СИСТЕМОТЕХНИКА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ В ИНФОРМАЦИОННОЙ СФЕРЕ

Толстой А. И.[1]

DOI: 10.21681/2311-3456-2024-5-47-57

Аннотация. *В статье рассмотрены основы методологии обеспечения безопасности (ОБ) объектов, использующих современные информационные технологии (Объектов), базирующиеся на концепции, принципах и методах системотехники. В рамках системотехники был развит процессный, системный и управленческий подходы к ОБ Объектов, основанные на разработанных процессных моделях Объекта как части Организации, самого Объекта и его систем ОБ. В работе обосновано выделены среди процессов ОБ Объекта четыре группы процессов – это обеспечение безопасности информации, устойчивости, информационно-психологической безопасности персонала и физической защиты Объекта с учетом необходимости обеспечить состояние защищенности основных активов Объекта и формулирования отдельных целей ОБ Объекта. В каждой из этих групп в рамках развития процессного подхода были выделена часть процессов, реализация которых направлена на достижение необходимого состояния защищенности активов Объекта, и часть процессов управления процессами из первой части, которые должны обеспечить необходимую результативность на стадиях их планирования, реализации, контроля и совершенствования. При этом показан адаптивный характер управления такими процессами. С учетом выделенных групп процессов была предложена структура систем, входящих в СОБ Объекта, и структура системы процессов ее поддержки (динамическое и статическое представление СОБ соответственно), а также структура комплексной системы безопасности Объекта. Использование системотехники при ОБ Объекта позволило на единой методологической базе обосновать направление подготовки профессионалов в области ОБ Объектов, определив их квалификацию (инженер-системотехник) и возможный перечень специальностей, входящих в это направление. Применение системотехники в рамках решении задач ОБ Объекта позволило осуществить системный (целостный) подход, необходимый для проведения исследований, проектирования, реализации и развития систем обеспечения безопасности конкретных Объектов. Предлагаемые в работе решения носят обобщенный характер и не противоречат существующему в настоящее время подходу, связанному с обеспечением информационной безопасности.*

Ключевые слова: *методология, концепция, принципы, метод, модель, процесс, система, актив, управление, безопасность информации, устойчивость, информационно-психологическая безопасность, физическая безопасность.*

Введение

Для объектов, имеющих отношение к обработке информации с использованием современных информационных технологий (ИТ), решение проблемы сохранения ее основных свойств (конфиденциальности, целостности и доступности) чаще всего сводится к принятию мер защиты информации (ЗИ) или к обеспечению информационной безопасности (ИБ). Признанной основой решения этой проблемы является принятая в настоящее время методология, базирующаяся на процессном, управленческом и системном подходах к обеспечению информационной безопасности (ОИБ)[2]. Проецируя определения понятия «ИБ», данное в Доктрине «Информационная безопасность РФ»[3] на уровень объекта, были даны определения понятий «ИБ объекта» как состояния защищенности его активов от угроз в информационной сфере, «процесс ОИБ объекта» как действия, направленного на достижения такого состояния, и «система ОИБ (СОИБ) объекта» как совокупности связанных процессов ОИБ [1, 2].

Анализ СОИБ объекта показал [2], что эта система существенно зависит от особенностей объекта, которому она относится (сложность объекта, интеграция современных информационных технологий на аппаратном, программном и информационном уровне), и от особенностей процессов ОИБ (связанности, разнородности, сложности). При этом необходимо отметить, что в некоторых случаях цели функционирования СОИБ и объекта могут быть близки (например, поддержка качества реализации основных процессов (бизнес-процессов), или противоположны (сохранение свойств информации для СОИБ и скорость обработки информации для объекта). Дополнительным фактором, который необходимо учитывать, является непременное участие людей (например персонала организации), имеющего отношение к качественному

1 Толстой Александр Иванович, кандидат технических наук., доцент, Национальный исследовательский ядерный университет «МИФИ», Москва, Россия. E-mail: AITolstoj@mephi.ru, http://orcid.org/0000-0001-9265-1510

2 ГОСТ Р ИСО/МЭК 27000-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

3 Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ от 05.12.2016 N 646.

функционированию и использованию объекта, относящегося к организации и его СОИБ, а также влияние окружающей среды на функционирование объекта и его СОИБ. Таким образом и сам объект, и его СОИБ можно отнести к сложным системам, объединяющим сложные системы [3], а также к социотехническим системам [3,4,5], требующим свои подходы к их исследованию, проектированию и эксплуатации.

Если рассмотреть особенности такой предметной области, как системная инженерия [6] (чаще называемая в русскоязычных информационных источниках системотехникой [7]), которая связанна с проектированием, созданием и эксплуатацией структурно сложных, крупномасштабных, человеко-машинных и социотехнических систем [6], а также особенности объектов системотехники, представляющих собой человеко-машинные системы, состоящие из разнородных элементов и связей, включая и окружающую среду [7], то саму систему обеспечения ИБ объекта можно обосновано считать объектом системотехники.

Это утверждение положено в основу исследований, результаты которого приводятся в данной работе. Особое внимание уделено применимости принципов системотехники к исследованию систем обеспечения безопасности объектов в информационной сфере (далее Объектов) в части формирования процессной модели организации (далее Организации), к которой относится Объект, и ее системы обеспечения безопасности (СОБ Объекта), а также формирования модели поддержки действий в отношении СОБ Объекта.

1.Основы системотехники и обеспечение безопасности Объекта

Формирование системотехники обеспечения безопасности Объекта непосредственно связано с основами системотехники. При этом важно уточнить особенности используемых понятий, рассмотреть современные концепции системотехники, ее принципы, методы и предмет в контексте выбранного объекта системотехники: СОБ конкретного объекта. В данной работе предлагаются следующие определения базовых понятий:

Безопасность объекта в информационной сфере *– это состояние защищенности активов объекта от угроз в информационной сфере, которому соответствует допустимый уровень риска нарушения безопасности объекта*.

