



Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук (СПИИРАН)

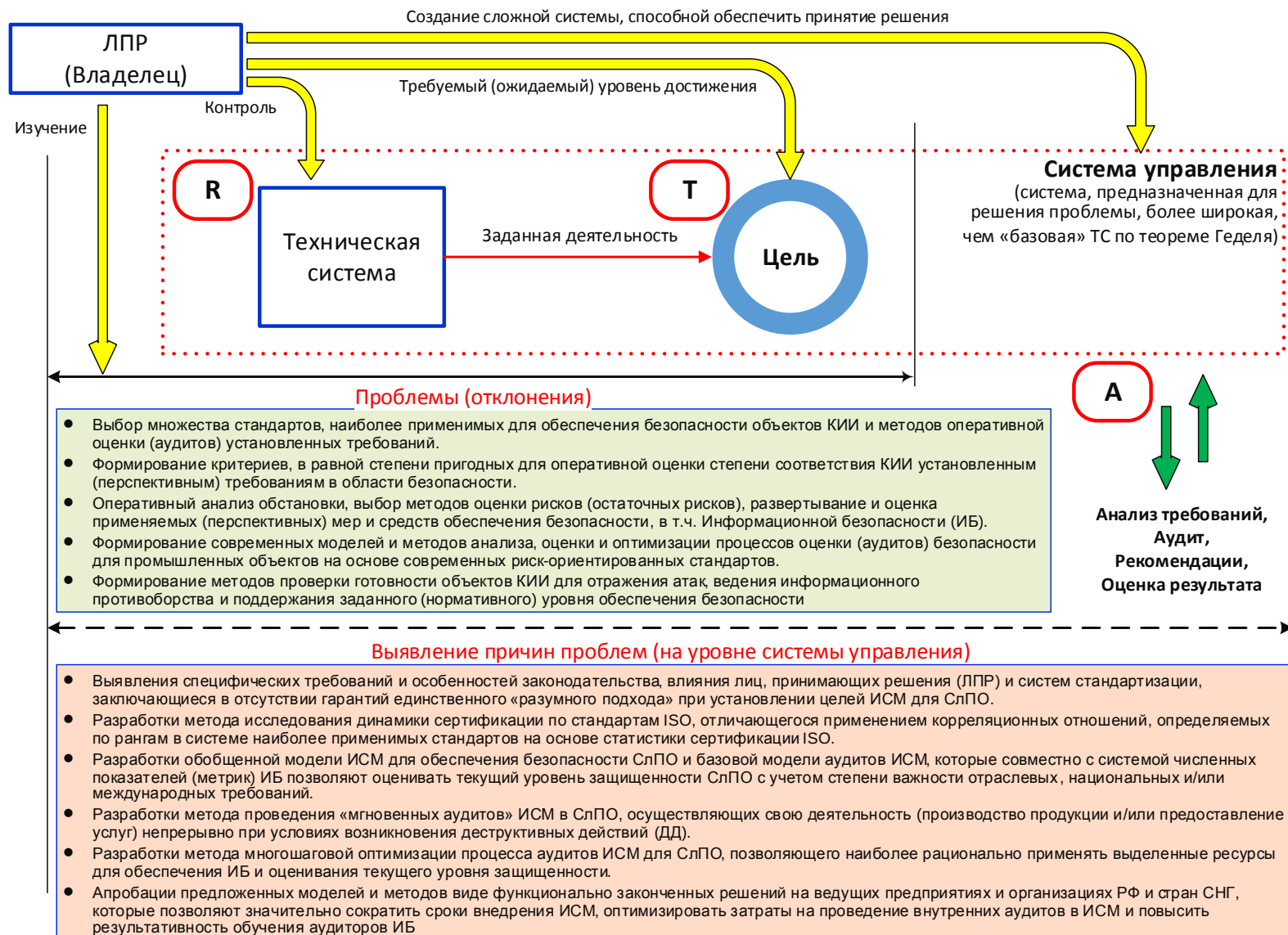


**Модели и методы аудита
информационной безопасности
интегрированных систем управления
для сложных промышленных объектов**

