ОСНОВЫ ТЕОРИИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ СЛОЖНЫХ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ

ГРИНЯЕВ СЕРГЕЙ НИКОЛАЕВИЧ

МОСКВА • 2026

Сергей Гриняев

Основы теории комплексной безопасности сложных социотехнических систем

https://litres.ru/74362288
SelfPub; 2026

Аннотация

Книга посвящена формированию основ теории комплексной безопасности сложных социотехнических систем. В работе безопасность рассматривается как способность системы сохранять критические функции, управляемость и потенциал восстановления при внутренних и внешних воздействиях. Предложен понятийный аппарат, включающий категории пространства, времени, системы, субъекта, цели, обстановки, ситуации, вызова, риска, угрозы, уязвимости и ущерба. Раскрыт механизм распространения гибридных угроз, возникающих в одном пространстве функционирования и реализующихся в другом либо нескольких взаимосвязанных пространствах. Проанализированы многосферные операции, гибридные конфликты и их значение для защиты российских объектов. Особое внимание уделено объектам ТЭК и ОПК, цифровому производству, критическим функциям,

каскадным рискам, технологической устойчивости и кадровому обеспечению. Книга адресована исследователям, специалистам по безопасности, инженерам, руководителям, преподавателям и обучающимся.

Содержание

Сергей Гриняев
Основы теории комплексной безопасности сложных социотехнических систем

Предисловие

Изменение характера угроз меняет требования к человеку, который отвечает за безопасность. На протяжении длительного времени безопасность развивалась как совокупность относительно самостоятельных профессиональных направлений. Инженер отвечал за надёжность оборудования и технологический режим. Специалист по защите информации обеспечивал устойчивость цифрового контура. Юрист контролировал соблюдение обязательных требований. Руководитель распределял полномочия, ресурсы и сроки. Такая специализация сохраняет своё значение, поскольку сложные объекты требуют глубоких знаний в каждой предметной области.

Однако современная реальность показывает, что опасные

процессы всё реже укладываются в границы одной профессиональной сферы. Воздействие может возникнуть в цифровой среде, проявиться в технологическом процессе, вызвать организационные затруднения, привести к экономическим потерям и затронуть социальную устойчивость. Нарушение связи способно лишить персонал своевременной информации. Недостоверные данные могут привести к ошибочному управленческому решению. Ошибка в решении способна изменить параметры технологического процесса. Далее возникает риск отказа оборудования, остановки производства, нарушения договорных обязательств или ущерба для людей и окружающей среды.

В этих условиях безопасность перестаёт быть суммой отдельных защитных мероприятий. Она становится способностью сложной системы сохранять критические функции, поддерживать управляемость и восстанавливать требуемое состояние после нарушения. Эта способность определяется согласованностью технических средств, цифровой инфраструктуры, кадровых компетенций, организационных процедур, правовых норм и ресурсных резервов. Если хотя бы один из этих элементов выпадает из общей системы управления, создаётся уязвимость, которая может проявиться далеко за пределами первоначального источника проблемы.

Именно поэтому современная угроза всё чаще приобретает гибридный характер. В настоящей книге гибридной называется угроза, которая зарождается в одном простран-

стве функционирования объекта, а реализуется в другом или нескольких пространствах одновременно. Она использует связи между техническими, информационными, кадровыми, ресурсными, организационными и социальными контурами. Её опасность определяется не только силой первоначального воздействия, но и тем, насколько система способна распознать это воздействие, локализовать его последствия и сохранить управление.

Например, нарушение цифрового контура может проявиться как изменение данных, потеря связи, ошибка в настройке программного обеспечения или ограничение доступа к системе управления. Само по себе такое событие относится к информационному пространству. Однако его последствия могут перейти в техническое пространство через неверные действия оператора, нарушение режима работы оборудования или снижение качества контроля. Далее последствия способны затронуть организационное и ресурсное пространства: потребуется перераспределение персонала, изменение производственного графика, использование резервов, привлечение подрядчиков и принятие решений в условиях дефицита времени.

Обратная последовательность также возможна. Кадровая проблема может выглядеть как локальная задача подбора или обучения персонала. При этом дефицит опытных специалистов способен привести к снижению качества технического обслуживания, накоплению неустранённых дефектов,

ухудшению состояния оборудования и росту вероятности аварийной ситуации. Угроза возникла в кадровом пространстве, однако реализовалась через технические, технологические, организационные и экономические последствия.

Исследования гибридных конфликтов подчёркивают, что современные воздействия могут соединять информационные, экономические, правовые, кибернетические, политические и силовые инструменты, использовать критические уязвимости и затруднять своевременное принятие защитных решений. Для специалиста по безопасности этот вывод имеет прикладное значение. Ему необходимо видеть не только отдельный инцидент, но и последовательность его возможного развития: источник воздействия, уязвимость объекта, нарушение функции, распространение последствий и вероятный ущерб.

Такой подход требует формирования нового профессионального облика специалиста. Этот специалист не должен заменять инженера, программиста, технолога, юриста, экономиста или руководителя. Он должен быть способен понимать взаимосвязи между их областями деятельности. Его задача заключается в том, чтобы собрать разнородные сведения в единую картину, определить критические функции объекта, выявить опасную динамику и подготовить обоснованное решение для субъекта управления.

Специалист в области комплексной безопасности должен уметь определять границы объекта защиты, устанавливать

его критические функции и выделять параметры, по которым можно судить о состоянии этих функций. Он должен видеть зависимость между техническим состоянием оборудования, качеством данных, кадровой обеспеченностью, ресурсными резервами и порядком принятия решений. Он должен уметь распознавать общие точки отказа, когда один компонент, поставщик, канал связи, носитель знаний или программное средство одновременно обеспечивает несколько значимых функций.

Особую роль приобретает способность работать с данными. Современные объекты формируют большие объёмы технической, производственной, организационной и информационной информации. Однако накопление данных само по себе не повышает безопасность. Данные становятся основой управления только тогда, когда определены их источники, качество, своевременность, достоверность и связь с конкретными действиями. Специалист должен понимать, какие параметры следует контролировать, какие отклонения имеют значение, какова скорость опасного процесса и сколько времени остаётся для реакции.

Исходные материалы, положенные в основу настоящей книги, связывают развитие теории комплексной безопасности с подготовкой двух взаимосвязанных профессиональных направлений: специалиста-аналитика в области комплексной безопасности и специалиста по моделированию, сбору и анализу данных цифрового следа. Первый формирует це-

лостное представление об объекте, его угрозах, уязвимостях, рисках и критических функциях. Второй создаёт аналитическую основу для мониторинга, моделирования и оценки динамики параметров. Их совместная работа позволяет соединить содержательный анализ с цифровыми средствами наблюдения и принятия решений.