Информационная сфера *– это совокупность информационного пространства, объединяющего объекты, обрабатывающие информацию с использованием современных ИТ, и субъекты, реализующие деструктивное воздействие на активы объекта, с учетом их взаимного расположения, и информационной среды, в которой взаимодействуют объекты и субъекты.*

Процесс обеспечения безопасности объекта в информационной сфере *– это деятельность, направленная на достижения необходимого состояния защищенности активов объекта от угроз в информационной сфере.*

Система обеспечения безопасности объекта в информационной сфере *– это совокупность связанных процессов, направленных на достижение необходимого состояния защищенности активов объекта от угроз в информационной сфере.*

1.1. Понятие «системотехника»

Понятие «системотехника» многогранно и имеет комплексный характер [6,7]. Из множества определений этого понятия можно выделить следующие общие факторы [7]:

1. *Сфера деятельности*, направленная на организацию процесса создания, использования и развития сложных инженерных систем.

Сфера деятельности, относящаяся к обеспечению безопасности (ОБ) Объекта, — это информационная сфера. Предметом деятельности является решение задач по ОБ конкретного объекта. Это комплексные задачи, решение которых предполагает кооперацию специалистов различных профилей с целью интеграции частей СОБ в единое целое.

2. *Область знания:* комплексная научно-техническую дисциплина, объединяющая средства, методы, принципы анализа и организации инженерной деятельности, а также средства, методы, приемы и процедуры проектирования и исследования сложных инженерных систем.

Область знания, относящаяся к предметной области ОБ Объекта, связана с методами и средствами современных математических, технических, естественнонаучных и общественных дисциплин, необходимых для исследования и проектирования СОБ Объекта.

3. *Конкретно-методологическую позицию*, связанную с целостным рассмотрением инженерной системы, процесса ее исследования, проектирования, создания и развития.

Основным методом системотехники является системный подход с его конкретными видами реализации: системным анализом, исследованием операций и кибернетикой [8].

Таким образом, системотехника – это научное направление, изучающее общесистемные свойства системотехнических комплексов, процессы их создания, совершенствования, использования и ликвидации в целях получения максимального социального эффекта [8].

Применение системотехники в рамках решения задач ОИБ конкретного Объекта позволяет осуществить системный (целостный) подход к рассмотрению СОБ Объекта при ее исследовании, проектировании, реализации и развитии.

1.2. Концепции системотехники

Для системотехники важное значение имеет системное представление ее объекта, обладающее чертами, присущими всем (или многим) сложным инженерным объектам. Выделяют пять основных системных представлений [7]: процессуальное, функциональное, макроскопическое, иерархическое и микроскопическое.

Исходя из этого, СОБ может быть представлена динамически как совокупность процессов, обеспечивающих состояние защищенности активов Объекта, статически как предмет, обладающий определенными внешними или внутренними свойствами (характеристиками) или функционально, когда внутреннее строение СОБ может быть представлено в виде структуры, реализующей совокупность связанных функций (действий) для достижения определенной цели (например, достижения целостности, доступности или конфиденциальности информации).

В основании системотехники лежит ряд концепций — общих абстрактных представлений, связанных с пониманием её предмета, а также совокупность принципов, то есть исходных, принимаемых за истину, правил, которые используются в качестве основы для рассуждений и/или для принятия решений [6].

Основные концепции системотехники включают следующие понятия: система, жизненный цикл и заинтересованные стороны [6].

Среди особенностей, которые имеет система, рассматриваемая системотехникой, необходимо в дополнение к уже отмеченным выше выделить признаки, которые полностью можно отнести и к СОБ Объекта [6]: структурная и функциональная сложность, большие информационные потоки, функционирование в условиях существенной неопределённости и воздействия среды на неё (объект функционирует в информационной сфере при деструктивном воздействии угроз, имеющих вероятностный характер проявления).

Использование понятия жизненного цикла системы признано фундаментальной основой практики системотехники [9]. При этом жизненный цикл системы (system life cycle) связывают с ее развитием во времени, начиная от замысла и заканчивая списанием . На каждом этапе жизненного цикла система имеет относительно стабильный набор характеристик. При моделировании жизненного цикла используются совокупности процессов жизненного цикла.

Для описания жизненного цикла СОБ Объекта можно применить процессный подход [3], основанный на циклической модели Деминга [10], предполагающий такие этапы жизненного цикла, как планирование, реализация, контроль и совершенствование процессов СОБ.

В системотехнике критически важной задачей является выявление ключевых заинтересованных сторон и их интересов, анализ их баланса с учётом механизмов их возникновения и необходимости гармонизации точек зрения, а также оценка относительной степени влияния разных заинтересованных сторон на принимаемые решения. является в системной инженерии критически важной задачей [6].

Заинтересованная сторона (stakeholder) или правообладатель[4] — это сторона, имеющая право, долю или претензии на систему или на владение ее характеристиками, удовлетворяющими потребности и ожидания этой стороны. Заинтересованные стороны преследуют различные цели, которые должны быть гармонично учтены на основе баланса их интересов, в том числе через регулирование отношений: между группами заинтересованных сторон; между заинтересованными сторонами и объектом интереса.

При ОБ Объекта заинтересованными сторонами могут быть владелец Объекта (Организации), владелец информации, партнеры Организации, регуляторы отношений в области ОБ, само государство. Важность выявления и учета интересов заинтересованных сторон подтверждена, например, при обеспечении кибербезопасности в киберпространстве[5].

1.3. Принципы системотехники

В процессе развития системотехники сложились её основные принципы [6, 11, 12]. Среди них наиболее важными для области ОБ Объектов будут:

1) Переход от редукционистского к системному подходу [6, 11].
2) Переход от структурного к процессному подходу [6].
3) Доказательно обоснованное принятие решений на основе фактов и с учётом риска — наиболее важным фактором при принятии решений является наличие доказательно обоснованного факта, а не плана, графика или календарного события [12].
4) Использование метода синтеза при выборе, описании и проектировании «правильных» составных частей системы, их соединении между собой так, чтобы достигалось необходимое и правильное сочетание для достижения необходимых свойств целого [11].

