Санкт-Петербургский Государственный Политехнический Университет

Моделирование требований к системам управления информационной безопасностью по стандартам семейства ISO/IEC 27001

Специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»

Автор:

Черемушкин Дмитрий Владимирович,
аспирант кафедры КИТвП, ФУИТ

Научный руководитель:

Любимов Александр Вилиевич,
кандидат технических наук,
Санкт-Петербургский Государственный Политехнический Университет

Общая характеристика работы

Цель работы: создание методической базы для разработки новых и совершенствования существующих организационных систем управления информационной безопасностью (СУИБ) в виде совокупности формализованных моделей требований к СУИБ, методов их построения и применения

Объект исследования: методология обеспечения информационной безопасности, представленная в семействе международных стандартов ISO/IEC 27000 «Системы управления информационной безопасностью»

Предмет исследования: концептуальная схема, представленная в стандартах семейства ISO/IEC 27000; требования к составу и структуре СУИБ и СУРИБ, представленные в стандартах ISO/IEC 27001 и ISO/IEC 27005

Структура доклада

1. **Объект и предмет исследования**
2. Актуальность темы, цели и задачи работы
3. Описание разработанных моделей и методов их построения
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. Описание методов применения объектных моделей
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Уровни обеспечения ИБ

Уровень		Типичные задачи	Исполнитель	Средства ИБ (примеры)
управленческий		формулировка и анализ требований безопасности, распределение ресурсов, создание и сопровождение единой политики организации в области ИБ	Высшее руководство, Директор по безопасности	Требования безопасности, политика ИБ, анализ СУИБ руководством
организационный		проектирование, внедрение, мониторинг, анализ и усовершенствование СОИБ организации, разработка и внедрение положений и процедур	Отдел ИБ, Директор по ИБ	анализ риска, внутренний и внешний аудит, положения, процедуры, регламенты и руководства по ИБ и т. д.
технологический	архитектурный	выбор архитектуры ИС и сетей, выбор программных и аппаратных средств ИС и сетей, выбор программных и аппаратных средств защиты, разработка защищенных ИС, создание и сопровождение системных политик ИБ	Отдел ИТ, Директор по ИТ, Директор по ИБ	защищенные ОС, средства резервного копирования, антивирусные средства, межсетевые экраны, средства организации VPN и т. д.
	администра-тивный	реализация системных политик ИБ, работа с пользователями	Отдел ИБ, Отдел ИТ, системный администратор	повышение квалификации и тренинги по ИБ, парольная защита, политики разграничения доступа, и т д.
	технический	конфигурирование и поддержка программных и аппаратных средств защиты	Отдел ИТ, системный администратор	штатные средства ОС, СУБД, приложений и аппаратуры

Подходы к построению систем организационного обеспечения ИБ

- **ISO/IEC 27000**
  - начало 2010 г. – более 12 000 сертификатов в мире по ISO/IEC 27001
  - в России приняты ГОСТ Р ИСО/МЭК 27001–2006 и ГОСТ Р ИСО/МЭК 17799–2005
  - методология лежит в основе СТО БР ИББС ЦБ РФ
- **IT-Grundschutz-Kataloge (IT Baseline Protection Catalogs)**
  - СУИБ по стандарту разрабатывается редко, в основном в Германии (менее 20 сертификаций в год)
- **Standard of Good Practice for Information Security**
  - отсутствует процессный или какой-либо другой подход, обеспечивающий системность внедрения и применения стандарта в организации
- **Information Security Management Maturity Model (ISM3)**
  - методика не стандартизирована и не имеет широкого применения

Объект исследования

Методология организационного обеспечения ИБ, представленная в семействе стандартов ISO/IEC 27000

Предмет исследования

- **словарь, содержащий концепты, представленные в стандарте ISO/IEC 27000, разделе «Термины и определения» стандартов ISO/IEC 27001 – ISO/IEC 27006**
- **требования к СУИБ и СУРИБ, представленные в стандартах ISO/IEC 27001 и ISO/IEC 27005:**
  - **функциональные требования** – требования к наличию определенных процессов, их входам и выходам;
  - **информационные требования** – требования к наличию определенных информационных элементов, определенным типам этих элементов, а также к наличию определенных процессов, порождающих и использующих эти элементы;
  - **внешние требования** – требования к наличию определенных внешних сущностей, а также к наличию информационных обменов этих внешних сущностей с СУИБ или СУРИБ.

Функциональные и информационные требования связаны и перекрываются друг другом: один и тот же документ или процесс может одновременно входить в одно или несколько информационных требований и одно или несколько функциональных требований

Структура доклада

1. Объект и предмет исследования
2. **Актуальность темы, цели и задачи работы**
3. Описание разработанных моделей и методов их построения
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. Описание методов применения объектных моделей
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Сложность внедрения систем управления ИБ на практике

1. **Отсутствие единообразного формализованного представления всей совокупности требований к СУИБ;**
2. **Слабость методической поддержки процессов внедрения стандартов семейства ISO/IEC 27000;**
3. **Недостатки стандартов семейства ISO/IEC 27000:**
   - нечеткость базовых понятий и их связей в стандартах и нормативных документах;
   - нечеткость описания структуры процессов и документов в стандартах и нормативных документах;
   - неполная согласованность стандартов в рамках одного семейства, стандартов с другими нормативных документами.
4. **Отсутствие информации о полноте выполнения требований стандартов инструментальными средствами поддержки СУИБ и открытых методов проверки такой полноты.**

Предлагаемые в работе модели и методы позволяют существенно ослабить влияние перечисленных факторов