Изменение характера угроз требует изменения образовательной системы. Подготовка кадров не может ограничиваться освоением нормативных требований, типовых алгоритмов и набора технических средств. Она должна формировать способность действовать в условиях неопределённости, неполной информации, ограниченных ресурсов и распределённой ответственности. Для этого необходимы практические занятия, моделирование сценариев, анализ инцидентов, междисциплинарные тренировки и разбор принятых решений.

В процессе обучения особое внимание должно уделяться слабым сигналам опасности. К ним относятся постепенное ухудшение технических параметров, рост числа малозаметных ошибок, сокращение резервов, перегрузка персонала, задержки в передаче информации, накопление неисполненных мероприятий и зависимость критических функций от единственного источника. Каждый из этих признаков может казаться несущественным при отдельном рассмотрении. В совокупности они способны свидетельствовать о снижении устойчивости системы и приближении опасной ситуа-

ции.

Цифровая грамотность становится обязательной частью подготовки. Специалист должен владеть основами работы с корпоративными системами, данными, электронными таблицами, базами данных и средствами аналитической обработки. В учебных материалах по экономической и информационно-технологической безопасности предусматривается знакомство с системами управления ресурсами и производством, а также со средствами обработки данных, включая SQL, Python, R и Matlab. Однако инструментальная подготовка должна быть подчинена содержательной задаче. Любая цифровая модель полезна только тогда, когда специалист понимает объект, цели управления, ограничения данных и последствия решения.

Эта книга адресована тем, кто участвует в проектировании, эксплуатации, управлении и защите сложных социотехнических систем. Она предназначена для специалистов по безопасности, инженеров, технологов, аналитиков, руководителей, преподавателей, исследователей и обучающихся. Её назначение состоит в формировании общего языка, который позволит представителям разных профессий совместно описывать объект, выявлять угрозы, оценивать риски и поддерживать критические функции.

Безопасность сложного объекта определяется качеством людей, которые способны видеть систему целиком. Они должны понимать, что угроза может возникнуть в одной

сфере, проявиться в другой и реализоваться через цепочку взаимосвязанных последствий. Подготовка таких специалистов является необходимым условием устойчивости государства, общества и экономики Российской Федерации в условиях технологической сложности, внешнего давления и возникающей неопределённости.

Введение

Безопасность в XXI веке определяется устойчивостью сложных систем, от которых зависят жизнедеятельность общества, функционирование государства, обороноспособность страны и развитие экономики. К таким системам относятся энергетическая и транспортная инфраструктура, объекты оборонно-промышленного комплекса, цифровые платформы, системы связи, производственные кооперации, территориальные комплексы и органы управления. Они соединяют технические средства, людей, данные, организационные процедуры, правовые нормы, ресурсы и отношения с внешней средой.

Усложнение объектов сопровождается ростом числа взаимосвязей. Цифровизация увеличивает скорость управления и объём доступных данных. Одновременно она создаёт зависимость от программного обеспечения, сетей связи, данных, поставщиков компонентов и квалификации персонала. Нарушение одного элемента может передаваться по цепочке зависимостей и приводить к последствиям, значительно превосходящим масштаб исходного события. В зарубежных документах по комплексным катастрофам, например, нарушение энергосистемы вследствие кибератаки рассматривается как фактор каскадных отказов критической инфраструктуры и ограничения возможностей самого реагирования.

В этих условиях представление о безопасности как о наборе самостоятельных направлений — физической, промышленной, информационной, пожарной, экологической и иных — оказывается недостаточным. Каждое направление сохраняет собственный предмет и методы, однако их раздельное применение не гарантирует целостной защищённости объекта. Угроза, возникшая в цифровом контуре, может приобрести технологические, экономические, социальные и правовые последствия. Ошибка в организационном решении способна усилить техническую неисправность. Дефицит кадров может уменьшить качество обслуживания, снизить наблюдаемость состояния и увеличить вероятность аварийного развития ситуации.

Следовательно, требуется теория, которая позволяет описывать объект как целостную социотехническую систему, выявлять взаимосвязи между его элементами и управлять безопасностью через сохранение критических функций. Настоящая монография посвящена построению такой теории.

Проблема и предмет книги

Понятие безопасности развивалось вместе с обществом. В этом развитии прослеживается переход от более простых представлений о защите к сложным моделям, включающим многочисленные факторы, а также движение от общих категорий к специализированным видам безопасности. Исход-

ные материалы к теории комплексной безопасности подчёркивают эту двойную динамику: от простого к сложному и от универсального к специальному.

Современное употребление термина «комплексная безопасность» часто сводится к перечислению частных видов безопасности, относимых к одному объекту. Такой подход удобен для распределения полномочий и выполнения нормативных процедур. Однако он не отвечает на главный вопрос: каким образом определить, достаточно ли совокупность мер защищает объект как целостную систему. Перечень мер ещё не образует теорию. Для построения теории необходимы понятия объекта, субъекта управления, цели, состояния, среды, угрозы, уязвимости, ущерба, риска и управленческого воздействия.

Предметом книги является комплексная безопасность сложных социотехнических объектов. Под такими объектами понимаются системы, в которых люди, техника, цифровые средства, организационные правила, ресурсы и данные образуют взаимосвязанную структуру, выполняющую общественно значимые функции. Объект рассматривается во времени, в конкретной среде и относительно целей субъекта управления.

Методологическая позиция

Монография исходит из необходимости сформировать

эффективную теорию комплексной безопасности. В данном контексте эффективная теория понимается как методологический каркас, который позволяет моделировать и объяснять наблюдаемые процессы без стремления исчерпывающе описать все детали каждого физического, социального, технического или экономического явления. Такой подход прямо сформулирован в исходных материалах как основа построения теории комплексной безопасности.

В центре предлагаемой модели находится **субъект управления**. Именно субъект является носителем потребностей, источником целей и организатором управленческих воздействий. Без определения субъекта невозможно установить, какие функции объекта являются критическими, какие параметры должны поддерживаться в допустимом диапазоне, какой ущерб признаётся неприемлемым и какие меры могут считаться достаточными.

Система описывается через пространства функционирования. Техническое пространство включает параметры оборудования, инфраструктуры и технологических процессов. Информационное пространство отражает состояние данных, связи, программных комплексов и цифровых контуров. Правовое пространство связано с обязательными требованиями, разрешениями, полномочиями и ответственностью. Кадровое, ресурсное, организационное, экономическое, социальное и экологическое пространства описывают другие стороны состояния объекта. Их объединение образует суперпро-

странство, в котором оценивается целостная устойчивость системы.