4 ГОСТ Р ИСО/МЭК 15288-2005 ИТ. Системная инженерия. Процессы жизненного цикла систем.

5 ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity.

5) Применение адаптивной оптимизация характеристик сложной системы к новым ситуациям и изменениям, происходящим в самой системе, во внешней среде и в других системах, взаимодействующих с целевой системой [11].
6) Постепенное уменьшение энтропии. Процессы системотехники должны реализовываться на протяжении всего жизненного цикла системы, в результате чего энтропия, характеризующая целевую систему, постепенно уменьшается с переходом от состояния беспорядка (высокая энтропия) к состоянию порядка (низкая энтропия) в конце цикла [11].
7) Достижение разумной ситуации для получения результатов, которые в данных условиях позволяют в наибольшей степени удовлетворить критически важные заинтересованные стороны [11].
8) Переход от методов жёсткого планирования к использованию гибких прогнозных методов [6].
9) Переход от монодисциплинарного к междисциплинарному подходу [6].

Принципы системотехники 1), 2) и 3) соответствуют современной методологии обеспечения ИБ, которая предполагает реализацию системного, процессного и риск-ориентированного подходов[2], что можно использовать и при ОБ Объектов.

Принцип 4) предполагает обоснованную структуризацию СОБ Объекта с формулированием требований к ее составным частям и требований, которые должны быть выполнены при синтезе этих частей для достижения необходимой результативности ОБ конкретного Объекта.

Наиболее важный аспект использования принципа 5) при ОБ Объекта – это учет особенностей самого Объекта при создании его СОБ, особенностей Организации, частью которой является Объект, а также особенностей внешней среды, в которой функционирует Организация, Объект и СОБ [1, 2].

Реализация принципа 6), направленная на постоянное совершенствование СОБ Объекта, позволяет достичь обоснованной прозрачности и упорядоченности действий для достижения требуемой результативности ОБ Объекта.

При ОБ Объекта удовлетворение требований заинтересованных сторон (правообладателей[4]), о которых говорилось выше, невозможно без реализации принципа 7).

Реализация СОБ Объекта предполагает противодействие актуальным угрозам нарушения безопасности Объекта, моделирование которых носит прогнозный характер, что можно сделать только при использовании принципа 8).

Особенности объектов в информационной сфере и их СОБ носят междисциплинарный характер, чему полностью соответствует принцип 9).

1.4. Методы системотехники

Все известные методы (процессы) системотехники (системной инженерии) предполагают итеративное применение процедур синтеза, анализа, оценки [6]:

1. Синтез включает формирование определённой совокупности требований к объекту системотехники со стороны заинтересованных сторон, описанных на языке функционирования. Основными элементами обеспечения синтеза являются команда разработчиков, компьютерно-ориентированные инструменты синтеза, а также результаты прикладных исследований и возможности использования известных технологий.
2. Анализ вариантов системных решений, относящихся к объекту системотехники, а также определение или предсказание его параметров. В целом, применение анализа — это необходимая, но не достаточная составляющая процедуры принятия решения о выборе проектного варианта объекта.
3. Оценка подразумевает, что каждый вариант решения (или альтернатива) оценивается в сравнении с другими вариантами, а также проверяется на соответствие требованиям заинтересованных сторон.

Набор методов системотехники в обобщенном виде, необходимых для создания результативной СОБ Объекта, может включать, как минимум, следующие действия:

- обеспечение надёжного проектной базы, включающей исходную информацию и требования, а также необходимые инструменты для совместной работы множества специалистов над мультидисциплинарной информацией в ходе создания СОБ Объекта и управления её жизненным циклом;
- точную оценку доступной информации и определение недостающей, необходимую для создания СОБ Объекта;
- проведение системного анализа для разработки проектных решений, отражающих поведение СОБ Объекта, которые должны соответствовать всем требованиям;
- проведение анализа компромиссных решений по создания СОБ Объекта для поддержки процесса принятия решений;
- создание исполняемых моделей для верификации и валидации работы СОБ Объекта.

Необходимо отметить, что перечисленные выше действия требуют проведения исследований, направленных на формализацию процессов создания СОБ Объекта, которые могут составить комплекс методов системотехники, относящихся к ОБ конкретных Объектов.

2. Процессный подход к обеспечению безопасности Объекта

Процессный подход в системотехнике как один из ее принципов [6] определяет требования к деятельности любой организации и ее объектов в виде ориентации процессов, реализуемых в организации, на конечный результат [13]. При этом понятие «процесс» определяется как совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующей контекст на входе в контекст на выходе процесса и требующей определенных ресурсов и управляющих воздействий (рис. 1) для получения намеченного результата[4].

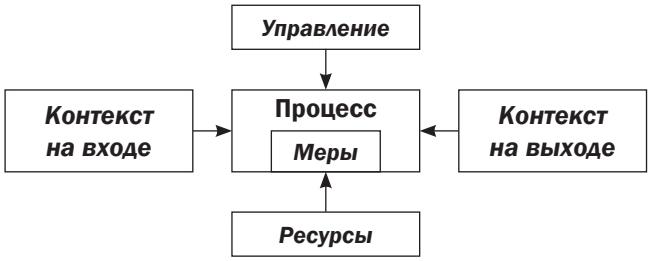

Рис. 1. Обобщенная структурная схема процесса

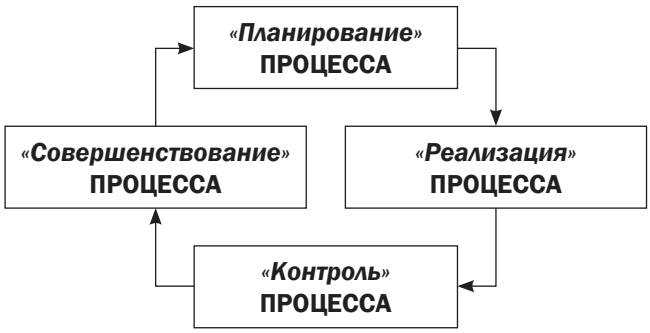

Рис. 2. Модель Деминга

При этом в отношении конкретного процесса достижение намеченного результата определяется в соответствии с циклической моделью Деминга [10] результативностью управления процессом на стадиях его «планирования», «реализации», «контроля» и «совершенствования» (рис. 1, рис. 2).