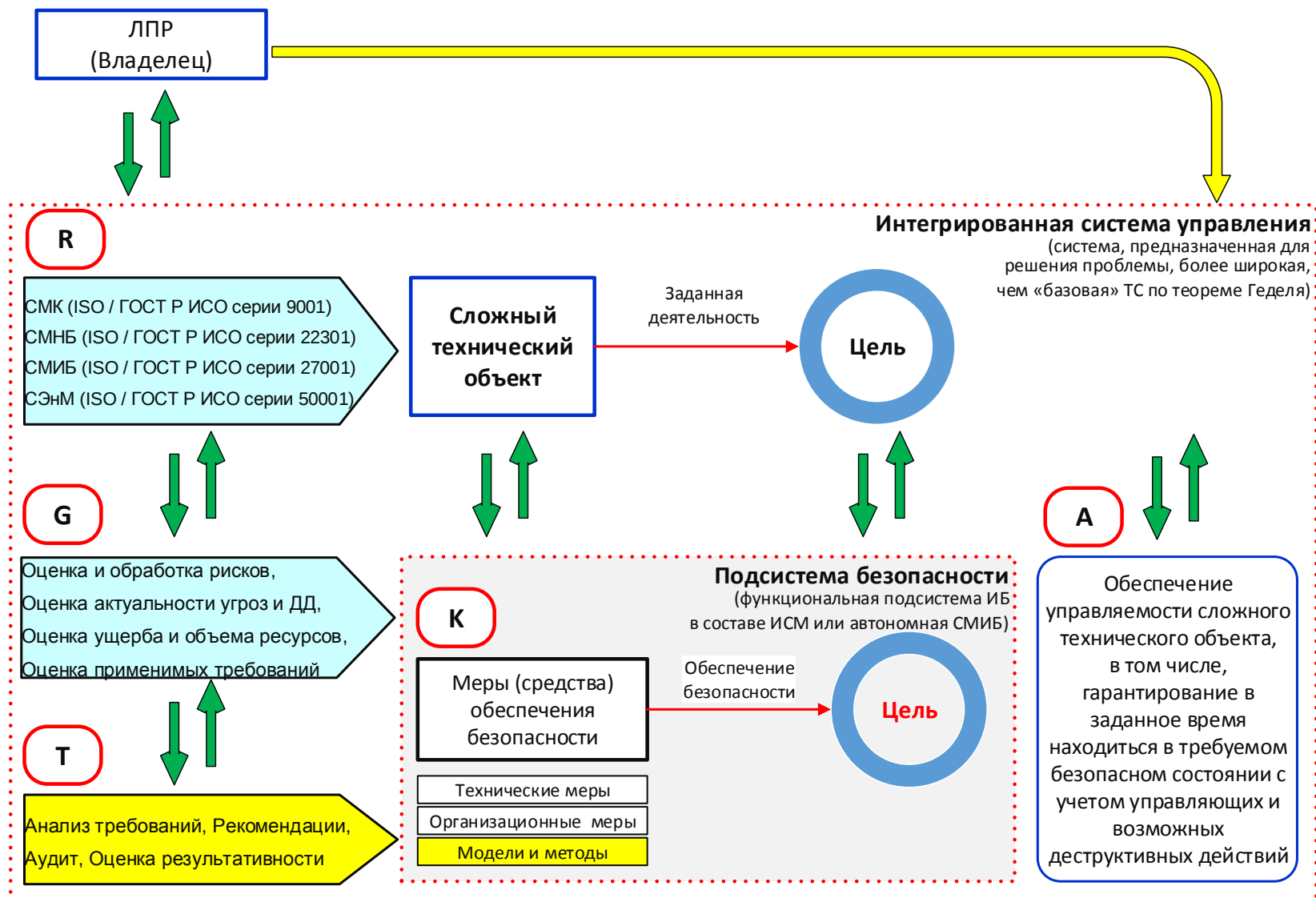
05.13.19 «Методы и системы защиты информации,
информационная безопасность»

Лившиц Илья Иосифович, 15.06.2018, г. Санкт-Петербург

Замысел исследования («как есть»)



Замысел исследования («как нужно»)





Общие характеристики исследования

- **Объект исследований**

Интегрированные системы менеджмента (в аспекте информационной безопасности) для сложных промышленных объектов.

- **Предмет исследований**

Методы анализа, оценки и оптимизации процессов оценки (аудита) ИБ для сложных промышленных объектов на основе современных риск-ориентированных стандартов.