Состояние объекта в момент времени может быть представлено набором параметров:

$$x(t) = \{X_1'(t), X_2'(t) \dots X_N(t)\}.$$

Требуемое состояние определяется субъектом управления с учётом целей, норм, ресурсов и условий среды:

$$x^*(t) = \{X_1^{*'}(t), X_2^{*'}(t) \dots X_N^*(t)\}.$$

Задача комплексной безопасности состоит в наблюдении динамики отклонений

$$\Delta x(t) = x(t) - x^*(t),$$

выявлении причин этих отклонений, прогнозировании последствий и организации управленческих воздействий, удерживающих критически значимые параметры в допустимых пределах.

Внешний контекст

Необходимость развития отечественной теории определяется также изменением характера современного противоборства. Концепция многосферных операций, развиваемая армией США, связывает достижение стратегических целей с быстрым и непрерывным объединением возможностей в наземной, морской, воздушной, космической, кибернетической, электромагнитной и информационной средах. Её ключевым механизмом выступает конвергенция, направленная на создание преимуществ и воздействие на уязвимости системы противника.

Исследования гибридных конфликтов дополняют эту картину. В них рассматривается согласованное применение дипломатических, информационных, экономических, правовых, кибернетических и военных инструментов для достижения политических целей. Такие действия могут быть распределены во времени, затруднять установление источника воздействия и использовать критические уязвимости общества, инфраструктуры и системы управления.

Для Российской Федерации этот контекст требует самостоятельного теоретического ответа. Он не состоит в зеркальном воспроизведении западных доктринальных конструкций. Теория комплексной безопасности строится вокруг защищаемого объекта и его способности сохранять

жизненно важные функции. Её исходная задача заключается в поддержании управляемости, технологической устойчивости, кадровой воспроизводимости, защищённости информационных контуров, устойчивости кооперационных связей и потенциала восстановления.

Цель и задачи

Цель монографии состоит в разработке теоретических положений комплексной безопасности сложных социотехнических объектов и в формировании методологической основы для их практического применения в интересах Российской Федерации.

Для достижения этой цели решаются следующие задачи:

1. Сформировать понятийный аппарат теории комплексной безопасности;
2. Обосновать представление о защищаемом объекте как о сложной социотехнической системе;
3. Раскрыть роль субъекта управления, целей и критических функций в определении безопасности;
4. Описать пространства функционирования, суперпространство и параметры состояния объекта;
5. Систематизировать понятия обстановки, ситуации, вызова, риска, угрозы, уязвимости и ущерба;
6. Раскрыть безопасность и опасность как динамические характеристики состояния и управляемости системы;

7. Проанализировать западные концепции многосферных операций и гибридных конфликтов как внешний контекст развития теории;

8. Сформулировать положения теории комплексной безопасности как российского подхода к защите сложных объектов;

9. Показать особенности применения теории к объектам топливно-энергетического и оборонно-промышленного комплексов;

10. Определить требования к кадровому и образовательному обеспечению комплексной безопасности.

Научная и практическая значимость

Научная значимость работы состоит в объединении философских, системных, кибернетических, математических, организационных и прикладных представлений в единой модели безопасности. Эта модель позволяет перейти от фрагментированного описания частных угроз к анализу состояния сложного объекта, его функций, связей, целей и потенциала восстановления.

Практическая значимость заключается в возможности применять положения теории для формирования моделей защищаемых объектов, разработки систем мониторинга, построения цифровых двойников, анализа каскадных рисков, оценки критических зависимостей, подготовки сценариев

реагирования и обучения специалистов. Исходные материалы связывают развитие теории с подготовкой специалистов-аналитиков комплексной безопасности и специалистов по моделированию, сбору и анализу данных цифрового следа.

Книга адресована исследователям, преподавателям, специалистам по безопасности, инженерам, руководителям предприятий, государственным служащим, аналитикам, разработчикам цифровых систем и обучающимся по направлениям безопасности, управления, технических наук и системного анализа. Её содержание рассчитано на читателя, который стремится понимать безопасность не как совокупность формальных требований, а как способность сложной системы сохранять цели, критические функции и управляемость в условиях неопределённости, внешнего давления и технологической сложности.

Часть I. Теоретико-методологические основания

Глава 1. Введение в проблему комплексной безопасности

1.1. Эволюция понятия безопасности

Понятие безопасности развивалось вместе с развитием общества, и это развитие никогда не было равномерным или однонаправленным. В этом процессе прослеживались две встречные тенденции: движение «от простого к сложному» и движение «от универсального к специальному». Первая тенденция отражала постепенное увеличение числа факторов, учитываемых при оценке защищённости объекта: если на ранних этапах развития общества опасность связывалась главным образом с прямым физическим воздействием, то со временем в поле зрения теории и практики безопасности попали экономические, информационные, экологические и социальные аспекты существования объекта. Вторая тенденция, напротив, отражала процесс дробления единого

представления о безопасности на множество специализированных направлений, каждое из которых обслуживало конкретную отрасль, конкретный тип объекта или конкретный вид деятельности. Обе тенденции действовали одновременно, порождая противоречие между стремлением к целостному описанию явления и практической потребностью в узкоспециализированных решениях.

Содержание понятия **«безопасность»** на разных исторических этапах определялось интересами конкретных сторон, а не объективными характеристиками защищаемого объекта. Его практическое применение прошло долгий путь: от произвольного использования силы, подчинённого принципу «сильный всегда прав», через постепенное утверждение обычая как регулятора общественных отношений, к провозглашению верховенства закона в сфере применения насилия. На каждом из этих этапов менялся не только механизм обеспечения безопасности, но и сам субъект, наделённый правом определять, что является угрозой и какие меры защиты являются допустимыми. Разным странам, регионам и общественно-экономическим формациям присущи собственные особенности обеспечения безопасности, что придаёт самому понятию безопасности выраженный субъективный характер. Это обстоятельство имеет прямое отношение к задаче формирования национальной теории комплексной безопасности: любая теория безопасности неизбежно отражает интересы того субъекта, который её формулирует, и по-

пытка построить универсальную, лишённую национальной специфики теорию безопасности методологически несостоятельна.