Обзор литературы

В ряде российских и зарубежных работ частичные модели требований ИБ (как правило – полуформальные) используются для решения частных практических задач, таких как:

- **разработка и внедрение процессов СУИБ** (Курило А. П., Машкина И.В., Костина А.Б., Милославская Н.Г.);
- **инвентаризация и категорирование защищаемых активов** (Кудрявцева Р. Т.);
- **разработка систем поддержки процессов внедрения и функционирования СУИБ** (Машкина И.В., Białas A.);
- **разработка методик и инструментальных средств оценки и управления рисками ИБ** (Львова А.В., Neubauer T., Ekelhart A., Fenz S.);
- **документирование результатов процессов оценки рисков ИБ** (Houmb S.-V., Braber F., Vraalsen F.);
- **проведение аудитов информационной безопасности** (Ерохин С.С.).

Обзор литературы: выводы

1. **Для решения каждой конкретной практической задачи** обеспечения ИБ **разрабатывается отдельная фрагментарная (частичная) модель** (как правило, полуформальная);
2. **Фрагментарные (частичные)** функциональные и объектные **модели СУИБ описывают отдельные компоненты СУИБ с узкими целями, с различных точек зрения, с разной детализацией** и по разным (часто не публикуемым) методикам
3. **Частичность и существенное различие в базовых параметрах моделей не допускают их повторного использования при решении других задач** обеспечения ИБ, для которых данные модели не разрабатывались (в том числе задач, близких по целям)
4. Используемые **частичные модели не проверены на соответствие стандартам**, что увеличивает вероятность получения не соответствующих стандарту решений

Цель и задачи исследования

Цель работы: создание методической базы для разработки и совершенствования организационных систем управления информационной безопасностью (СУИБ) в виде совокупности формализованных моделей требований к СУИБ, методов их построения и применения

Для достижения поставленной цели необходимо решить следующие задачи:

1. **Разработать полуформальные модели требований к СУИБ и СУРИБ;**
2. **Разработать полуформальную концептуальную модель методологии СОИБ;**
3. **Разработать методы применения построенных моделей в следующих задачах внедрения СУИБ в организациях:**
   - проектирование СУИБ;
   - проверка соответствия программного обеспечения поддержки СУИБ требованиям стандартов ИБ;
   - анализ, коррекция и согласование словаря стандартов семейства ISO/IEC 27000

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. **Описание разработанных моделей и методов их построения**
   - **объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения**
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ (СОИБ) и метод ее построения
4. Описание методов применения объектных моделей
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Объектная модель требований к системе управления ИБ

Представление информационных элементов в объектной модели требований к СУИБ

Информационный элемент –

группа документов СУИБ, документ СУИБ или раздел документа СУИБ, имеющий самостоятельное значение

Типы информационных элементов:

- **документ** – содержит информацию о целях, намерениях, мотивациях, условиях или состоянии определенной деятельности
- **политика** – **содержит информацию о требованиях к определенной деятельности, рекомендации и ответственность по их реализации; как правило ограничена конкретной областью применения; часто развивает определенный документ**
- **процедура** – **содержит информацию о методах, алгоритмах и средствах выполнения определенной деятельности; обычно создается в поддержку** определенной политики
- **запись** – **содержит свидетельствующую информацию о действиях, событиях, их результатах и последствиях; часто порождается в ходе выполнения некоторой процедуры**
- **группа нескольких документов**

Представление информационного элемента в модели:

Представление функциональных элементов в объектной модели требований к СУИБ

Функциональный элемент (процесс) –

регламентируемая стандартом деятельность в виде процесса, который может потреблять, преобразовывать и порождать информационные ресурсы

Типы функциональных элементов:

- **элементарный** – функциональный элемент, структура которого не детализирована в стандарте
- **структурированный** – функциональный элемент, который согласно стандарту включает в себя группу других функциональных элементов

Представление информационного элемента в модели:

элементарный **структурированный**

Представление внешних элементов в объектной модели требований к СУИБ

Внешний элемент (внешняя сущность) –

сущность, не входящая в состав СУИБ и взаимодействующая с СУИБ посредством обмена информационными элементами

Внешние элементы СУИБ:

- **Организация**
- **Высшее руководство**
- **Заинтересованные стороны**
- **Правовая среда**
- **Каталог контрмер ИБ**
- **Внешние источники информации**
- **Международный стандарт ISO/IEC 27001:2005**

Представление внешнего элемента в модели:

Представление связей информационных элементов в объектной модели требований к СУИБ

1. **Информационные элементы связаны через функциональные элементы (процессы)**

2. **Информационные элементы связаны отношением группировки («целое–часть»)**

Представление связей функциональных элементов в объектной модели требований к СУИБ

1. **Функциональные элементы (процессы) связаны через информационные элементы**

2. **Функциональные элементы (процессы) образуют иерархию**
   (под иерархией понимается отношение композиции/вложенности)

Представление информационных требований в объектной модели требований к СУИБ

Информационное требование –
совокупность, включающая:

- **требование к наличию в организации определенного информационного элемента;**
- **требование к содержанию этого элемента;**
- **требование к структуре этого элемента** (требования к наличию отношений группировки с другими информационными элементами);
- **требование к наличию определенного процесса или внешней сущности, которая порождает этот элемент;**
- **одно или несколько требований к наличию определенных процессов или внешних сущностей, которые используют этот элемент.**