- **Методы исследования**

В качестве основных методов исследования использованы методы системного анализа, методы декомпозиции и агрегирования, теории автоматизированного управления, теории множеств, теории вероятности, теории многокритериального выбора при фиксированном наборе альтернатив.



Актуальность исследования

- ♦ **Актуальность** исследования обусловлена вниманием к проблеме создания ИСМ для комплексного обеспечения безопасности объектов, именуемых «*сложными промышленными объектами*» – СлПО.
- * *Под термином СлПО, в исследовании понимается «технический объект, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями».*
- ♦ **Проведенный анализ** выполненных проектов создания ИСМ (как в РФ, так и в мире) с целью обеспечения ИБ для СлПО, а также конкретных систем менеджмента информационной безопасности (СМИБ) – как отдельно, так и в составе ИСМ, оценка их результативности за длительные периоды наблюдений, позволил установить ряд объективных противоречий между требованиями практики и существующими положениями теории обеспечения ИБ.



Исследование. Выявленные противоречия. 1

Первое противоречие связано с тем фактом, что значительное количество разработанных стандартов (международных, государственных, отраслевых), применительно к рассматриваемой проблеме, обуславливает широчайшую вариативность вариантов их применения для целей обеспечения ИБ в ИСМ для СлПО. В частности, национальные стандарты ГОСТ Р не успевают обновляться синхронно с пересмотром международных стандартов ISO (например, ISO/IEC 27001:2013 и ГОСТ Р ИСО/МЭК 27001-2006).

Более серьезное отставание: более чем на 2 поколения демонстрируют ведомственные (отраслевые) системы стандартизации и государственной аттестации:

- *Стандарт СТО Газпром 4.2-3-003-2009 СОИБ «Анализ и оценка рисков» содержит ссылку на отмененный британский стандарт BS серии 7799 версии 2002 г.;*
- *«Положение по аттестации объектов информатизации по требованиям безопасности информации» – утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.*



Исследование. Выявленные противоречия. 2

Второе противоречие определяется тем фактом, что выбор оптимального множества применимых стандартов для формирования ИСМ по критерию наилучшего достижения поставленной цели – обеспечение заданного уровня ИБ в ИСМ для СлПО, затруднен отсутствием механизма единственного гарантированного «разумного подхода» ЛПР (в терминах Парето). В частности, существующий ряд положений (Т) существенно ограничивает (и даже исключает) роль ЛПР в формировании «разумного подхода» к выбору и ограничению требований (критериев).

Соответственно, возникают следующие критические риски:

- *неверного определения (неизмеримость) целей создания ИСМ как единой системы управления для СлПО;*
- *функциональной неполноты при формировании области распространения ИСМ (scope), в частности, процессов ИБ.*

Для целей обеспечения заданного уровня ИБ (А) необходимо решать совместно несколько противоречивых задач, в частности: перечень критериев ИБ, ограниченность ресурсов (К), технических средств, бюджета, времени и квалифицированного персонала и иных.



Исследование. Выявленные противоречия. 3

Третье противоречие вызвано несогласованным снижением ЛПР издержек (К) в процессах жизненного цикла (ЖЦ) и требованиями (Т) формирования контекста (*context*) СМИБ (ИСМ) для формирования «управляющих условий» для минимизации потерь от рисков ИБ в СлПО (G).

Данное противоречие обусловлено также динамикой структурных изменений, присущих всем СлПО, тем более, функционирующим круглосуточно, например: объектам топливно-энергетического комплекса (ТЭК) и аэропортовым комплексам (АК).

- *В частности, произошедшие инциденты ИБ на объектах ТЭК (Япония, Украина, США, Китай, Саудовская Аравия) и АК (Польша, Великобритания, Бельгия, Россия) объективно подтверждают этот факт – ЛПР устанавливает требования снижения издержек без должного учета требований к СМИБ (ИСМ).*



Исследование. Выявленные противоречия. 4

Четвертое противоречие связано с проблемой соответствия множественным общим законодательным требованиям (*compliance*) и конкретным требованиям обеспечения сохранения СлПО как совокупности ценных активов благодаря низкой аварийности, высокой устойчивости (*sustainability*) и лучшей отраслевой репутации.