2.1. Процессная модель Организации

Если сам объект рассматривать как часть организации, то в соответствии с принципом системотехники 5) процессы обеспечения безопасности Объекта должны рассматриваться в связи с процессами Организации и другими процессами, реализуемыми в ней [13]. В данном случае представляется целесообразным прежде всего рассмотреть процессную модель Организации, состоящую из отдельных процессов, отнесенных к определенным объектам Организации (рис. 3).

Интересы любой организации достигаются через деятельность, которую в терминах процессного подхода можно представить в виде совокупности следующих трех групп высокоуровневых процессов [13]: основные процессы (процессы основной деятельности, формирующие бюджет организации, или бизнес-процессы); вспомогательные процессы; процессы управления.

К основным процессам можно отнести (рис. 3) деятельность по оказанию бизнес-услуг, по производству продукции, по выполнению обязательств по договору, по обработке информации ограниченного доступа (если необходима соответствующая лицензия) и др.

Вспомогательные процессы классифицируются по видам обеспечения основных процессов. Например, к вспомогательным процессам можно отнести (рис. 3) деятельность по бухгалтерскому облуживанию, по планированию деятельности организации, по осуществлению контроля и др.

Рис. 3. Структура процессной модели Организации

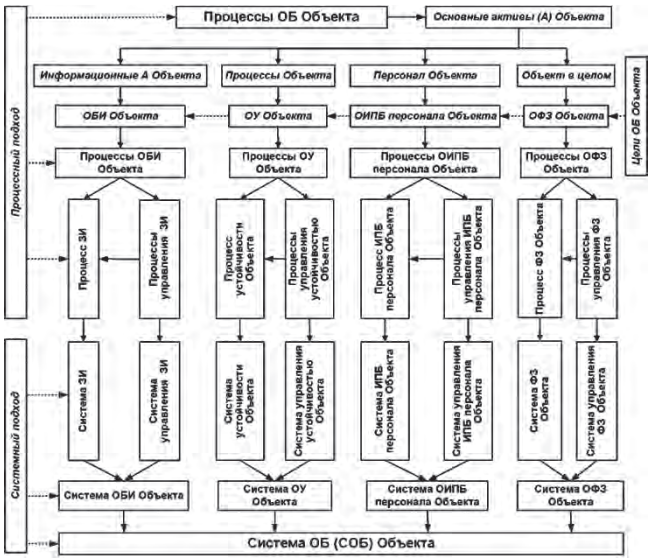

Рис. 4. Структура процессной модели СОБ Объекта

Процессы ОБ относятся к вспомогательным процессам [13], которые, прежде всего, связывают с объектами, относящимся к основными или вспомогательными процессам (рис. 3). Причем, как правило,

такими объектами являются те, которые реализуют процессы автоматизации обработки информации (тоже вспомогательные процессы) с использованием современных информационных технологий (ИТ-сервис). К таким объектам можно отнести информационные системы, автоматизированные системы (АС), объекты информатизации, АС управления (АСУ), АСУ технологическим процессом (АСУ ТП), объекты систем интернет-вещей, киберфизические системы и т.д.

Процессы управления в организации играют особую роль. Совокупность процессов управления в организации образуют процессы, относящиеся к различным объектам организации и к различным процессам организации. В соответствии с процессным подходом реализацией процесса управления в отношении к конкретному процессу достигается намеченный результат (результативность процесса). Это распространяется и на процессы ОБ.

2.2. Процессная модель обеспечения безопасности Объекта

Обеспечение безопасности Объекта в соответствии с принципом 2) системотехники необходимо связать с совокупностью процессов ОБ, относящихся к СОБ Объекта. Их структуру предлагается представить в виде процессной модели, показанной на рис. 4.

Совокупность процессов ОБ Объекта предлагается сформировать с учетом принципа системотехники 4) и необходимости достижения результативности при синтезе СОБ Объекта (основной метод системотехники), разделив их на четыре группы с учетом определения основных активов Объекта: информационные активы, процессы Объекта, персонал объекта и объект в целом. Это позволило разделить область ОБ Объекта на:

- обеспечение безопасности информации (ОБИ), связанной с сохранением необходимого состояния защищенности информации, обрабатываемой на Объекте;
- обеспечение функциональной устойчивости (ОУ) Объекта (его процессов);
- обеспечение информационно-психологической безопасности (ОИПБ) персонала Организации, имеющего отношение к Объекту, при деструктивном воздействии на него информации;
- обеспечение физической защиты (ОФЗ) Объекта с учетом его расположения (помещение, этаж, здание, территория Организации).

В данном случае ОБИ на Объекте, ОУ Объекта, ОИПБ персонала Объекта и ОФЗ Объекта можно использовать не только как совокупности процессов, но и как отдельные цели действий на Объекте, направленных на ОБ Объекта.

В каждой подобласти, которые формируют область ОБ Объекта, будет своя группа процессов безопасности (ПБ): процессы защиты информации, обрабатываемой на Объекте (ПЗИ); процессы устойчивости Объекта (ПУ); процессы ИПБ персонала Объекта (ПИПБ); процессы ФЗ Объекта (ПФЗ).