Представление информационных требований в объектной модели требований к СУИБ

Пример представления информационного требования «Список угроз ИБ» в стандарте

- ***Организация должна <…> идентифицировать угрозы для активов*** [ISO/IEC 27001, 4.2.1d)2)]
- ***Организация должна пересматривать оценки рисков, учитывая изменения <…> в выявленных угрозах*** [ISO/IEC 27001, 4.2.3d)4)]
- ***Документы, необходимые для СУИБ, должны быть защищены и находиться под контролем*** [ISO/IEC 27001, 4.3.2]

Пример представления информационного требования «Список угроз ИБ» в модели

Представление функциональных требований в объектной модели требований к СУИБ

Функциональное требование –
совокупность, включающая:

- **требование к наличию в организации определенного процесса;**
- **требование к содержанию этого процесса;**
- **требование к структуре этого процесса** (требования к наличию отношения подчинения с другими процессами);
- **одно или несколько требований к наличию на входе процесса определенных информационных элементов;**
- **одно или несколько требований к наличию на выходе процесса определенных информационных элементов.**

Представление функциональных требований в объектной модели требований к СУИБ

Пример представления функционального требования «Определение области действия СУИБ» в стандарте

- Этап ***планирования (разработка СУИБ): Определение политики, целей, процессов и процедур СУИБ <…> для достижения результатов в соответствии с общей политикой и целями организации*** [ISO/IEC 27001, 0.2]
- ***Организация должна <…> определить область действия и границы СУИБ с учетом характеристик бизнеса, организации, ее местоположения, активов и технологий, а также подробности и обоснование для любых исключений из области действия*** [ISO/IEC 27001, 4.2.1a)]

Пример представления функционального требования «Определение области действия СУИБ» в модели

Представление внешних требований в объектной модели требований к СУИБ

Внешнее требование –

совокупность, включающая:

- **требование к наличию определенного внешнего элемента;**
- **одно или несколько требований к наличию определенных информационных элементов, которые порождаются этой внешней сущностью и используются СУИБ;**
- **одно или несколько требований к наличию определенных информационных элементов, которые порождаются СУИБ и используются этой внешней сущностью.**

Представление внешних требований в объектной модели требований к СУИБ

Пример представления внешнего требования «Руководство организации» в стандарте ISO/IEC 27001

- **Организация должна <…> определит ь полит ику СУИБ, кот орая: <…> ут верждает ся руководст вом организации.** [ISO/IEC 27001, 4.2.1b)]
- **Организация должна <…> получит ь ут верждение руководст вом предполагаемых ост ат очных рисков.** [ISO/IEC 27001, 4.2.1h)]
- **Организация должна <…> получит ь разрешение руководст ва на внедрение и эксплуат ацию СУИБ.** [ISO/IEC 27001, 4.2.1i)]

Пример представления внешнего требования «Руководство организации» в модели

Метрики объектной модели требований к системе управления ИБ

Пакет объектной модели	Кол-во классов	Кол-во процессов	Кол-во диаграмм
Пакет функциональных требований	0	50	11
Пакет информационных требований	84	0	2
Пакет внешних требований	7	0	0
Итого в модели	**91**	**50**	**13**

В объектной модели требований к СУИБ представлено:

- **82 информационных требования**
- **49 функциональных требований, из них 40 элементарных**
- **7 внешних требований**

Метод построения объектной модели требований к системе управления ИБ

Основан на методе функционального моделирования SADT, модифицированного с учетом следующих факторов:

1) **специфика объекта моделирования:**
   a. структура разделов и подразделов стандарта ISO/IEC 27001 составляет основу иерархии требуемых процессов;
   b. некоторые требования и их связи представлены в стандарте неявно, отдельные требования дублируются.
2) **использование UML в качестве языка моделирования (вместо IDEF0/DFD, для которых разрабатывалась методика SADT):**
   a. функциональные блоки модели представляются с помощью элементов Activity;
   b. ресурсы, а также внешние сущности и хранилища данных представляются с помощью элементов Class;
   c. порождение и использование ресурсов функциональными блоками представляется с помощью отношения Information flow;
   d. слияние и ветвление ресурсов представляется на диаграммах классов пакета ISMS information requirements с помощью отношения группировки (aggregation).

Метод построения объектной концептуальной модели методологии систем обеспечения ИБ

1. **Представление внешних требований;**
2. **Представление и анализ функциональных элементов СУИБ:**
3. **Представление и анализ информационных элементов СУИБ.**

Представление элемента:

- именование элемента;
- определение элемента.

Анализ элементов:

- проверка непересекаемости;
- проверка полноты;
- представление связей элементов.

Метод построения объектной концептуальной модели методологии систем обеспечения ИБ

I. **Представление и анализ внешних требований:**
   1.1. Представление и анализ внешних элементов СУИБ;
   1.2. **Представление и анализ информационных элементов СУИБ, связанных с внешними элементами по входу и выходу**

В результате: **модель внешних требований СУИБ (пакет)**

II. **Представление и анализ функциональных элементов СУИБ:**
   1.1. Представление функциональных элементов СУИБ;
   1.2. **Анализ функциональных элементов СУИБ**

В результате: **иерархия функциональных элементов (по отношению композиции)**

Метод построения объектной концептуальной модели методологии систем обеспечения ИБ

III. Представление и анализ информационных элементов СУИБ в каждом узле иерархии функциональных элементов СУИБ:

1.1. **Анализ вложенных в узел функциональных элементов**;

1.2. **Представление и анализ информационных элементов СУИБ, связанных с вложенными функциональными элементами по входу и выходу**

В результате:

- группа функциональных требований, связанных с вложенными в узел функциональными элементами (представляется диаграммой Activity узла)
- иерархия функциональных элементов СУИБ (по отношению композиции)

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. **Описание разработанных моделей и методов их построения**
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - **объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения**
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. Описание методов применения объектных моделей
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Объектная модель требований к системе управления рисками ИБ

Для построения ОМ требований к СУРИБ использовался метод, аналогичный методу построения ОМ требований к СУИБ, с минимальной модификацией, состоящей в изменении названий этапов и шагов.