Это противоречие на практике подтверждается разноплановыми требованиями регуляторов (ФСТЭК, ФСБ, МЧС), частыми изменениями законодательной базы (ФЗ-149, ФЗ-184, ФЗ-187) и вынужденными рассогласованными действиями ЛПР при управлении СлПО.

В практике аудита наблюдается факт, что ЛПР уделяют вопросам соответствия законодательным требованиям ровно такое минимальное внимание, которое позволяет принятая бизнес-практика (ПП-608, ПП-127).

- *Указанная проблема наиболее явно проявилась при внезапном прекращении сервиса со стороны Visa и MasterCard в 2014 г. Этот пример показал, что банковская система РФ оказалась не готова к реализации известных угроз, даже при наличии собственной отраслевой системы стандартизации в области ИБ – СТО БР ИББС.*



Анализ современных работ по теме диссертации

В настоящее время известны работы в области аудита ИБ: «школы Юсупова», в области оценки соответствия: Маркова А.С. («Эшелон»), теоретические работы Деминга, Райфа, Кини, Винера, Шнайера, Койбле и др. Также известны требованиями международных стандартов (ISO, IEC, IATA, NIST), национальных стандартов ГОСТ Р и ГОСТ Р В, отраслевых систем стандартизации (СТО БР ИББС, СТО Газпром СОИБ) и методик (COBIT и др.).

Объективно отметим недостаточную разработку методических подходов к обеспечению ИБ для СлПО. За исключением отдельных актов (Приказ ФСТЭК России № 31) практически не применяется подход риск-менеджмента и учет остаточных рисков ИБ для СлПО (Приказы ФСТЭК России № 235 и № 239).

В работах «школы Юсупова» представлена перспективная концепция ИБ, под которой, в отличие от «стандартной базы» ISO, понимается триада:

- *защита информации,*
- *защита от информации,*
- *добывание информации о намерениях и возможностях противоборствующей стороны в информационной сфере.*

Данная триада лишь частично рассматривается в современных нормативных документах и, к сожалению, в настоящее время не предложены подходы для обеспечения аудита ИБ во всех фазах ЖЦ.



Исследование. Существующие подходы

В настоящее время известны следующие основные подходы:

- Научно-методические подходы ФСТЭК и ФСБ к построению моделей угроз и защиты государственных информационных ресурсов, а также ключевых систем информационной инфраструктуры (КСИИ), которые применяются только в РФ. Основной акцент сделан на формировании статической модели нарушителя, фиксированного перечня ДД и угроз безопасности информации (УБИ). Часть документов не прошли регистрацию в Минюсте.
- Решения класса GRC (*Governance, Risk, Compliance*), предложенные разработчиками (например, RSA, Oracle, SAP, Allgress), пока не находят широкого применения в РФ в силу фрагментарного охвата функций ИБ, сложности внедрения, обязательным участием многочисленного персонала для настройки и высокой стоимости совокупного владения;
- Зарубежные методики (ISAGO, ITIL, COBIT и пр.) уделяют внимание проблеме обеспечения ИБ для СлПО, однако, несмотря на значительно более частое применение риск-ориентированных стандартов, единой концепции, увязанной с фазами ЖЦ и процессами «сквозного» управления и обработки рисков ИБ, к настоящему времени не представлено.



Научная проблема

- ♦ **Научная проблема** представленной диссертационной работы формулируется как проблема разрешения противоречий между состоянием теории ИБ (в частности, неполноты определения требований к аудитам ИБ) и современными требованиями практики по обеспечению ИБ в ИСМ для СлПО.
- ♦ Для решения данной проблемы потребуется пересмотр существующих статичных моделей УБИ и ДД, дополнительная и всеобъемлющая интеграция риск-менеджмента, учет требований, предъявляемых к планированию, выполнению и совершенствованию системы аудита ИБ в СлПО, принятие решения ЛПР при фиксированном множестве альтернатив, создание новых подходов к реализации аудита ИБ в СлПО, базирующихся на применении новых моделей и методов:

Научная проблема. Математическая постановка

- Модели ($M = \{ M \mid f(a', r', k', t', g') \}$), свойства которых (a', r', k', t', g') функционально зависят $f(a', r', k', t', g')$ от свойств: A (требований к аудитам ИБ), R (собственных свойств ТС), K (мер (средств) обеспечения ИБ), G (совокупности ДД и выявленных рисков) и T (требований (совокупности требуемых свойств) в аспекте ИБ для СлПО);
- Методы (m), обеспечивающих идентификацию, оценку и анализ объективных свидетельств (C) аудита ИБ при формировании эффективных решений ЛПР (N) с помощью оператора (O) в соответствии с установленными требованиями.

