развитых странах. Это и привело к более узкому толкованию приставки кибер-... как сущности, определяющей область своего применения только как в цифровом киберпространстве. С позиций полипарадигмального подхода это вполне допустимо, хотя в информационном противоборстве более важной и существенной частью является содержательный (контентный) подход, чем технологическая (инструментальная), составляющая.

Заключение

Представленные выше результаты анализа полипарадигмального подхода к толкованию сущности понятий ИБ и кибербезопасность, исходя из понятийной базы наук гуманитарного профиля и кибернетики, показывает, что в условиях, казалось бы, терминологического «хаоса» возможно достижение достаточно удовлетворительного уровня защищенности отечественной информационной инфраструктуры.

В то же время актуализируется необходимость дальнейшего совершенствования учебно-методической базы подготовки соответствующих специалистов в интересах ОВД, как совокупности структур отдельного вида государственной службы, обеспечивающего практически полную совокупность вопросов обеспечения ИБ Российской Федерации.

В частности, с позиций представленных подходов уже были проанализированы проекты новых ФГОС 4+ применительно к системе ОВД, подготовлены соответствующие предложения по их корректировке, которые в ближайшее время будут опубликованы в одном из научных изданий, входящих в перечень ВАК России.

Литература

1. *Горбатов, Виктор С.; Эрдниев, Александр С. Совершенствование подготовки кадров по обеспечению безопасности информационной инфраструктуры органов внутренних дел. Безопасность информационных технологий, [S.l.], т. 31, № 1, с. 100–119, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.*
2. *Девдариани Н. В., Рубцова Е. В. Законы диалектики в языке. Балтийский гуманитарный журнал. 2018, т. 7, № 2(23), с. 31–34. – EDN XULTMD.*
3. *Марков А. С. Кибербезопасность и Информационная Безопасность как Бифуркация Номенклатуры Научных Специальностей. Вопросы кибербезопасности. 2022, № 1(47), с. 2–9. DOI: 10.21681/2311-3456-2022-1-2-9. – EDN XMKFJH.*
4. *Столяров А. В. Информационная свобода и информационное насилие: специальность 09.00.11 «Социальная философия»: автореферат диссертации на соискание ученой степени кандидата философских наук. М. 2012 – 27 с.*
5. *Корягин В. В. Информационная реальность: сущность и особенности: специальность 09.00.11 «Социальная философия»: автореферат диссертации на соискание ученой степени кандидата философских наук. Улан-Удэ, 2018. – 25 с.*
6. *Медняк И. А. Военная безопасность современного общества в условиях новой информационной реальности: специальность 5.7.7. «Социальная и политическая философия»: диссертация на соискание ученой степени кандидата философских наук. Новочеркасск, 2022. – 160 с.*
7. *Добродеев А. Ю. Кибербезопасность в Российской Федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века. Вопросы кибербезопасности. 2021, № 4(44), с. 61–72. DOI: 10.21681/2311-3456-2021-4-61-72. – EDN MXUVBS.*
8. *Жуйков А. Е. Информационная безопасность в условиях генезиса виртуального пространства трансформирующегося российского общества: специальность 22.00.04 «Социальная структура, социальные институты и процессы»: диссертация на соискание ученой степени кандидата социологических наук. Краснодар, 2016. – 155 с.*
9. *Артамонова Я. С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения: специальность 23.00.02 «Политические институты, процессы и технологии»: автореферат диссертации на соискание ученой степени доктора политических. М., 2014. – 56 с.*
10. *Туликов А. В. Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ): специальность 12.00.01 «Теория и история права и государства; история учений о праве и государстве»: автореферат диссертации на соискание ученой степени кандидата юридических наук. М., 2017. – 24 с.*
11. *Мамедов Э. Ф. Терминология законодательства об информации, информационных технологиях и о защите информации как средство обеспечения информационной безопасности. Теория государства и права. 2023, № 1(30), с. 163–174. DOI: 10.25839/MATGIP_2023_1_163. – EDN NZVWLS.*
12. *Мнацаканян А. В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореферат на соискание ученой степени кандидата юридических наук. М., 2016. – 40 с.*
13. *Григорьев А. Н., Локтионов О. В., Подружкина Т. А. и др. Основы информационной безопасности в органах внутренних дел: Учебник. СПб: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2019. – 312 с. – EDN SQGZCB.*
14. *Толстой Александр И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 130–148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.*
15. *Герасименко В. А. Основы информационной грамоты. М.: Энергоатомиздат, 1996. – 320 с.*

CYBER PARADIGM OF INFORMATION SECURITY IN THE INTERNAL AFFAIRS BODIES

Gorbatov V. S.[14], Erdniev A. S.[15]

The purpose of the study *is to study the possibility and necessity of using a terminological description of the security of information technologies and systems.*

14 Viktor S. Gorbatov, Ph.D. in Engineering sciences, Associate Professor, National Research Nuclear University «MEPhI», (Moscow Engineering Physics Institute), Moscow, Russia. E-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733

15 Aleksandr S. Erdniev, Ph.D. in Pedagogical sciences, Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V. Y. Kikot, Moscow, Russia. E-mail: konfuci@inbox.ru, https://orcid.org/0009-0007-5363-8365

Research methods: *dialectical and polyparadigm approaches, system analysis, synthesis of solutions.*