Представление элементов в объектной модели требований к СУРИБ

Информационные, функциональные и внешние элементы СУРИБ представляются в объектной модели таким же образом, как информационные, функциональные и внешние элементы СУИБ

В объектной модели требований к СУРИБ представлены 3 рода элементов:

- **информационные и функциональные элементы СУРИБ, идентичные по содержанию элементам СУИБ**
- **информационные и функциональные элементы СУРИБ, являющиеся частным случаем элементов СУИБ**
- **информационные и функциональные элементы СУРИБ, не имеющие аналогов среди элементов СУИБ**

Представление требований в объектной модели требований к СУРИБ

Информационные, функциональные и внешние требования к СУРИБ представляются в объектной модели таким же образом, как информационные, функциональные и внешние требования к СУРИБ

В объектной модели требований к СУРИБ представлены 3 рода требований:

- **информационные, функциональные и внешние требования к СУРИБ, которые идентичны по содержанию требованиям к СУИБ;**
- **информационные, функциональные и внешние требования к СУРИБ, которые детализируют требования к СУИБ;**
- **информационные, функциональные и внешние требования к СУРИБ, которые не охвачены требованиями к СУИБ.**

Метрики объектной модели требований к системам управления рисками ИБ

Пакет объектной модели	Кол-во классов	Кол-во процессов	Кол-во диаграмм
Пакет функциональных требований	0	34	11
Пакет информационных требований	49	0	2
Пакет внешних требований	3	0	0
Итого в модели	**52**	**34**	**12**

В объектной модели требований к СУРИБ представлено:

- **48 информационных требования**
- **33 функциональных требований, из них 24 элементарных**
- **3 внешних требований**

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. **Описание разработанных моделей и методов их построения**
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - **объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения**
4. Описание методов применения объектных моделей
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Объектная концептуальная модель методологии систем обеспечения ИБ

(фрагмент)

Всего в модели: 58 концептов, 81 отношение

Метод построения объектной концептуальной модели методологии систем обеспечения ИБ

1. **Моделирование концептуальной схемы, описанной в стандарте ISO/IEC 27000:**
   1.1. Создание элементов Class и Activity, соответствующих определенным в стандарте концептам;
   1.2. Выявление отношений между концептами, размещение концептов и отношений на диаграмме классов.
2. **Уточнение и дополнение концептуальной схемы на основе остальных стандартов семейства (ISO/IEC 27001 – ISO/IEC 27006):**
   2.1. Добавление в модель концептов и отношений, отсутствующих в словаре стандарта ISO/IEC 27000, из остальных стандартов семейства;
   2.2. Уточнение концептов, присутствующих в словарях нескольких стандартов. Формы уточнения включают:
   - принятие определения концепта из стандарта ISO/IEC 27000;
   - фиксацию нескольких определений для их дальнейшей коррекции или согласования;
   - копирование информации из определения одного концепта в определение другого концепта.

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. Описание разработанных моделей и методов их построения
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. **Описание методов применения объектных моделей**
   - **в задаче проектирования СУИБ малой/средней организации**
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Задача проектирования системы управления ИБ организации

Исходные данные:

- **малая или средняя организация, в которой существуют отдельные компоненты обеспечения ИБ на организационно-управленческом уровне;**
- требования к СУ**ИБ, представленные в стандарте ISO/IEC 27001:2005.**

Необходимо:

- разработать проект и план внедрения СУИБ организации, удовлетворяющей требованиям стандарта.

Существующая практика проектирования системы управления ИБ

1. **Подход, основанный на собственных методиках организаций и консультантов**
   - осложняется недостатками стандарта ISO/IEC 27001;
   - существенные временные, трудовые и материальные затраты.
2. **Подход, основанный на стандарте ISO/IEC 27003**
   - стандарт ISO/IEC 27003 существенно усиливает и расширяет требования стандарта ISO/IEC 27001;
   - стандарт ISO/IEC 27003 предлагает длительную и дорогостоящую процедуру реализации СУИБ.

Перечисленные подходы эффективны в крупных организациях, но имеют ограниченное применение в малых и средних организациях вследствие следующих особенностей:

- **значительный разрыв между текущим уровнем ИБ и уровнем ИБ, требуемым для сертификации;**
- **существенное ограничение в ресурсах.**

Метод применения ОМ требований к СУИБ в задаче проектирования СУИБ

1. **Предпроектное обследование существующих компонентов СУИБ**

   Методы сбора информации: чтение и анализ документации, опрос ответственных лиц, наблюдение за деятельностью по обеспечению ИБ.

2. **Разработка объектной модели СУИБ организации путем конкретизации объектной модели требований к СУИБ**

   Замена общих имен и описаний элементов объектной модели требований к СУИБ именами и описаниями существующих и планируемых компонентов СУИБ;

   Представление требований, выполненных частично, и невыполненных требований, особым образом:

   - к именам процессов и информационных элементов, соответствующих не всем требованиям стандарта, добавляется классификатор «[mod]», невыполненные требования перечисляются в описаниях;
   - к именам процессов и информационных элементов, требуемых стандартом, но отсутствующих в организации, добавляется классификатор «[add]».