Математическая запись научной проблемы может быть представлена как:

Найти M : $(A \rightarrow A', R \rightarrow R', K \rightarrow K', T \rightarrow T', G \rightarrow G')$, (1)

для $\forall a' (a' \in A), \forall r' (r' \in R), \forall k' (k' \in K), \forall t' (t' \in T), \forall g' (g' \in G)$,

такие что: $\exists (N = N' \{M, a, a', r, r', k, k', t, t', g, g', \Delta N\})$,

при $\| N - N'_0 \| \rightarrow \Delta N_{\min}$

$m: C \rightarrow N$



Цель диссертационного исследования

- ♦ Цель представленной диссертационной работы формулируется как повышение уровня гарантированного обеспечения ИБ за счет использования новых моделей и методов аудита СМИБ (ИСМ), реализующих оперативное формирование количественной оценки уровня защищенности в СлПО, выбор и применение наилучшего множества средств (мер) обеспечения ИБ для обработки выявленных рисков.



Задачи диссертационного исследования

Достижение поставленной цели потребовало решение ряда задач:

- ♦ Исследование системных требований, предъявляемых к процессам обеспечения ИБ в СлПО и выявление закономерностей между изменениями требований регуляторов, стандартов (международных, отраслевых) и объективными потребностями создания ИСМ для различных отраслей промышленности;
- ♦ Исследование системных требований, предъявляемых при создании современных ИСМ, для защиты ценных активов и анализ аспектов применения риск-ориентированного подхода при обеспечении ИБ для СлПО, а также методов формирования оптимального перечня критериев для оценки результативности ИСМ;
- ♦ Исследование, анализ и создание иерархической структуры метрик ИБ в процессах обеспечения ИБ, в том числе аудита ИБ, предназначенных для формирования и оценивания требований к ИСМ для СлПО;
- ♦ Разработка и обоснование методов обеспечения ИБ в составе ИСМ, с учетом минимизации издержек по защите перечня активов и, в частности, увеличения стоимости нематериальных активов (*goodwill*) СлПО;
- ♦ Исследование практической применимости предложенных методов обеспечения ИБ в составе ИСМ для СлПО для различных отраслей промышленности.



Соответствие паспорту специальности 05.13.19

- ♦ п. 1. Теория и методология обеспечения информационной безопасности и защиты информации.
- ♦ п. 7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.
- ♦ п. 9. Модели и методы оценки защищенности информации и информационной безопасности объекта.
- ♦ п. 14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.
- ♦ п. 15. Модели и методы управления информационной безопасностью.



Научные положения, выносимые на защиту. 1

Первое научное положение – обобщенная модель ИСМ для обеспечения безопасности СлПО, базовая модель аудита ИСМ и система численных показателей (метрик) ИБ для выполнения аудита ИСМ.