Из сказанного следует важный вывод для дальнейшего изложения. Поскольку понятие безопасности исторически формировалось под влиянием интересов конкретных субъектов, задача построения теории комплексной безопасности предполагает явное определение того субъекта, чьи интересы данная теория обслуживает, и того объекта защиты, применительно к которому она разрабатывается. Без такого явного определения теория рискует остаться абстрактной конструкцией, оторванной от практических задач обеспечения национальной безопасности.

1.2. Критика существующих подходов к комплексной безопасности

Словосочетание «комплексная безопасность» уже многократно использовано в отечественной научной и методической литературе, что создаёт определённую терминологическую инерцию. Наиболее распространённые подходы к его определению исходят, в первую очередь, из документов Министерства по чрезвычайным ситуациям и рассматривают комплексную безопасность как совокупность отдельных видов безопасности — пожарной, экологической, промышленной, антитеррористической и других — объединённых по

формальному признаку принадлежности к одному защищаемому объекту[1]. Такой подход удобен с точки зрения нормативного регулирования: каждому виду безопасности соответствует собственный набор требований, стандартов и контролирующих органов, а задача обеспечения комплексной безопасности сводится к одновременному выполнению всех этих требований.

Однако данный подход обладает существенной методической слабостью. Явление или понятие корректно определять через его собственное содержание, раскрывающее внутреннюю природу описываемого феномена, а не через перечисление того, чем оно не является, и не через простое суммирование смежных категорий. Определение комплексной безопасности как суммы частных видов безопасности оставляет без ответа ключевой вопрос: что именно делает совокупность разрозненных мер целостной системой, а не случайным набором независимых процедур? Из такого суммирующего определения невозможно вывести критерий достаточности принимаемых мер защиты, поскольку сумма частных видов безопасности не порождает нового качества, отсутствующего у каждого из слагаемых по отдельности. Иными словами, простое объединение пожарной, экологической и промышленной безопасности под одной вывеской не со-

---

[1] **Сергеев, А. А.** Комплексная безопасность объектов: теория, методология, практика : монография / А. А. Сергеев, И. В. Громов. – Москва : Техносфера, 2020. – 312 с. – ISBN 978-5-94836-582-4.

здаёт «комплексности» в строгом теоретическом смысле — оно лишь удобно с точки зрения административного управления, но не решает задачи целостного описания защищённости объекта как единой системы.

При этом следует признать: альтернативного термина, столь же точно и ёмко описывающего рассматриваемую когнитивную модель защищённости сложного объекта, в русском научном языке на сегодняшний день не найдено. Отказ от использования уже закрепившегося в литературе термина потребовал бы введения нового слова, что создало бы дополнительный барьер для восприятия теории профессиональным сообществом. Поэтому задача настоящей работы состоит не в замене термина «комплексная безопасность» новым словом, а в наполнении уже существующего термина иным, методологически более строгим содержанием, опирающимся на точный понятийный аппарат, а не на административное перечисление частных видов безопасности.

1.3. Комплексная безопасность как эффективная теория

Для решения поставленной задачи применяется методологический приём, заимствованный из теоретической физики. Эффективная теория в физике представляет собой каркас, созданный для моделирования определённых наблюдаемых явлений без необходимости детального описания всех

лежащих в их основе фундаментальных процессов. Классическим примером эффективной теории служит термодинамика: она успешно описывает поведение газа через макроскопические параметры — давление, объём, температуру — не обращаясь к описанию траекторий отдельных молекул. Именно такой методологический ход предлагается применить и к описанию комплексной безопасности сложных социотехнических объектов.

Применительно к рассматриваемой теории этот приём означает следующее. Теория не претендует на исчерпывающее объяснение всех физических, технических, экономических и социальных процессов, протекающих внутри защищаемого объекта и его окружения. Вместо этого она предлагает единый понятийный и математический аппарат, позволяющий описывать состояние объекта в целом, динамику развития угроз в его отношении и эффективность принимаемых защитных мер через ограниченный набор измеримых параметров. Такая экономия описательных средств не является недостатком теории — напротив, она является необходимым условием практической применимости теории для целей мониторинга, прогнозирования и управления.

Реализация подобного подхода требует введения ряда базовых категорий с точностью, допускающей их дальнейшее использование при построении цифровых моделей защищаемых объектов. К числу таких категорий относятся пространство, время, система, субъект. Каждая из этих катего-

рий получает в рамках теории собственное строгое определение, отличное от бытового или сугубо философского понимания соответствующего термина, но сохраняющее связь с его исходным смысловым содержанием.

Особое значение в этом ряду категорий имеет рассмотрение сложного объекта как социотехнической системы. Такое рассмотрение имеет принципиальное методологическое значение: оно позволяет ввести понятие субъекта как источника целеполагания, без которого невозможно определить критерий достаточности обеспечиваемой безопасности. Технический объект сам по себе не обладает целями — цели возникают у субъекта, который этим объектом управляет или в интересах которого объект функционирует. Цели субъекта возникают под давлением потребностей, связанных с его жизнедеятельностью и взаимодействием со средой и объектом управления. Именно наличие субъекта с его потребностями и целями превращает абстрактную задачу защиты технической системы в содержательную задачу обеспечения безопасности в интересах конкретного носителя целей — будь то отдельное предприятие, отрасль или государство в целом.

1.4. Внешний контекст: многосферное противостояние

Формирование национальной теории комплексной безопасности происходит не в изоляции от общемирового кон-

текста развития военной и невоенной мысли, а в прямом диалоге — и в определённой мере в противостоянии — с концепциями, развиваемыми ведущими зарубежными военными структурами. Армия США развивает концепцию многосферных операций, охватывающую взаимодействие в сферах суши, моря, воздуха, космоса, киберпространства и информационного пространства[2]. Согласно этой концепции, эффективность военного противостояния определяется не превосходством в отдельной сфере, а способностью синхронизировать действия одновременно во всех перечисленных сферах, создавая для противника ситуацию, в которой преимущество в одной области нейтрализуется уязвимостью в другой.

Прогнозируемая операционная среда до 2034 года описывается западными военными аналитиками как пространство непрерывного стратегического соперничества, в котором грань между войной и миром размывается, а конкуренция ведётся практически постоянно, переходя в открытые крупномасштабные боевые действия лишь на отдельных этапах этого непрерывного противостояния[3]. Параллельно с развитием доменной логики многосферных опе-

---

[2] Operations : Field Manual No. 3-0 / Department of the Army. – Washington, DC : Headquarters, Department of the Army, 2022. – 280 p.

[3] International humanitarian law and the challenges of contemporary armed conflicts. – URL: http://international-review.icrc.org/articles/reports-and-documents-ihl-and-the-challenges-of-contemporary-armed-conflicts-927 (дата обращения: 23.08.2026).