The results obtained *can be useful to information security specialists in the creation and improvement of the internal (local) regulatory framework, as well as in the creation of educational and methodological materials in the field of educational services in the field of information security. The results obtained can also be recommended to potential authors of scientific publications in the aspect of dialectical presentation of their scientific achievements.*

Scientific novelty: *the author pays attention to the discussion of the cybernetic essence of the phenomenon under consideration, which from a pragmatic point of view has a relatively general nature and determines a more general interpretation of various concepts with the prefix cyber-..., in particular, the relationship between the terms information security and cybersecurity.*

Practical value: *from a practical point of view, this study is considered as a solution to a particular problem within the framework of the general problem of improving the training of personnel for internal affairs bodies.*

Keywords: *laws of dialectics, information security, cybernetics, cybersecurity, critical information infrastructure, meta-subjectivity, paradigm, conceptual apparatus, terminology*

References

1. *Gorbatov, Viktor S.; Erdniev, Aleksandr S. Sovershenstvovanie podgotovki kadrov po obespecheniju bezopasnosti informacionnoj infrastruktury organov vnutrennih del. IT Security, [S.l.], v. 31, no. 1, p. 100–119, 2024. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2024.1.06.*
2. *Devdariani N. V., Rubtsova E. V. Zakony dialektiki v jazyke. Baltic Humanitarian Journal. 2018, v. 7, no. 2(23), p. 31–34 – EDN XULTMD.*
3. *Markov A.S. Kiberbezopasnost' i Informacionnaja Bezopasnost' kak Bifurkacija Nomenklatury Nauchnyh Special'nostej. Issues of cybersecurity 2022, no. 1(47), p. 2–9 – EDN XMKFJH.*
4. *Stolyarov A. V. Informacionnaja svoboda i informacionnoe nasilie: special'nost' 09.00.11 «Social'naja filosofija»: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata filosofskih nauk, A. V. Stolyarov M. 2012 – 27 p.*
5. *Koryagin V. V. Informacionnaja real'nost': sushhnost' i osobennosti: special'nost' 09.00.11 «Social'naja filosofija»: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata filosofskih nauk. Ulan-Ude, 2018 – 25 p.*
6. *Mednyak I. A. Voennaja bezopasnost' sovremennogo obshhestva v uslovijah novoj informacionnoj real'nosti: special'nost' 5.7.7. «Social'naja i politicheskaja filosofija»: dissertacija na soiskanie uchenoj stepeni kandidata filosofskih nauk. Novocherkassk, 2022. – 160 p.*
7. *Dobrodeev A. Y. Kiberbezopasnost' v Rossijskoj Federacii. Modnyj termin ili prioritetnoe tehnologicheskoe napravlenie obespechenija nacional'noj i mezhdunarodnoj bezopasnosti XXI veka. Issues of cybersecurity. 2021, no. 4(44), p. 61–72. DOI: 10.21681/2311-3456-2021-4-61-72 – EDN MXUVBS.*
8. *Zhuikov A. E. Informacionnaja bezopasnost' v uslovijah genezisa virtual'nogo prostranstva transformirujushhegosja rossijskogo obshhestva: special'nost' 22.00.04 «Social'naja struktura, social'nye instituty i processy»: dissertacija na soiskanie uchenoj stepeni kandidata sociologicheskih nauk. Krasnodar, 2016. – 155 p.*
9. *Artamonova Ya. S. Informacionnaja bezopasnost' rossijskogo obshhestva: teoreticheskie osnovanija i praktika politicheskogo obespechenija: special'nost' 23.00.02 «Politicheskie instituty, processy i tehnologii»: avtoreferat dissertacii na soiskanie uchenoj stepeni doktora politicheskih. M., 2014. – 56 p.*
10. *Tulikov A. V. Informacionnaja bezopasnost' i prava cheloveka v uslovijah postindustrial'nogo razvitija (teoretiko-pravovoj analiz): special'nost' 12.00.01 «Teorija i istorija prava i gosudarstva; istorija uchenij o prave i gosudarstve»: avtoreferat dissertacii na soiskanie uchenoj stepeni kandidata juridicheskih nauk. M., 2017. – 24 p.*
11. *Mammadov E. F. Terminologija zakonodatel'stva ob informacii, informacionnyh tehnologijah i o zashhite informacii kak sredstvo obespechenija informacionnoj bezopasnosti. 2023, no. 1(30), p. 163–174. DOI: 10.25839/MATGIP_2023_1_163 – EDN NZVWLS.*
12. *Mnatsakanyan A. V. Informacionnaja bezopasnost' v Rossijskoj Federacii: ugolovno-pravovye aspekty: special'nost' 12.00.08 «Ugolovnoe pravo i kriminologija; ugolovno-ispolnitel'noe pravo»: avtoreferat na soiskanie uchenoj stepeni kandidata juridicheskih nauk. M., 2016. – 40 p.*
13. *Grigoriev A. N., Loktionov O. V., Druzhkina T. A. et al. Osnovy informacionnoj bezopasnosti v organah vnutrennih del: Uchebnik. SPb: Sankt-Peterburgskij universitet Ministerstva vnutrennih del Rossijskoj Federacii, 2019. – 312 p. – EDN SQGZCB.*
14. *Tolstoy Alexandr I. Sistematika ponjatij v oblasti informacionnoj bezopasnosti. IT Security (Russia), [S.l.], v. 30, no. 1, p. 130–148, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.*
15. *Gerasimenko V. A. Osnovy informacionnoj gramoty. M.: Energoatomizdat, 1996. – 320 p.*