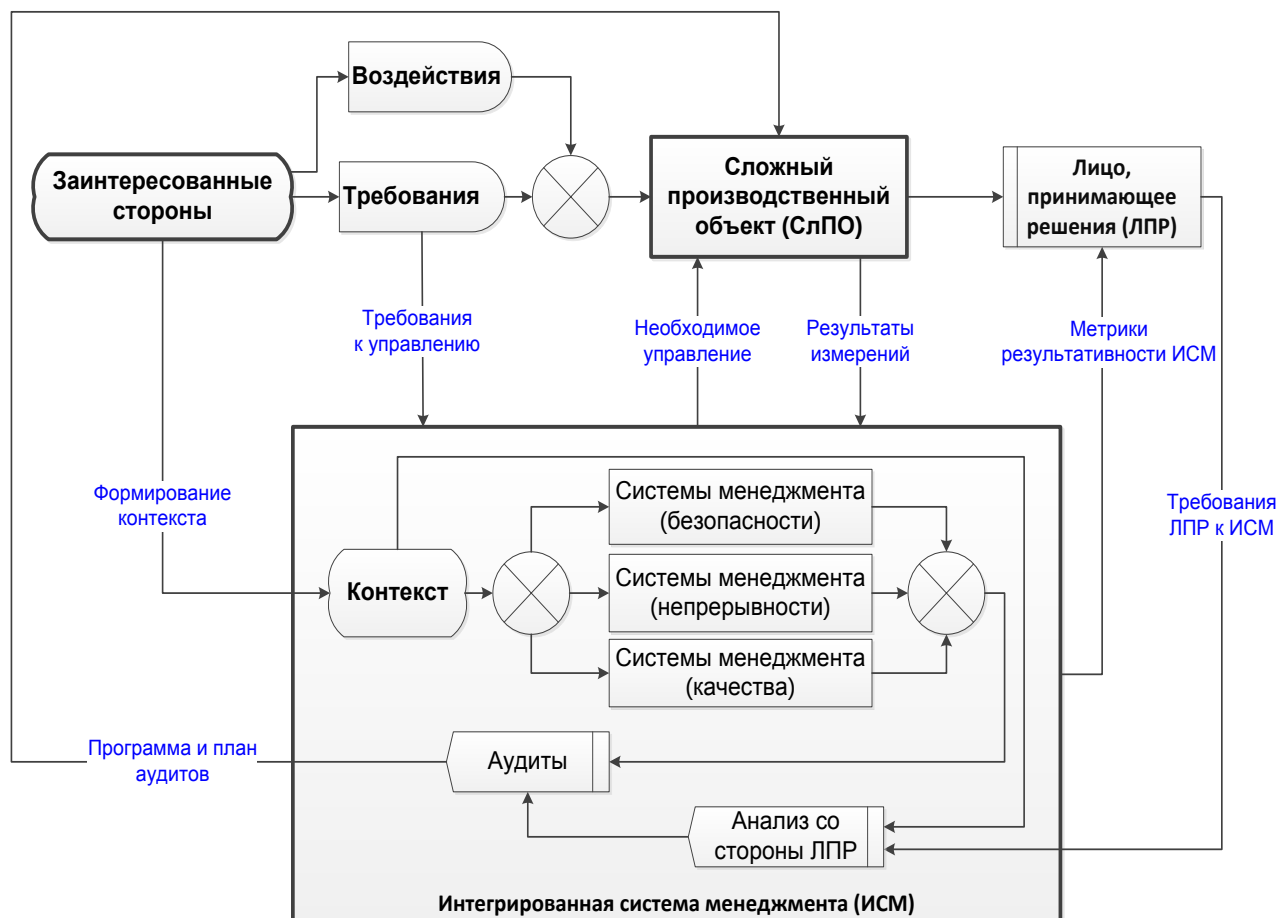
Раскрыта специфика процесса планирования, выполнения и анализа результатов аудита ИБ в ИСМ, заключающаяся в широком применении системы численных показателей (метрик) ИБ для оценки результативности ИСМ согласно применимым требованиям.

Предложенные новые модели: обобщенная модель ИСМ для обеспечения безопасности СлПО и базовая модель аудита ИСМ совместно с новой системой численных показателей (метрик) ИБ дополняют существующие традиционные методы выполнения аудита и позволяют применять численные оценки показателей (метрик) ИБ как оценки результативности ИСМ в статическом и динамическом (прогнозном) вариантах в режиме, близком к режиму реального времени (РРВ).

Научные положения, выносимые на защиту. 1

Отличительные свойства:

- Непредсказуемость последующих состояний и наличие иерархической структуры;
- Постоянное изменение требований: юридических, технологических, регуляционных и пр., приводящих к появлению возмущений в существующих каналах управления;
- Крайне малое время реакции на возмущения, требующее создания новых моделей, позволяющих ЛПР принимать «разумные решения» в режиме, близком к РРВ.