3. **Формирование перечня задач, необходимых для построения СУИБ, соответствующей требованиям стандарта ISO/IEC 27001**

Метод применения ОМ требований к СУИБ в задаче проектирования СУИБ

Эффективность применения объектных моделей в задаче проектирования СУИБ

Критерий оценки эффективности – уровень зрелости СУИБ

Метод расчета уровня зрелости СУИБ основан на модифицированном методе расчета уровней зрелости и результативности СМК.

Принятые модификации состоят в следующем:

- В качестве показателей зрелости СУИБ **используются 16 групповых показателей ИБ** (включающие в себя 109 частных показателей ИБ), выбранные **из стандарта СТО БР ИББС–1.2–2007**
- Фактические значения частных показателей ИБ **оцениваются по шкале из стандарта СТО БР ИББС–1.2–2007**, при их расчете **учитываются коэффициенты значимости каждого частного показателя**, определенные в стандарте СТО БР ИББС–1.2–2007

Метод расчета уровня зрелости систем управления ИБ

1. **Определение фактических значений частных показателей** $K_{\Phi i}$ по шкале $\{0;\ 0{,}25;\ 0{,}5;\ 0{,}75\}$, предложенной в стандарте СТО БР ИББС–1.2–2007

2. **Вычисление значения каждого группового показателя**

$$E = \sum_{i=1}^{n} \frac{K_{\Phi_i}}{K_{П_i}} \alpha_i \quad (1)$$

n – количество частных показателей ИБ, входящих в данный групповой показатель ИБ;

$K_{\Phi i}$ – фактическое значение i-го частного показателя ИБ;

$K_{П i}$ – нормативное (максимально возможное) значение i-го частного показателя ИБ;

α_i – коэффициент значимости i-го частного показателя ИБ.

3. **Вычисление общего уровня зрелости СУИБ**

$$P_{СУИБ} = \frac{1}{N} \sum_{j=1}^{N} E_j \quad (2)$$

где N – количество групповых показателей ИБ.

Результаты применения объектной модели для проектирования СУИБ ЗАО «СетКом»

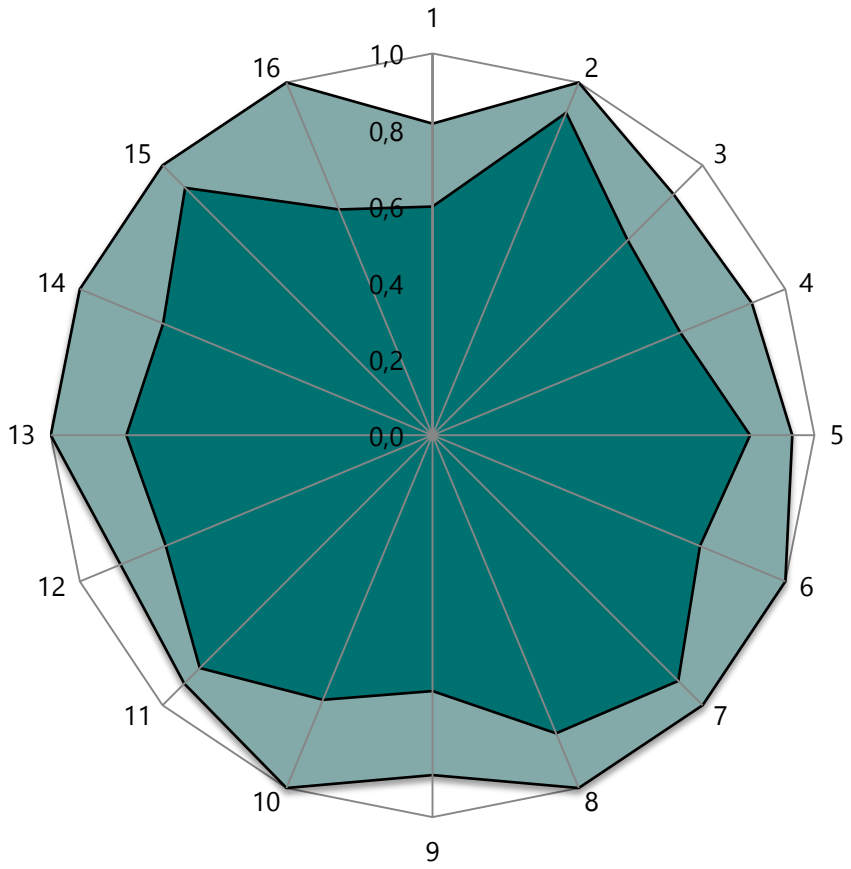
1. **Разработана объектная модель СУИБ организации**, представляющая структуру процессов и документации собственной СУИБ, отвечающую требованиям стандарта ISO/IEC 27001
2. **Подготовлен план внедрения СУИБ в организации**, включающий перечень задач, которые необходимо выполнить для достижения соответствия стандарту ISO/IEC 27001, ответственных лиц и сроков выполнения задач

- **разработка 10 документов СУИБ**: документированная процедура выполнения превентивных действий; положение о применимости; …
- **модификация 3 документов СУИБ**: политика ИБ (определить сроки и ответственность за пересмотр политики), процедура управления записями СУИБ (определить порядок восстановления записей), …
- **разработка 9 форм регистрации записей СУИБ**: записи внутренних аудитов ИБ, записи улучшения эффективности СУИБ, …
- **внедрение 14 процессов СУИБ**: определение подхода к оценке рисков ИБ, идентификация рисков ИБ, вычисление и оценивание рисков ИБ, …
- **изменение порядка выполнения 6 процессов**: улучшение эффективности СУИБ: добавить функции по обновлению планов оценки и обработки рисков, улучшению методов проверки эффективности СУИБ; …

Эффективность применения объектной модели для проектирования СУИБ ЗАО «СетКом»

Уровень зрелости СУИБ, спроектированной с использованием объектной модели требований к СУИБ, 0,953

Уровень зрелости СУИБ, спроектированной без использования объектных моделей, 0,778



ОМ требований к СУИБ обеспечивает методическую поддержку для повышения уровня зрелости СУИБ до (0,953-0,778)*100% = 17,5%.