раций развивается отдельное направление — когнитивная война, рассматривающая человеческое сознание, индивидуальное и коллективное, как самостоятельную сферу воздействия, наравне с традиционными физическими сферами. В рамках этого направления объектом воздействия становится не столько материальная инфраструктура противника, сколько его система восприятия реальности, принятия решений и формирования общественного мнения.

Гибридные конфликты характеризуются рядом западных исследовательских центров как «новая нормальность» международных отношений — то есть не как временное отклонение от привычной модели межгосударственного взаимодействия, а как устойчивая и, по всей видимости, долгосрочная форма ведения противостояния[4]. В рамках этой модели военные, экономические, информационные и киберинструменты применяются в сочетании друг с другом, причём отдельные элементы такого воздействия могут не достигать порога, формально классифицируемого как акт войны, но в своей совокупности создавать для противника ощутимый стратегический ущерб.

Перечисленные концепции формируют целостную доктринальную рамку, в рамках которой противостояние ведётся одновременно во всех перечисленных сферах, а объек-

[4] **Sweijs, T.** Hybrid conflicts: the new normal? / T. Sweijs, S. De Spiegeleer, J. Van Metre [et al.] ; The Hague Centre for Strategic Studies (HCSS) ; Netherlands Organisation for Applied Scientific Research (TNO). – The Hague : HCSS, 2019. – 156 p.

том воздействия становится не только территория, вооружённые силы или инфраструктура противника, но и его система принятия решений, общественное сознание и способность к организованному сопротивлению. Российская теория комплексной безопасности сложных социотехнических объектов формулируется именно как самостоятельный ответ на этот вызов. Принципиально важно, что этот ответ не сводится к копированию доменной структуры западной доктрины путём простого перевода понятия «домен» в понятие «сфера» — такой перевод оставил бы неизменной саму логику построения теории, заимствованную у иностранного первоисточника. Вместо этого предлагается собственный понятийный аппарат: пространства функционирования объекта, суперпространство объекта, субъект управления и его цели. Этот аппарат строится вокруг объекта защиты и его субъекта, а не вокруг перечня сфер противостояния, что меняет саму логику построения теории защищённости — от логики симметричного ответа на каждую сферу воздействия противника к логике целостного описания состояния защищаемого объекта независимо от того, из какой сферы исходит конкретное деструктивное воздействие.

1.5. Задачи и структура последующего изложения

Настоящая работа решает несколько взаимосвязанных за-

дач. Первая задача — определение границ и общих подходов к пониманию сущности комплексной безопасности, свободное от административного суммирования частных видов безопасности. Вторая задача — описание отраслей знания, необходимых для создания и эксплуатации систем обеспечения комплексной безопасности сложных объектов, поскольку построение подобной теории требует привлечения философии, кибернетики, теории систем и разделов прикладной математики. Третья задача — формирование представления о компетенциях специалистов, занятых в области обеспечения комплексной безопасности, поскольку любая теория, не находящая практического воплощения в подготовке кадров, остаётся сугубо академической конструкцией.

Изложение материала строится последовательно, без разрывов в цепочке рассуждений. Сначала рассматриваются философско-математические основания описания сложного объекта — категории пространства, суперпространства и времени, необходимые для точного описания состояния объекта в каждый момент его существования. Затем на основе этих оснований вводятся понятия ситуации, вызова, риска, угрозы и уязвимости, раскрывающие механизм зарождения и развития опасности для объекта. Далее эти понятия объединяются в итоговое определение самой комплексной безопасности и в описание практической деятельности по её обеспечению. Такая последовательность соответствует логике движения «от простого к сложному», отмеченной в нача-

ле настоящей главы, и обеспечивает методологическую строгость всех последующих разделов книги: каждое новое понятие вводится только после того, как определены все понятия, необходимые для его строгого формулирования.

Глава 2. Философско-математические основания описания сложных систем

2.1. Назначение философско-математического аппарата

Теория комплексной безопасности требует языка, который позволяет последовательно описывать защищаемый объект, его среду, изменения его состояния и действия субъекта управления. Обыденный язык пригоден для первоначального указания на проблему, однако он допускает неоднозначность терминов. В практической работе такая неоднозначность ведёт к различному пониманию объекта защиты, угроз, критериев ущерба и состава защитных мероприятий. Поэтому понятийный аппарат комплексной безопасности должен соединять философские категории, кибернетические представления об управлении, системный анализ и методы математического моделирования.

Философия необходима для раскрытия исходного смысла

категорий пространства, времени, системы, причины, цели и изменения. Кибернетика задаёт представление об объекте управления, субъекте управления, управляющем воздействии и обратной связи. Теория систем позволяет рассматривать объект как целостность, обладающую структурой, функциями и границами. Математический аппарат обеспечивает возможность количественного описания состояния объекта и динамики его параметров. Совокупность этих подходов образует методологическую основу для построения цифрового двойника сложного социотехнического объекта.

Под **цифровым двойником** в настоящей работе понимается формализованное информационное описание объекта, его структуры, параметров, связей со средой и возможных траекторий изменения состояния. Цифровой двойник не является механической копией реального объекта. Его назначение состоит в том, чтобы отразить только те свойства, связи и процессы, которые существенны для поставленной управленческой задачи. Для задач комплексной безопасности это означает необходимость фиксировать параметры, определяющие устойчивость функционирования объекта, его уязвимости, источники угроз, последствия нарушений и доступные меры противодействия.

Сложный объект существует одновременно в нескольких взаимосвязанных областях деятельности. Производственное предприятие действует в физическом, техническом, технологическом, правовом, экономическом, информационном,

кадровом, экологическом и социальном пространствах. Его безопасность не может быть корректно оценена через состояние только одного из этих пространств. Нормальная работа оборудования при нарушении правовых требований, утрате управляемости персоналом, разрушении информационного контура или критическом ухудшении финансового положения не свидетельствует о безопасном состоянии объекта в целом. Следовательно, теория должна располагать средствами для совместного рассмотрения разнородных параметров без утраты содержательной связи между ними.

2.2. Пространство как форма описания состояния

Понятие **пространства** относится к числу фундаментальных категорий человеческого мышления. Оно используется для описания множественности предметов, объектов, явлений и данных, одновременно присутствующих в восприятии и деятельности человека. В естественных науках пространство традиционно связывается с протяжённостью материальных тел и возможностью определить их положение. В математике понятие пространства получило более широкий смысл: пространством может считаться совокупность элементов, для которой заданы правила различения элементов, способы измерения расстояний между ними и допустимые операции перехода от одного состояния к другому.