В соответствии с процессным подходом (рис. 2, рис. 3) и принципом 2) системотехники, реализация каждого процесса предполагает использование

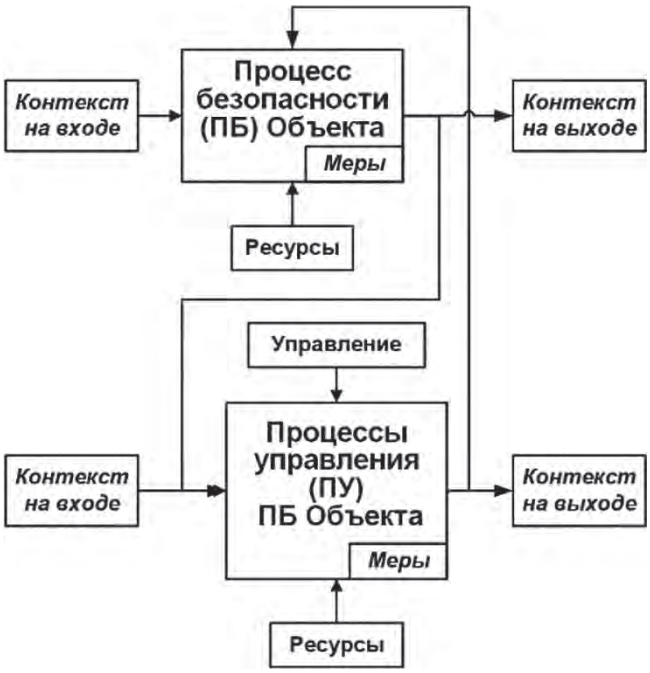

Рис. 5. Процессный подход к ОБ Объекта

Рис. 6. Процессный подход к поддержке СОБ Объекта

своих мер (технических и/или организационных), а результативность каждого процесса на стадиях его планирования, реализации, контроля и совершенствования требует применения соответствующих процессов управления: процессом ЗИ (УПЗИ); процессом устойчивости Объекта (УПУ); ИПБ персонала Объекта (УПИПБ); ФЗ Объекта (УПФЗ).

Необходимо отметить, что реализация процессов управления конкретным процессом ОБ Объекта будет зависит не только от особенностей Объекта и его окружения, но и от результатов реализации самого процесса (рис. 5). Речь идет об адаптивном управлении, что в полной мере соответствует принципу 5) системотехники. Процессам управления процесса ОБ Объекта необходимы свои меры, ресурсы и свое управление. В данном случае можно констатировать факт, что реализуется не только процессный, но и управленческий подход.

3. Системный подход к обеспечению безопасности Объекта

В соответствии со сформулированными концепциями системотехники [6,7]. основным ее понятием является «система», что позволяет утверждать, что при рассмотрении проблем обеспечения безопасности объектом исследования будет СОБ Объекта, которая может быть рассмотрена динамически и статически.

3.1. Динамическое представление СОБ Объекта

Динамический подход к СОБ – это объединение связанных процессов ОБ Объекта, целью которых является сохранение основных активов Объекта. Анализ структуры предложенной в данной работе процессной модели СОБ Объекта (рис. 4) приводит к структуризации СОБ Объекта на подсистемы, выделив в ней систему ОБИ (СОБИ), систему ОУ (СОУ), систему ОИПБ персонала (СОИБП) и систему ОФЗ Объекта:

СОБ = СОБИ + СОУ + СОИПБ + СОФЗ.

Каждая подсистема состоит системы, объединяющей соответствующие процессы безопасности – ПБ (ПЗИ, ПУ, ПИПБ, ПЗИ), и системы, в которые включаются процессы управления процессами безопасности – УПБ (УПЗИ, УПУ, УПИПБ, УПЗИ):

СОБИ=СПЗИ+СУПЗИ; СОУ=СПУ+СУПУ;
СОИПБ=СПИПБ+СУПИПБ; СОФЗ=СПФЗ+СУПФЗ.

С учетом этого можно обосновано утверждать, что при динамическом представлении СОБ Объекта целесообразно рассматривать ее как совокупность системы процессов безопасности (СПБ) и системы управления процессами безопасности (СУПБ):

СОБ = СПБ + СУПБ,

где: **СПБ = СПЗИ+СПУ+СПИПБ+СУПИПБ+ СПФЗ;**
СУПБ=СУПЗИ+СУПУ+СУПИПБ+СУПФЗ.

Связь процессов безопасности (ПБ) из СПЗИ, СПУ, СПИБП и СПФЗ с соответствующими процессами управления (ПУ) процессом безопасности, входящими в системы СУПЗИ, СУПУ, СУПИБП и СУПФЗ, определяет процессный подход к ОБ Объекта (рис. 5).

В зависимости от целей ОБИ Объекта при решении пракритских задач может быть учтены отдельные подсистемы или различные их комбинации вплоть до учета всех подсистем, что соответствует известному методу системотехники – применению процедур синтеза [6].

3.2. Статическое представление СОБ Объекта

Статический подход к СОБ Объекта связан с представлением этой системы в виде предмета, обладающего определенными внешними или внутренними свойствами (характеристиками). При этом важным является поддержка СОБ Объекта (как предмета) на стадиях ее проектирования, реализации, контроля и совершенствования. Причем поддержку СОБ Объекта в виде действий (процессов) и управления этими действиями предлагается описать в рамках процессного подхода, иллюстрируемого рисунком 6, а жизненный цикл СОБ Объекта, как фундаментальной основы практики системотехники [9], также может быть описан моделью Деминга (рис. 2).