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. Описание разработанных моделей и методов их построения
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. **Описание методов применения объектных моделей**
   - в задаче проектирования СУИБ малой/средней организации
   - **в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов**
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. Заключение, выводы и перспективы работы

Задача проверки соответствия ПО поддержки СУИБ требованиям стандартов ИБ

Исходные данные:

- **информация о функциональности ПО: интерфейс ПО, документация, описание опыта разработки и использования**
- информация о функциональных и информационных требованиях стандарта ИБ.

Необходимо:

- количественно оценить соответствие ПО поддержки СУИБ требованиям стандарта ИБ.

Метод применения ОМ требований к СУРИБ в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов

1. **Представление иерархии процессов, поддерживаемых ПО, и связанных с ними информационных элементов в виде объектной модели**
2. **Анализ и представление в ОМ соответствий процессов и информационных элементов, поддерживаемых ПО, функциональным и информационным требованиям к СУРИБ**
   - полное соответствие – отношение двунаправленной ассоциации;
   - частичное соответствие – отношение однонаправленной ассоциации.
3. **Вычисление степени соответствия ПО стандарту на основе выявленных соответствий**
   - степень соответствия ПО функциональным требованиям $C_f = \sum_{j=1}^{N_f} a_j v_j$
   - степень соответствия ПО информационным требованиям $C_i = \sum_{k=1}^{N_i} b_k w_k$

a_j, b_k – степень выполнения требований, v_j, w_k – весовые коэффициенты

Метод применения ОМ требований к СУРИБ в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов

Степень выполнения функционального требования

a_j	**Критерий определения степени выполнения функционального требования**
0	Процесс, к которому относится функциональное требование, не поддерживается инструментальным средством
0,5	Процесс, к которому относится функциональное требование, поддерживается инструментальным средством в неполном объеме
1	Процесс, к которому относится функциональное требование, полностью поддерживается инструментальным средством

Степень выполнения информационного требования

b_k	**Критерий определения степени выполнения информационного требования**
0	Информационный элемент, к которому относится информационное требование, не поддерживается инструментальным средством
0,5	Информационный элемент, к которому относится информационное требование, поддерживается инструментальным средством, но используется не во всех процессах, в которых его использование регламентировано стандартом
1	Информационный элемент, к которому относится информационное требование, поддерживается инструментальным средством и используется во всех процессах, в которых этого требует стандарт

Результаты использования метода для проверки соответствия ПО CORAS Tool и ПО MEHARI требованиям ISO/IEC 27005

ПО CORAS Tool:

- поддерживает 15 из 18 процессов (5 – частично);
- поддерживает 23 из 43 информационных элемента (4 – частично);
- $C_{f\,CORAS} = 0{,}70;\ C_{i\,CORAS} = 0{,}48$

ПО MEHARI:

- поддерживает 18 из 18 процессов (4 из них – частично);
- поддерживает 38 из 43 информационных элементов (3 – частично);

$$C_{f\,MEHARI} = 0{,}89;\ C_{i\,MEHARI} = 0{,}84$$

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. Описание разработанных моделей и методов их построения
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. **Описание методов применения объектных моделей**
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - **в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000**
5. Заключение, выводы и перспективы работы

Недостатки словаря стандартов семейства ISO/IEC 27000

Существующие процессы разработки и пересмотра международных стандартов не позволяют в полной мере выявлять и устранять недостатки стандартов. Это подтверждается наличием в семействе стандартов ISO/IEC 27000 следующих недостатков:

- **неполнота словаря**
  - Отсутствуют концепты «Политика СУИБ», «Цели СУИБ», «Политика информационной безопасности», «Цель контрмеры ИБ» и др.
- **некорректность некоторых определений**
  - В определении концепта «Доступность» не указан концепт, свойством которого он является
- **противоречия между определениями терминов и другими положениями стандартов**
  - Согласно определению процесс «Управление рисками» включает 4 подпроцесса, однако в его подробном описании указано 6 подпроцессов
- **несогласованность определений концептов между стандартами семейства.**
  - Концепты «Руководство» и «Целостность» имеют разные определения в разных стандартах

Примеры недостатков словаря стандартов семейства ISO/IEC 27000

Концепты «Информация» и «Информационный актив» отождествляются (для концептов дано одно определение, они взаимозаменяются в словаре и тексте стандартов):

- *NOTE: There are many types of assets, including: a) information (2.18) [ISO/IEC 27000, 2.3]*
- *2.18* information asset *– knowledge or data that has value to the organization [ISO/IEC 27000, 2.18]*

Для концепта «Доступность» не указано, свойством чего он является:

- *availability – property of being accessible and usable upon demand by an authorized entity [ISO/IEC 27000, 2.7]*

Определение концепта «Руководство» не согласовано между стандартами ISO/IEC 27000 и ISO/IEC 27002:

- *guideline – recommendation of what is expected to be done to achieve an objective [ISO/IEC 27000:2009, 2.16]*
- *guideline – a description that clarifies what should be done and how, to achieve the objectives set out in policies [ISO/IEC 27002:2005, 2.3]*

Метод использования объектной концептуальной модели методологии СОИБ для анализа, коррекции и согласования словаря семейства стандартов ISO/IEC 27000

1. **Коррекция и согласование концептуальной схемы, представленной в объектной концептуальной модели методологии СОИБ**
   - 2.1. Устранение несоответствий в определениях концептов на **диаграммах классов, размещенных в новом пакете модели;**
   - 2.2. Согласование определений концептов **на диаграммах классов, размещенных в новом пакете модели;**
2. **Выработка предложений по коррекции и согласованию определений концептов в текстах стандартов семейства ISO/IEC 27000**
   - 3.1. Выявление определений концептов, которые необходимо добавить, на основе определений связанных концептов и текстов стандартов;
   - 3.2. Формулировка модификаций определений концептов, которые содержат несоответствия или не согласованы, на основе словаря и текстов стандартов;
   - 3.3. Выявление определений и контекста использования концептов, которые предлагается объединить.

Результаты использования объектной концептуальной модели методологии СОИБ для анализа, коррекции и согласования словаря семейства стандартов ISO/IEC 27000

Сформулированы конкретные предложения

- **по устранению 13 несоответствий в концептуальной схеме семейства стандартов**, которые связаны с концептами «Актив», «Риск», «Управление рисками», «Сертификат», «Организация», «Высшее руководство», «Документ», «Политика ИБ»

- **по согласованию определений 2 концептов**: «Руководство» и «Целостность»

Результаты использования объектной концептуальной модели методологии СОИБ для анализа, коррекции и согласования словаря семейства стандартов ISO/IEC 27000

Пример предложений по устранению несоответствий, связанных с концептом «Актив»

- **Добавить концепт «Информационный актив» в словари стандартов ISO/IEC 27001, ISO/IEC 27002** со следующим определением: Information asset – information that has value for organization and related information processing facilities.
- **Заменить существующее определение концепта «Информационный актив» в словаре стандарта ISO/IEC 27000** вышеприведенным определением;
- **Добавить концепт «Информация» в словари стандартов ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002** со следующим определением: Information – meaningful knowledge or data.
- **Перенести из определения концепта «Актив» в определение концепта «Информационный актив» в стандарте ISO/IEC 27000 следующее примечание**: NOTE There are many types of information assets, including: a) information; b) software, such as a computer program; c) physical, such as computer; d) services; e) people, and their qualifications, skills, and experience; and f) intangibles, such as reputation and image.
- **Добавить концепт «Средства обработки информации» в словари стандартов ISO/IEC 27000 и ISO/IEC 27001** со следующим определением: Information processing facilities – any information processing system, service or infrastructure, or the physical locations housing them.
- …

Структура доклада

1. Объект и предмет исследования
2. Актуальность темы, цели и задачи работы
3. Описание разработанных моделей и методов их построения
   - объектная модель требований к системе управления ИБ (СУИБ) и метод ее построения
   - объектная модель требований к системе управления рисками ИБ (СУРИБ) и метод ее построения
   - объектная концептуальная модель методологии систем обеспечения ИБ и метод ее построения
4. Описание методов применения объектных моделей
   - в задаче проектирования СУИБ малой/средней организации
   - в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов
   - в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000
5. **Заключение, выводы и перспективы работы**

Результаты работы

1. **Объектная модель требований к СУИБ по стандарту ISO/IEC 27001 и метод ее построения;**
2. **Объектная модель требований к СУРИБ по стандарту ISO/IEC 27005;**
3. **Объектная концептуальная модель методологии СОИБ по семейству стандартов ISO/IEC 27000 и метод ее построения;**
4. **Метод применения объектной модели требований к СУИБ в задаче проектирования СУИБ малых и средних организаций;**
5. **Метод применения объектной модели требований к СУРИБ в задаче проверки соответствия ПО поддержки СУИБ организации требованиям стандартов ИБ;**
6. Метод применения объектной концептуальной модели методологии СОИБ в задаче анализа, согласования и коррекции словаря стандартов семейства ISO/IEC 27000;
7. Метод расчета уровня зрелости СУИБ, разработанной с использованием объектной модели требований к СУИБ.

цветом выделены научные положения, выносимые на защиту

Заключение

1. **Разработаны следующие полуформальные модели компонентов системы обеспечения ИБ организации:**
   - **объектная модель требований к системе управления информационной безопасностью по стандарту ISO/IEC 27001:2005 и метод ее построения;**
   - **объектная модель требований к системе управления рисками информационной безопасности по стандарту ISO/IEC 27005:2008;**
   - **объектная концептуальная модель методологии СОИБ по семейству стандартов ISO/IEC 27000 и метод ее построения.**
2. **Разработан и реализован метод применения объектной модели требований к СУИБ в задаче проектирования СУИБ;**
3. **Разработан и реализован метод применения объектной модели требований к СУРИБ в задаче проверки соответствия ПО поддержки СУИБ требованиям стандартов ИБ;**
4. **Разработан и реализован метод применения объектной концептуальной модели методологии СОИБ в задаче анализа, коррекции и согласования словаря стандартов семейства ISO/IEC 27000.**

Выводы

Разработанные в работе объектные модели и методы их построения и применения:

1. **представляют все требования стандартов ISO/IEC 27001, ISO/IEC 27005 в единообразной формализованной форме;**
2. **усиливают методическую поддержку и повышают эффективность процессов внедрения стандарта ISO/IEC 27001 в малых и средних организациях, включая задачу анализа, коррекции и согласования нормативно-методической документации в области ИБ;**
3. **позволяют полностью устранить на объектных моделях и частично в текстах следующие недостатки стандартов данного семейства:**
   - нечеткость базовых понятий и их связей;
   - нечеткость описания структуры процессов и документов;
   - неполная согласованность стандартов в рамках одного семейства.
4. **дают возможность оценить полноту выполнения требований стандартов ИБ инструментальными средствами, в частности – инструментальными средствами анализа и управления рисками ИБ.**
5. **демонстрируют возможность эффективного решения разнородных задач организационного обеспечения ИБ на единой методической основе (система согласованных полуформальных моделей методологии ИБ, методы их построения и применения).**

Перспективы использования результатов и развития работы

1. **Разработанные модели могут быть повторно использованы для** решения частных задач обеспечения информационной безопасности в рамках СОИБ, в частности задач:
   - аудита систем управления ИБ;
   - разработки проектных спецификаций для программного обеспечения поддержки СУИБ;
   - согласования международных, национальных, отраслевых и корпоративных стандартов в области ИБ, а также согласования нормативно-методической документации в области ИБ.
2. **Объектная концептуальная модель методологии СОИБ может быть использована в качестве основы для построения начальной онтологии методологии СОИБ;**
3. **Построенные в работе объектные модели и методы могут также использоваться при обучении и переподготовке специалистов в области управления информационной безопасностью**.

Список публикаций

1. **Черемушкин Д.В. Задача объектного моделирования системы управления информационной безопасностью. // Научно-технический вестник СПбГУ ИТМО. Выпуск 52. Прикладные информационные технологии. / Главный редактор д.т.н., проф. В.О. Никифоров. – СПб: СПбГУ ИТМО, 2008. – сс. 237–241.**
2. **Cheremushkin D.V., Lyubimov A.V. An application of integral engineering technique to information security standards analysis and refinement // Proceedings of the 3rd international conference on Security of information and networks. Taganrog, Rostov-on-Don, Russian Federation, September 07-11, 2010. – NY, USA: ACM. – сс. 12-18.**
3. **Черемушкин Д.В. Исследование вредоносного кода // Научно–технический вестник СПбГУ ИТМО. Выпуск 25. Исследования в области информационных технологий. / Главный редактор д.т.н., профессор В.Н. Васильев – СПб: СПбГУ ИТМО, 2006. – сс. 182-184.**
4. Черемушкин Д.В. Задача объектного моделирования системы управления информационной безопасностью. // Сборник тезисов V Всероссийской межвузовской конференции молодых ученых. – СПб: СПбГУ ИТМО, 2008. – с. 90.
5. Черемушкин Д.В. Полуформальное моделирование методологии стандарта ISO/IEC 27001. // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22-24 октября 2008 г.: Материалы конференции \ СПОИСУ. – СПб, 2008. – с. 115.
6. Черемушкин Д.В. Объектная модель общего контекста безопасности организации по семейству стандартов ISO/IEC 2700x. // Тринадцатая Санкт-Петербургская ассамблея молодых ученых и специалистов. Аннотации научных работ победителей конкурса грантов Санкт-Петербурга 2008 года для студентов, аспирантов, молодых ученых и молодых кандидатов наук. – СПб.: Фонд «ГАУДЕАМУС», 2008. – с. 114.
7. Черемушкин Д.В. Корректировка стандартов семейства ISO/IEC 27000 на основе объектной модели словаря. // Сборник трудов конференции молодых ученых, Выпуск 6. Информационные технологии / Главный редактор д.т.н., проф. В.Л. Ткалич. – СПб: СПбГУ ИТМО, 2009. – сс. 43–48.
8. Потравнов А.С., Черемушкин Д.В. Функциональное моделирование процесса управления рисками согласно стандарту ISO/IEC 27005:2008 // Информационная безопасность регионов России (ИБРР-2009). VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)». Санкт-Петербург, 28-30 октября 2009 г.: Материалы конференции. СПОИСУ. – СПб, 2009. – с. 76.
9. Черемушкин Д.В. Объектное моделирование методологии семейства стандартов ISO/IEC 27000 // Четырнадцатая Санкт-Петербургская Ассамблея молодых ученых и специалистов. Аннотации работ победителей конкурса грантов Санкт-Петербурга 2009 года для студентов, аспирантов, молодых ученых и молодых кандидатов наук. – СПб.: Изд-во Политехн. ун-та, 2009. – с. 124.

Перечень докладов, грантов

- **Основные положения и результаты диссертационной работы доложены и обсуждены на следующих конференциях:**
  1. V Всероссийская межвузовская конференция молодых ученых, Санкт-Петербург, 15-18 апреля 2008 г.
  2. XI Санкт-Петербургская международная конференция «Региональная информатика-2008 (РИ-2008)», Санкт-Петербург, 22-24 октября 2008 г.
  3. VI Всероссийская межвузовская конференция молодых ученых, Санкт–Петербург, 14-17 апреля 2009 г.
  4. VI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2009)», Санкт-Петербург, 28-30 октября 2009 г.
  5. Third International Conference on Security of Information and Networks (SIN 2010), 7-11 September 2010, Southern Federal University, Russia, Taganrog

- **Работа поддержана грантами Правительства Санкт-Петербурга № 3.11/30-04/39 (2008 г.) и № 3.11/30-04/40 (2009 г.).**

Спасибо за внимание.