Для теории комплексной безопасности важна именно эта расширенная трактовка. Она позволяет описывать пространственно не только физическое расположение объектов, но и их положение в системе правовых норм, технологических регламентов, финансовых показателей, информационных процессов и социальных отношений. Такое использование термина не означает отождествления разных предметных областей. Оно означает применение общей процедуры: для каждой области определяются наблюдаемые параметры, способы их измерения, диапазоны допустимых значений и правила интерпретации изменения этих значений.

Пространством функционирования объекта далее называется упорядоченная совокупность параметров, характеризующих состояние объекта в определённой предметной области, вместе с правилами измерения, сравнения и интерпретации этих параметров. Для каждого пространства должны быть определены:

- состав параметров;
- единицы измерения или шкалы оценивания;
- исходная точка отсчёта;
- допустимые диапазоны значений;
- правила выявления отклонений;
- связь параметров с целями управления и критериями безопасности.

Например, техническое пространство производственного объекта может включать параметры вибрации, температу-

ры, давления, износа, пропускной способности, исправности датчиков и готовности резервных систем. В правовом пространстве параметрами выступают действующие обязательные требования, разрешительные документы, сроки их действия, результаты проверок, наличие предписаний и факты исполнения установленных обязанностей. В информационном пространстве значимы доступность данных, целостность информационных массивов, достоверность сообщений, состояние средств связи, права доступа и устойчивость контуров управления.

Каждое пространство описывает объект с определённой стороны. Однако один и тот же объект не распадается на независимые части только потому, что его параметры измеряются разными средствами. Отказ технического оборудования может инициировать производственное нарушение, вызвать экономический ущерб, повлечь правовые последствия, изменить общественное восприятие организации и создать нагрузку на органы управления. Следовательно, пространственное описание необходимо сочетать с представлением о взаимосвязях между пространствами.

2.3. Координатные оси, состояние и метрика

Для математического описания пространство задаётся совокупностью точек. Каждая точка соответствует определённому состоянию объекта. Положение точки определяется

значениями параметров, выступающих координатными осями данного пространства. В теории комплексной безопасности координатная ось представляет собой параметр, который характеризует значимое свойство объекта и допускает измерение либо упорядоченное оценивание.

Если состояние объекта в выбранном пространстве определяется параметрами, оно может быть представлено вектором:

$$x = \{X_1, X_2, \ldots, X_N\},$$

Где $X_1, X_2, \ldots, X_N$ — значения параметров объекта, а — размерность пространства. Такой вектор не заменяет реальный объект. Он представляет его формализованное описание, применимое для анализа состояния в конкретной предметной области.

Например, состояние технического участка может быть задано набором параметров:

$$x_{\text{тех}} = \{T, P, V, W, R\},$$

где — температура критического узла; — давление в си-

стеме; — уровень вибрации; — показатель износа; — готовность резервного оборудования. В рамках конкретной модели набор параметров может расширяться или сокращаться. Выбор определяется целями управления, доступностью данных и характером угроз.

Размерность пространства показывает число параметров, используемых для описания состояния. С ростом размерности повышается детализация модели. Одновременно возрастает объём данных, необходимый для её наполнения, усложняются вычисления и растёт риск включения слабосвязанных либо плохо интерпретируемых показателей. В материалах к теории комплексной безопасности данная проблема связывается с известным в математическом моделировании «проклятием размерности»: увеличение количества координат может приводить к резкому росту сложности анализа и потребности в исходных данных. Поэтому набор параметров должен быть достаточным для решения конкретной задачи, но не избыточным.

Для сопоставления двух состояний необходимо определить метрику пространства, то есть правило измерения различия между точками. В простейшем случае расстояние между состояниями и описывается выражением:

$$d(x_1, x_2) = \sqrt{\sum_{i=1}^{N} (X_i^2 - X_i^1)^2}.$$

Практическое значение метрики состоит в возможности оценить величину изменения состояния объекта. Однако прямое применение этой формулы в задачах безопасности обычно ограничено. Параметры имеют разные единицы измерения, различную критичность и неодинаковую связь с ущербом. Поэтому перед объединением параметров в единую метрику требуется нормирование показателей, введение весов и обоснование пороговых значений. Такие операции должны опираться на данные мониторинга, нормативные требования, результаты экспертиз и анализ конкретных сценариев, а не на произвольные допущения.

2.4. Время, процесс и динамика

Описание состояния объекта без учёта времени является неполным. Время выражает последовательность смены состояний материальных систем и процессов. Для задач комплексной безопасности важно фиксировать не только значение параметра в отдельный момент, но и направление, ско-

рость, устойчивость и обратимость его изменения. Один и тот же показатель может находиться в допустимом диапазоне, однако его быстрая отрицательная динамика способна свидетельствовать о приближении опасной ситуации.

Время в модели сложного объекта может рассматриваться в двух аспектах. Первый аспект связан с внешним временем: календарной последовательностью событий, сменой режимов работы, сроками действия нормативных документов, периодичностью контроля, сезонными и иными внешними факторами. Второй аспект относится к внутреннему времени объекта: сроку службы оборудования, циклу технологических процессов, стадии жизненного цикла проекта, накоплению износа, деградации ресурсов и развитию внутренних конфликтов. Эти аспекты не тождественны, однако оба должны учитываться при оценке безопасности.

Динамика состояния означает изменение параметров объекта во времени. Если в момент объект находился в состоянии

$$x(t_1) = \{X_1'(t_1), X_2'(t_1) \dots X_N(t_1)\},$$

а в момент — в состоянии

$$x(t_2) = \{X_1'(t_2), X_2'(t_2) \dots X_N(t_2)\},$$

то изменение состояния может быть представлено вектором:

$$\Delta x = x(t_2) - x(t_1).$$

Такой вектор показывает, какие параметры изменились, в какую сторону и насколько. В прикладной системе мониторинга он может служить основой для выявления отклонений от установленной траектории функционирования. Однако оценка опасности не сводится к величине отклонения. Требуется учитывать контекст: допустимые пределы, взаимное влияние параметров, скорость развития процесса, наличие резервов, управляемость ситуации и возможность восстановления требуемого состояния.

Существенную роль играет явление «дрейфа нуля». Под ним понимается изменение исходного состояния объекта по отношению к первоначальной точке отсчёта. В технической сфере дрейф может быть вызван старением оборудования, накоплением погрешностей измерения или изменением условий эксплуатации. В правовой сфере он возникает вследствие изменения законодательства, появления

новых обязательных требований или пересмотра практики контроля. В организационной сфере дрейф связан с изменением кадрового состава, распределения полномочий, компетенций и условий принятия решений. Следовательно, модель комплексной безопасности должна предусматривать регулярный пересмотр исходных параметров, порогов и критериев оценки.