Для формирования совокупности процессов поддержки СОБ Объекта можно воспользоваться опытом системного подхода к управлению ИБ[6], который дает основание разделить процессы поддержки (ПП) СОБ Объекта на следующие группы (ГПП): «Контекст» (А), «Руководство» (Б), «Планирование» (В), «Ресурсы» (Г), «Эксплуатация» (Д), «Контроль» (Е), «Улучшение» (Ж). Перечень типовых ПП, распределенных по этим группам, с привязкой к результату реализации конкретного процесса (контекст на выходе – Квых), этапу жизненного цикла (ЭЖЦ) СОБ Объекта («Планирование» – П; «Реализация» – Р; «Контроль» – К; «Совершенствование» – С) и к соответствующим процессам управления – ПУ (рис. 6), приведен в табл. 1 со следующими обозначениями в отношении СОБ Объекта: УД – управление документированием; УА – правление активами Объекта; УР – управление рисками; УОНОБ – управление обеспечением непрерывности обеспечения безопасности (ОНОБ) Объекта; УФиМР – управление финансовыми и материальными ресурсами (ФиМР); УП – управление персоналом Организации; УКП – управление компетентностью персонала Организации; УПБ – управление процессами ОБ Объекта; УИнБ – управление инцидентами безопасности Объекта; УИз – управление изменениями структуры Объекта и систем, относящихся к его безопасности.

6 ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

Таблица 1.

Типовые процессы поддержки СОБ Объекта

ГПП	Типовые ПП	Квых	ЭЖЦ	ПУ ПП
А	Определение контекста на входе (внешнего и внутреннего)	Описание особенностей Объекта и Организации с учетом внешних и внутренних факторов	П	УД
	Описание процессов, реализуемых Объектом и Организацией	Процессные модели Организации и Объекта	П	УД
	Идентификация активов Объекта	Описание активов Объекта и их уязвимостей	П	УА, УД
	Определение потребностей и ожиданий заинтересованных сторон в отношении к ОБ Объекта	Описание потребностей и ожиданий заинтересованных сторон в отношении к ОБ Объекта	П	УД
	Определение требований к СОБ и области ее функционирования	Описание требований к СОБ Объекта и области ее функционирования	П	УД
Б	Определение ролей в отношении ОБ Объекта, порядка их распределения и назначения в Организации	Ролевая модель Организации в отношении ОБ Объекта	П	УД
	Разработка политики ОБ Организации	Политика ОБ Организации	П	УД
В	Анализ угроз безопасности Объекта, оценка и оценивание рисков нарушения безопасности Объекта	Перечень актуальных угроз безопасности Объекта	П	УД, УР
	Описание угроз безопасности Объекта	Модель угроз и модель нарушителя безопасности Объекта	П	УД
	Определение ПБ СОБ, обработка рисков нарушения безопасности Объекта	Перечень ПБ СОБ Объекта	П	УД, УР
	Разработка политик ОБ Объекта	Политики ОБ Объекта	П	УД
	Разработка программы ОНБ Объекта	Программа ОНБ Объекта	П	УОНБ
Г	Выделение финансовой и материальной (ФиМ) поддержки СОБ	Финансовая и материальная поддержка СОБ	П, Р, К, С	УФиМР, УД
	Подбор персонала Организации для ОБ Объекта	Персонал Организации для ОБ Объекта		УП
	Проведение инструктажа и обучения персонала для ОБ Объекта	Поддержка необходимого уровня осведомленности и компетентности персонала для ОБ Объекта		УКП
	Документирование действий, направленных на поддержку СОБ Объекта	Формирование базы внутренних документов, относящихся к ОБ Объекта		УД
Д	Реализация ПБ Объекта	Результаты выполнения политик ОБ Объекта	Р	УПБ, УД
	Реализация процессов управления инцидентами нарушения безопасности (ИнБ) Объекта	Результаты выполнения политики управления ИнБ Объекта	Р	УИнБ
	Реализация процессов ОНОБ Объекта	Результаты выполнения программы ОНОБ Объекта	Р	УОНОБ, УД
Е	Мониторинг событий безопасности Объекта	Выявление ИНБ Объекта	К	УИнБ, УД
	Аудит СОБ Объекта	Выявление нарушений положений политик ОБ Объекта	К	УК, УД
	Самооценка ОБ Объекта			
	Анализ ОБ Объекта со стороны руководства			
Ж	Принятия решения по совершенствованию СОБ	Планы по совершенствованию СОБ	С	УИз, УД
	Реализация процессов по совершенствованию СОБ	Выполнение планов по совершенствованию СОБ	П или Р	УИз, УД

Анализ информации, приведённой в табл. 1, позволяет сформировать систему поддержки СОБ (СПОБ) Объекта, включив в нее систему процессов поддержки СОБ (СППОБ) и систему управления процессами поддержки СОБ (СУППОБ):

СПОБ = СППОБ + СУППОБ.

3.3. Комплексная система обеспечения безопасности Объекта

Следующий этап применения системотехники при обеспечении безопасности Объекта связан с объединением динамического и статического подходов к СОБ Объекта, что позволяет сформировать комплексную систему безопасности Объекта (КСБ), объединяющую систему обеспечения безопасности (СОБ) и систему ее поддержки (СПОБ): **КСБ = СОБ + СПОБ**.

Если выделить в КСБ в отдельные системы процессы обеспечения безопасности и процессы их поддержки (СПБ и СППОБ), процессы управления процессами безопасности и процессы управления поддержки СОБ (СУПБ и СУППОБ), то можно определить КСБ следующим образом:

КСБ = КСПБ + КСУБ,

где: **КСПБ = СПБ + СППОБ; КСУБ = СУПБ + СУППОБ**.

Результатом применения в рамках системотехники системного подхода является обоснованное разделение всех процессов безопасности Объекта на две группы (КСПБ и КСУБ). Причем формирование второй группы полностью соответствует современному управленческому подходу к обеспечению безопасности конкретных объектов (например, для обеспечения ИБ[2]) и отражает фундаментальные особенности безопасности [3]. Структура КСУБ показана на рис. 7.