2.5. Суперпространство сложного объекта

Сложный социотехнический объект функционирует в совокупности пространств. Для их совместного описания вводится понятие **суперпространства**. Суперпространством называется объединение нескольких пространств, необходимых для анализа заданного объекта. В суперпространстве состояние объекта представляется расширенным набором параметров, принадлежащих различным предметным областям.

Если техническое пространство имеет размерность , а правовое — размерность , то их объединение образует пространство размерностью, не превышающей :

$$L \leq N + M.$$

Неравенство имеет принципиальное значение. Одни и те же свойства объекта могут получать отражение в нескольких пространствах. Например, состояние системы автоматического контроля относится одновременно к технической, информационной и правовой областям. Введение отдельной координаты для каждого повторяющегося описания создаст искусственную избыточность модели. Поэтому при формировании суперпространства требуется выявлять совпадающие показатели, устанавливать их смысловую связь и определять, в каком виде они будут использоваться в интегральной модели.

Для защищаемого объекта суперпространство может включать следующие пространства: физическое, техническое, технологическое, информационное, экономическое, кадровое, правовое, экологическое и социальное. Такой перечень не является универсальным и не должен механически применяться к каждому объекту. Его состав зависит от масштаба объекта, характера выполняемых функций, критичности последствий нарушения его работы, условий внешней среды и поставленной аналитической задачи.

Суперпространство не следует понимать как абстрактную сумму всех возможных данных. Его назначение состоит в том, чтобы выявить связи между параметрами, которые в узкоспециализированном анализе остаются разобщёнными. Например, техническая неисправность оборудования может быть обнаружена по данным датчиков. Однако ре-

шение о выводе оборудования из эксплуатации определяется также экономическими возможностями, наличием персонала, правовыми ограничениями, доступностью запасных частей, устойчивостью информационной системы и последствиями для потребителей. В суперпространстве такая цепочка рассматривается как единый процесс управления состоянием объекта.

2.6. Интегрирование и дифференцирование пространств

Сложный социотехнический объект функционирует одновременно в нескольких пространствах. Он имеет техническое состояние, использует информационные системы, действует в пределах правовых требований, расходует ресурсы, опирается на кадровые компетенции и реализует организационные процедуры. Каждое пространство отражает отдельную сторону объекта. Однако реальный объект не разделён на независимые части. Изменение параметра в одном пространстве способно вызвать последствия в других пространствах.

Поэтому теория комплексной безопасности использует две взаимодополняющие аналитические операции: **интегрирование** и **дифференцирование пространств**. Первая операция необходима для построения целостной модели объекта. Вторая позволяет ограничить область анализа и де-

тально исследовать конкретную проблему. Эти операции не являются механическим сложением или исключением показателей. Они представляют собой способы организации знания об объекте, его состояниях, функциях, угрозах и управляющих воздействиях.

В исходных материалах суперпространство определяется как объединение нескольких пространств, необходимых для работы с заданным объектом. Интегрирование понимается как объединение координатных осей нескольких пространств с образованием нового суперпространства. Дифференцирование связано с сокращением числа рассматриваемых координат и выделением пространства меньшей размерности.

2.6.1. Интегрирование пространств

Под **интегрированием пространств функционирования** далее понимается объединение параметров двух или нескольких пространств в единую модель, предназначенную для анализа состояния объекта, его критических функций и взаимосвязей между ними.

Пусть техническое пространство объекта задано множеством параметров:

$$X_{\text{тех}} = \{x_1, x_2, \ldots, x_N\},$$

а информационное пространство задано множеством:

$$X_{\text{инф}} = \{y_1, y_2, \ldots, y_M\}.$$

Их простое объединение образует расширенное описание:

$$X_{\text{суп}} = X_{\text{тех}} \cup X_{\text{инф}}.$$

Если параметры двух пространств полностью независимы, размерность нового пространства равна сумме размерностей исходных пространств:

$$L = N + M.$$

В реальных системах часть параметров отражает одну и ту же характеристику с разных сторон. Например, доступность автоматизированной системы управления относится к информационному пространству, но одновременно влияет на

технологическую управляемость. Квалификация оператора относится к кадровому пространству, но определяет способность правильно интерпретировать технические данные. Поэтому при построении суперпространства число независимых координат обычно удовлетворяет условию:

$$L \leq N + M.$$

Это ограничение имеет принципиальное значение. Интегрированная модель не должна дублировать одну и ту же зависимость под разными наименованиями. Она должна отражать причинные связи между параметрами и показывать, каким образом изменение одного состояния преобразуется в изменение другого.

Интегрирование необходимо в тех случаях, когда управленческая задача не может быть решена в пределах одного пространства. Например, отказ технологического оборудования сам по себе является технической проблемой. Однако решение о его ремонте, выводе из эксплуатации или переводе на резервный режим требует учёта доступности запасных частей, квалификации персонала, сроков поставки, юридических ограничений, состояния цифрового контура управления и последствий для критических функций объекта. В этом случае технический анализ должен быть интегрирован с ресурсным, кадровым, информационным, правовым и ор-

ганизационным анализом.

Интегрирование позволяет выявлять три вида связей.

Первый вид — **функциональные связи**. Они показывают, какие параметры разных пространств совместно обеспечивают выполнение критической функции. Например, функция дистанционного управления требует работоспособности оборудования, достоверности данных, наличия связи, компетентности оператора и установленного порядка принятия решений.

Второй вид — **причинные связи**. Они показывают, каким образом отклонение в одном пространстве вызывает изменения в другом. Дефицит кадров может привести к увеличению срока технического обслуживания. Увеличение срока обслуживания способно повысить вероятность отказа. Отказ оборудования может вызвать нарушение производственного процесса и потребовать перераспределения ресурсов.

Третий вид — **компенсационные связи**. Они отражают способность одного контура временно поддерживать другой. Например, потеря автоматизированного канала связи может компенсироваться резервной процедурой ручного управления. Однако такая компенсация возможна только при наличии подготовленного персонала, актуальной документации, независимых средств связи и достаточного времени для перехода на резервный режим.

Интегрирование пространств даёт возможность видеть систему как объект управления, а не как совокупность ве-

домственных направлений. Оно связывает техническую надёжность с качеством данных, организационную устойчивость — с распределением полномочий, кадровую готовность — с возможностью выполнения критических операций, а ресурсную обеспеченность — со скоростью восстановления.