Рис. 7. Структура комплексной системы управления безопасностью (КСУБ) Объекта

КСУБ Объекта, входящего в Организацию, обеспечивает системный подход к созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению процессов безопасности Объекта (КСПБ) для достижения бизнес-целей Организации. В данном случае предлагается следующее определения понятия КСУБ Объекта:

Комплексная система управления безопасностью (КСУБ) Объекта *– это часть общей системы управления Организации, основанная на риск-ориентированном подходе (на оценке бизнес-рисков), предназначенная для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения безопасности Объекта, и включающая необходимые для этого организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы.*

4. Подготовка профессионалов в области обеспечения безопасности Объекта

Реализация системотехнического подхода к ОБ Объектов предполагает привлечение специалистов различных профилей, подготовка которых тоже должна иметь системный характер. Речь идет об отдельном направлении инженерной подготовки «Обеспечение безопасности объектов в информационной сфере», с единой квалификацией «инженер-системотехник». Это направление может объединять, как минимум, четыре специальности: «Обеспечение безопасности информации», «Обеспечение устойчивости объектов в информационной сфере», «Обеспечение информационно-психологической безопасности объектов в информационной сфере», «Обеспечение физической защиты объектов в информационной сфере». Эти специальности будут иметь общий цикл фундаментальных дисциплин (математика, физика, информатика, основы системотехники, основы управления, основы психологии), общий цикл общепрофессиональных дисциплин (методология обеспечения безопасности объектов, современные информационные технологии, управление обеспечением безопасности объектов, объекты в информационной сфере) и цикл профессиональных дисциплин (отражают специфику отдельной специальности). Причем каждая специальность может иметь специализации, разделение которых возможно на основе выбора отдельного вида объекта в информационной сфере.

Следует отметить, что в настоящее время существует укрупненное направление подготовки специалистов по защите информации 10.00.00 «Информационная безопасность». Название направления и номенклатура специальностей, входящих в это направление, сформировались в контексте развития этого образовательного направления в условиях отсутствия устоявшейся понятийной базы данной предметной области. Например, понятие «информационная безопасность» прежде всего отражает

аспекты, связанные с безопасностью объекта от воздействия информации, что соответствует только информационно-психологической безопасности. Следствием этого является отсутствие у данного направления необходимой методологической базы.

Выводы

В работе впервые рассмотрены основы методологии обеспечения безопасности объектов, использующих современные информационные технологии (Объектов), базирующиеся на понятиях, концепции, принципах и методах системотехники.

В рамках системотехники был развит процессный, системный и управленческий подходы к ОБ Объектов, основанные на разработанных процессных моделях Организации, Объекта как части Организации и его систем ОБ.

В работе дано обоснование выделения среди процессов ОБ Объекта четырех групп процессов: обеспечение безопасности информации, обеспечение устойчивости Объекта, обеспечение информационно-психологической безопасности персонала Объекта и обеспечение физической защиты Объекта с учетом необходимости обеспечить состояние защищенности основных активов Объекта (информационных активов, процессов, персонала и Объекта в целом соответственно) и формулирования отдельных целей ОБ Объекта. В каждой из этих групп в рамках развития процессного подхода были выделена часть процессов, реализация которых направлена на достижения необходимого состояния защищенности активов Объекта, и часть процессов управления процессами из первой части, которые должны обеспечить необходимую результативность реализации процессов из первой части на стадиях их планирования, реализации, контроля и совершенствования. При этом показан адаптивный характер управления такими процессами.

С учетом выделенных групп процессов была предложена структура систем, входящих в СОБ Объекта (динамическое представление СОБ). Ее анализ показал, что важным дополнением к СОБ Объекта с учетом системотехнического подхода является планирование, реализация, контроль и совершенствование процессов поддержки СОБ Объекта как предмета (статическое представление СОБ), что привело к формированию системы поддержки СОБ (СПОБ) со своими процессами поддержки и процессами их управления и к формированию комплексной системы безопасности (КСБ) Объекта, состоящей из СОБ и СПОБ, которую также можно представить совокупностью комплексной системы процессов безопасности (КСПБ) и комплексной системы управления безопасностью (КСУБ). Учитывая важность КСУБ Объекта в работе была определена ее структура и было сформулировано определение понятия, относящиеся к КСУБ.

Использование системотехники при ОБ Объекта позволило на единой методологической базе обосновать направление подготовки профессионалов в области ОБ Объектов, определив их квалификацию (инженер-системотехник) и возможный перечень специальностей, входящих в это направление. Таким образом результаты работы также имеют практическую значимость для образовательной области, особенно на этапе проходящей в настоящее время реформы системы высшего образования.

Применение системотехники в рамках решении задач ОБ Объекта позволило осуществить системный (целостный) подход, необходимый для проведения исследований, проектирования, реализации и развития систем обеспечения безопасности конкретных Объектов. Предлагаемые в работе решения носят обобщенный характер и не противоречат существующему в настоящее время подходу, связанному с обеспечением информационной безопасности.

Литература

1. *Толстой, Александр И. Обеспечение безопасности объектов в информационной сфере. Безопасность информационных технологий, [S.l.], т. 31, № 3, с. 105–123, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1677. DOI: http://dx.doi.org/10.26583/bit.2024.3.05.*
2. *Толстой, Александр И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, [S.1], т. 30, № 1, с.130–148, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1478. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.*
3. *Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. Под общей ред. А. П.Курило. — 2-е изд., перераб. и доп. — М.: Альпина Паблишерз, 2011. — 373 с.*
4. *Кравченко Сергей. И. Безопасность социотехнических систем// НБИ технологии. 2018. Т. 12. № 2, с. 20-24. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3.*
5. *Корганова О. Г., Панфилова И. Е. Модель управления информационными рисками социотехнической системы на основе поведенческих особенностей человека // Сборник научных трудов НГТУ. – 2020 – № 1–2 (97). – С. 89–98. – DOI: 10.17212/2307-6879-2020-1-2-89-98.*
6. *Батоврин В. К., Голдберг Ф. Н., Александров П. С., Малер Е. А. Системная инженерия / Гуманитарный портал: Концепты [Электронный ресурс]// Центр гуманитарных технологий, 2002–2023 (последняя редакция: 08.12.2023). URL: https://gtmarket.ru/concepts/7110.*
7. *Горохов В. Г. Методологический анализ системотехники. – Москва: Радио и связь, 1982. 162 с.*
8. *Николаев, В. И. Системотехника: методы и приложения / В. И. Николаев, В. М. Брук. – Л.: Машиностроение, Ленингр. отд-ние, 1985. – 199 с.*
9. *Blanchard B. S., Fabrycky W. J. Systems Engineering and Analysis. — Prentice Hall, 2006.*

10. Нив Г. Пространство доктора Деминга. М.: Альпина Бизнес Букс, 2007.
11. Hitchins D. What are the General Principles Applicable to Systems? — INCOSE INSIGHT. — V. 12, Issue 4. — December 2009. — pp. 59–64).
12. Boehm B. et al. Principles for Successful Systems Engineering. — Procedia Computer Science — № 8, 2012. — pp. 297–302.
13. Аудит информационной безопасности / А. П. Курило, С. Л. Зефиров, В. Б. Голованов и др. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.

SYSTEM ENGINEERING FOR ENSURING SECURITY OF OBJECTS IN THE INFORMATION SPHERE

Tolstoy A. I.[7]

Abstract. *The article considers the fundamentals of the methodology for ensuring the security of objects using modern information technologies (Objects), based on the concepts, principles and methods of systems engineering. Within the framework of systems engineering, the process, system and management approaches to ensuring the security of Objects were developed, based on the developed process models of the Object as a part of the Organization, the Object itself and its security ensuring systems (SES). In the work, four groups of processes are substantiated among the processes of ensuring the security of the Object – this is ensuring of information security, resilience, information and psychological security of personnel and physical protection of the Object, taking into account the need to ensure the secure state of the main assets of the Object and the formulation of separate goals of ensuring the security of the Object. In each of these groups, within the framework of the development of the process approach, a part of the processes were identified, the implementation of which is aimed at achieving the required secure state of the assets of the Object, and a part of management processes for the processes from the first part, which should ensure the necessary effectiveness at the stages of their planning, implementation, control and improvement. At the same time, the adaptive nature of the management of such processes is shown. Taking into account the identified groups of processes, a structure of systems included in the Object's SES and a structure of the system of its support processes (dynamic and static representation of the SES respectively), as well as a structure of the Object's integrated SES were proposed. The usage of systems engineering in the Object's security ensuring allowed us to substantiate the direction of training professionals in the field of Object's security ensuring on a single methodological basis, defining their qualifications (systems engineer) and a possible list of specialties included in this direction. The usage of systems engineering in solving Object's security ensuring problems allowed us to implement a systemic (integrated) approach necessary for conducting research, designing, implementing and developing SESs for specific Objectss. The solutions proposed are generalized and do not contradict the currently existing approach related to ensuring information security.*

Keywords: *methodology, concept, principles, method, model, process, system, asset, management, information security, resilience, information and psychological security, physical security.*

References

1. Tolstoy, Alexandr I. Obespechenie bezopasnosti ob'ektov v informatcionnoi sferi. Bezopasnost informacionnih tehnologiy, v. 31, no 3, p. 105–123, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1677. DOI: http://dx.doi.org/10.26583/bit.2024.3.05.
2. Tolstoy, Alexandr I. Sistematika poniytii v oblasti informacionnoy bezopasnosti. Bezopasnost informacionnih tehnologiy, [S.l.], v. 30, no. 1, p. 130–148, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1478. DOI: http://dx.doi.org/10.26583/bit.2023.1.10.
3. Obespechenie informacionnoi bezopasnosti biznesa / V. V. Andrianov, S. L. Zefirov, V. B. Golovanov, N. A. Golduev.- M.: Alpina Паблишерз, 2011. – 373 p.
4. Kravchenko S. I. Bezopasnost sociotehnicheskih system// NBI tehnologii. 2018. v. 12. № 2, p. 20–24. DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.3
5. Korganova O. G., Panfilova I. E. Model upravleniya informatsionnymi riskami sotsiotekhnicheskoi sistemy na osnove povedencheskikh osobennostei cheloveka [Model of information risk management of a sociotechnical system based on human behavioral features]. Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university, 2020, no. 1–2 (97), pp. 89–98. DOI: 10.17212/2307-6879-2020-1-2-89-98.
6. Batovrin V. K., Goldberg F. N., Aleksandrov P. S., Maler E. A. Sistemnaia inhzeneria / Gumanitarnii portal: Koncepti [Elektrronnii resurs] // Centr gumanitarnih tehnologii, 2002–2023 (posledniy redakciya 20.08/2024). URL: https://gtmarket.ru/concepts/7110.
7. Gorohov V. G, Metodologicheskiy analiz sistemotehniki. – Radio i sviyz, 1982. 162 p.
8. Nikolaev V. I., Bruk V. M. Sistemotehnika: metodi i prilozheniy. – L.: Mashinostroenie, 1985.– 199 p.
9. Blanchard B. S., Fabrycky W. J. Systems Engineering and Analysis. – Prentice Hall, 2006.
10. Niv G. Prostranstvo doktora Deminga. M.: Alpina Niznes Buks, 2007
11. Hitchins D. What are the General Principles Applicable to Systems? – INCOSE INSIGHT. – V. 12, Issue 4. – December 2009.– pp. 59–64).
12. Boehm B. et al. Principles for Successful Systems Engineering. – Procedia Computer Science – № 8, 2012. – pp. 297–302.
13. Audit informacionnoy bezopasnosti / A. P.Kurilo, S. L. Zefirov, V. B. Golovanov i dr. – M.: Izdatelskaya gruppa «BDC-press», 2006.– 304 p.

7 Alexandr I. Tolstoy, Ph.D, Associate Professor, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow. E-mail: AITolstoj@mephi.ru, http://orcid.org/0000-0001-9265-1510