2.6.2. Интегрирование и гибридные угрозы

Особое значение интегрирование приобретает при анализе гибридных угроз. Гибридная угроза может возникать в одном пространстве, а реализовываться в другом или нескольких пространствах. Её воздействие распространяется через связи между элементами системы. Современные исследования гибридных конфликтов указывают на согласованное использование разных инструментов — информационных, кибернетических, экономических, правовых, политических и иных — для использования уязвимостей и затруднения защитных решений.

Для теории комплексной безопасности гибридность угрозы определяется не наименованием источника, а траекторией развития последствий. Эта траектория может быть представлена в общем виде:

$$P_a \rightarrow U_b \rightarrow F_c \rightarrow D,$$

где — воздействие, возникшее в пространстве ; — уязвимость, проявившаяся в пространстве ; — нарушение критической функции в пространстве ; — итоговый ущерб.

Например, искажение данных в информационном пространстве может привести к ошибке в организационном пространстве, затем — к нарушению технологического процесса в техническом пространстве и, в конечном счёте, к материальному, социальному или экологическому ущербу. Интегрированная модель необходима для того, чтобы выявить такую цепочку до реализации ущерба.

При отсутствии интегрирования каждый участник системы будет видеть только локальную проблему. Специалист по защите информации зафиксирует цифровой инцидент. Технолог обнаружит отклонение процесса. Руководитель увидит нарушение сроков или рост затрат. Однако связь между событиями может остаться неустановленной. В результате меры будут приниматься раздельно, с запозданием и без оценки их общего эффекта.

Интегрирование позволяет перейти от фиксации отдельных инцидентов к анализу сценариев. Сценарий связывает источник воздействия, уязвимость, последовательность изменений параметров, нарушаемую функцию, возможный

ущерб и доступные меры противодействия. Именно сценарный анализ делает возможной оценку каскадных рисков и выбор меры, направленной на разрыв наиболее опасной связи.

2.6.3. Дифференцирование пространств

Под **дифференцированием пространства** далее понимается аналитическое выделение части суперпространства или отдельного пространства меньшей размерности для решения конкретной задачи. Дифференцирование сокращает число рассматриваемых параметров и позволяет сосредоточить внимание на связях, значимых для данного вопроса.

Если суперпространство объекта задано набором параметров:

$$X_{\text{суп}} = \{X_1, X_2, \ldots, X_L\},$$

то частная модель может быть описана как подмножество:

$$X_{\text{част}} = \{X_{i_1}, X_{i_2}, \ldots, X_{i_K}\},$$

Где $K < L$. Выбор параметров должен определяться не удобством сбора данных, а целью анализа. В частную модель включаются только те координаты, которые оказывают существенное влияние на рассматриваемую функцию, угрозу, риск или управленческое решение.

Дифференцирование необходимо по трём причинам.

Во-первых, оно уменьшает сложность анализа. В исходных материалах отмечается проблема роста размерности: с увеличением числа параметров растут требования к данным, вычислениям и интерпретации результатов. Избыточно сложная модель может стать неуправляемой и утратить практическую ценность.

Во-вторых, дифференцирование позволяет выделять ответственность. Для устранения конкретного отклонения требуется определить, какой субъект обладает полномочиями, ресурсами и профессиональной компетенцией для воздействия на соответствующую группу параметров. Например, техническая служба отвечает за состояние оборудования, подразделение информационной безопасности — за цифровые контуры, а руководство — за согласование действий и распределение ресурсов.

В-третьих, дифференцирование создаёт условия для глубокой экспертной оценки. Каждый частный анализ использует специфические методы, данные и критерии. Техническая диагностика требует одних показателей. Анализ кадро-

вой устойчивости — других. Оценка правовых рисков или устойчивости кооперации требует иных источников информации. Попытка сразу применить единый метод ко всем пространствам часто приводит к потере содержательности.

Дифференцирование не означает разрыв связей между пространствами. Оно является временным ограничением области анализа. После решения частной задачи результаты должны возвращаться в суперпространство для оценки их влияния на состояние объекта в целом.

2.6.4. Последовательность аналитической работы

Интегрирование и дифференцирование образуют единый цикл аналитической работы. Его можно представить в следующей последовательности.

1. Определение критической функции. Субъект управления устанавливает, какую функцию необходимо сохранить и почему её нарушение создаёт неприемлемый ущерб.

2. Интегрированное описание функции. Выявляются пространства, параметры, ресурсы, участники и связи, обеспечивающие выполнение этой функции.

3. Дифференцирование проблемы. При появлении отклонения выделяется частная область анализа: техническая, информационная, кадровая, ресурсная, правовая или

организационная.

4. Локальный анализ. Профильные специалисты устанавливают причины отклонения, динамику параметров, доступные меры и ограничения.

5. Возврат результата в суперпространство. Оценивается, как локальная мера повлияет на другие функции, ресурсы, риски и состояние объекта в целом.

6. Принятие комплексного решения. Субъект управления выбирает меры с учётом ожидаемого системного эффекта, времени реакции, ресурсов и остаточного риска.

7. Контроль и корректировка. Фактическое изменение параметров сопоставляется с ожидаемым результатом. При необходимости модель и меры уточняются.

Такая последовательность обеспечивает связь между частным профессиональным знанием и целостным управлением. Она исключает две противоположные ошибки. Первая ошибка состоит в рассмотрении объекта как набора несвязанных направлений безопасности. Вторая ошибка возникает при стремлении сразу описать все параметры объекта, что делает модель чрезмерно сложной и непригодной для практических решений.

2.6.5. Пример применения

Рассмотрим условную ситуацию: в цифровой системе мониторинга производственного объекта выявлены периодиче-

ские задержки передачи телеметрических данных. При дифференцированном анализе проблема может быть отнесена к информационному пространству. Проверяются каналы связи, серверное оборудование, настройки сети, программное обеспечение и права доступа.

Однако интегрированный анализ должен поставить дополнительные вопросы. Влияет ли задержка на способность оператора своевременно обнаружить техническое отклонение? Существует ли резервный канал получения данных? Может ли персонал перейти на ручной режим контроля? Насколько актуальны бумажные или автономные схемы? Каков допустимый интервал отсутствия достоверных данных? Какие критические функции зависят от своевременной телеметрии? Имеются ли признаки того, что задержка связана с перегрузкой системы, техническим отказом, ошибкой конфигурации, действиями пользователя или внешним воздействием?

Конец ознакомительного фрагмента.