Обобщенная модель ИСМ для обеспечения безопасности СлПО

Научные положения, выносимые на защиту. 1

Модель проблемной ситуации описывается в нотации [*] как:

$$\langle U, A, G, Y, H, \Psi, W, K, \Omega, \theta \rangle \quad (2)$$

где:

- U – множество стратегий ЛПР;
- A – множество значений определенных и неопределенных факторов;
- G – множество исходов операции;
- Y – вектор характеристик исхода $g \in G$ (числовое выражение результаты операции);
- H – модель соответствия множеств: $H: U \times A \rightarrow Y (G)$
- Ψ – оператор соответствия «результат – показатель»;
- W – показатель эффективности;
- K – критерий эффективности;
- Ω – модель предпочтений ЛПР на элементах множества: $D = \{U, A, G, Y, W, K\}$,
- **θ – общая информация о проблемной ситуации.**

* *Надежность и эффективность в технике: Справочник в 10 т./Ред. совет: В.С. Авдеевский, (пред.) и др. – М.: Машиностроение, 1988. – (в пер.) Т. 3. Эффективность технических систем/Под общ. ред. В.Ф. Уткина, Ю.В. Крюкова. – 328 ст.: ил.*

Научные положения, выносимые на защиту. 1

Общая постановка задачи моделирования предпочтений представлена в виде:

$$\langle D, \theta_N ; \Omega_D \rangle \quad (3)$$

где:

- $D = \{U, A, G, Y, W, K\}$
- θ_N – дополнительная информация о проблемной ситуации.

Предложено расширить состав дополнительной информации о проблемной ситуации θ_N за счет новых факторов и представить задачу формирования множества стратегий ЛПР в новом виде:

$$\langle \theta_{A0}, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, A_N, U_N \rangle \quad (4)$$

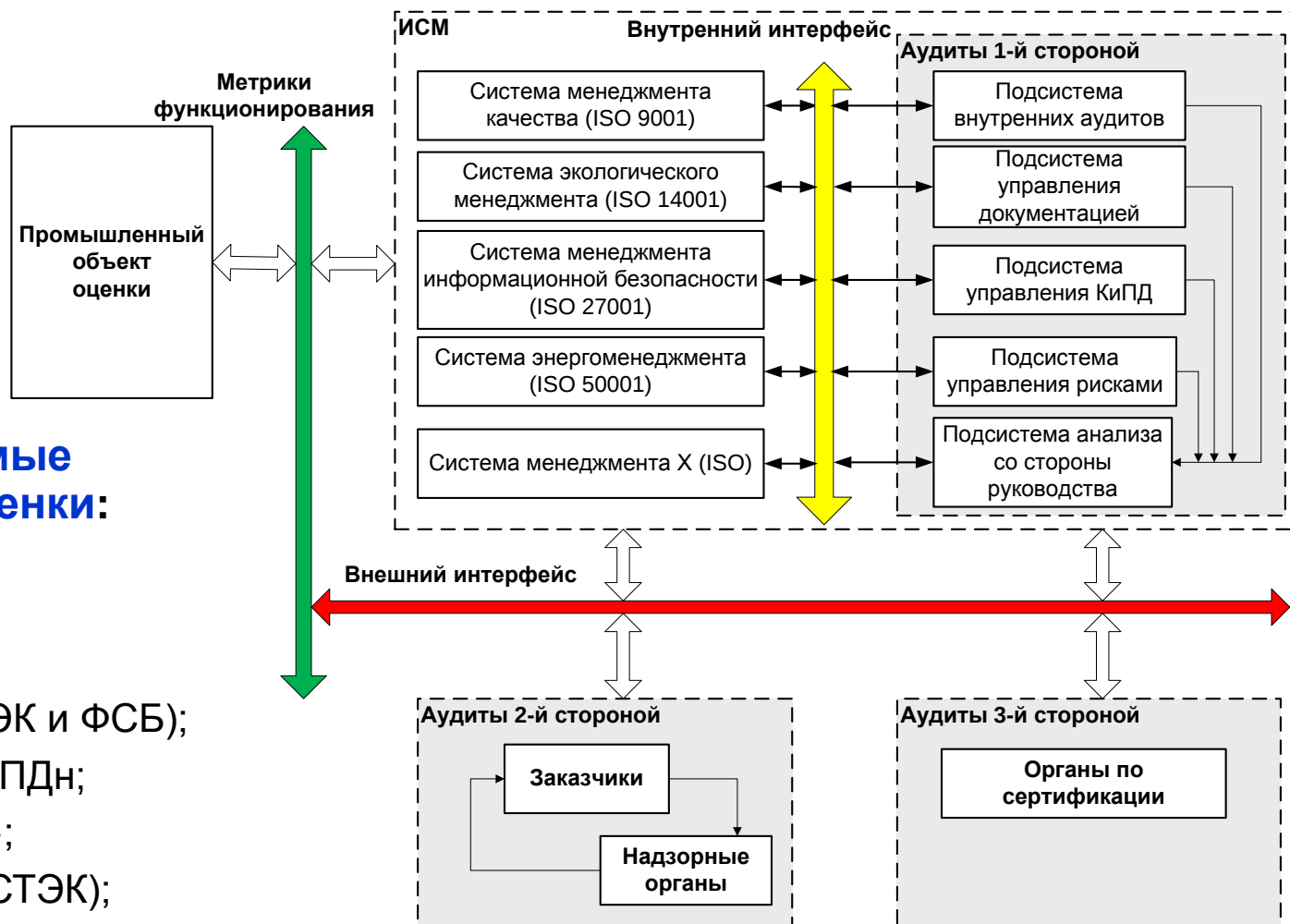
где:

- θ_{A0} – информация о начальной (исходной) цели операции;
- θ_1 – информация о результативности «мгновенных аудитов» ИБ;
- θ_2 – информация о результативности аудитов всех типов;
- θ_3 – информация об инцидентах ИБ (например, от SIEM, DLP, SOC и пр.);
- θ_4 – информация о новом «контексте» СМИБ (ИСМ);
- θ_5 – информация о новых предпочтениях ЛПР;
- θ_6 – информация о важных изменениях ФЗ (например, ФЗ-187 «ГосСОПКА»).

Научные положения, выносимые на защиту. 1

Применяемые методики оценки:

- КСИИ ФСТЭК;
- КИИ (ФЗ-187);
- Оценка УБИ (ФСТЭК и ФСБ);
- Защищенность ИСПДн;
- «Общие критерии»;
- Аттестация ОИ (ФСТЭК);
- Сертификация СМИБ.



Базовая модель аудита ИСМ

Научные положения, выносимые на защиту. 1

Объективные результаты любых аудитов ИСМ, как статистика инцидентов ИБ, являются достоверными и объективными данными, которые могут быть приняты как апостериорные оценки свойств фактически реализованной системы безопасности для СлПО.

При этом ЛПР имеет возможность сколь угодно уточнять (на основе полученных данных) оценки фактического состояния безопасности СлПО как по отдельным функциональным подсистемам, так и по отдельным процессам, в том числе, сопоставляя затраты на эти компоненты и величину ущерба (если имел место инцидент ИБ).

Таким образом, может быть предложена следующая математическая оценка риска ИБ для СлПО как математическое ожидание двух компонент (прямого и косвенного ущерба соответственно), с учетом применимых указанных выше методик:

$$R_t = M_t(R_t^1 + R_t^2) = \sum_{i=1}^n \sum_{j=1}^m S_{ij}^1 \cdot V_{ij}^1 + \sum_{i=1}^n \sum_{j=1}^m S_{ij}^2 \cdot V_{ij}^2$$

где:

- i – возможные ДД для конкретного СлПО (с учетом возможности реализации),
- j – возможные сценарии реализации ДД для конкретного СлПО,
- S_{ij}^1 – величина прямого ущерба при реализации риска возможных ДД,
- S_{ij}^2 – величина косвенного ущерба при реализации риска возможных ДД,
- V_{ij} – вероятность реализации риска возможных ДД.

Научные положения, выносимые на защиту. 1

Метод формирования метрик ИБ и выполнения измерений результативности СМИБ

№ п.п.	Последовательность действий	Префикс по ISO 27004	Новый элемент
1	Определение области сертификации СМИБ (<i>scope</i>) исходя из поставленной задачи и дополнительной информации θ_N	–	+
2	Обеспечение максимальной полноты перечня активов (<i>asset</i>), в аспекте дополнительной информации θ_N	–	+
3	Определение мер (средств) обеспечения ИБ (<i>controls</i>) (из «Заявления о применимости» / <i>Statement of Applicability</i>)	–	+
4	Определение реализации меры (средства) обеспечения ИБ	–	+
5	Определение объектов измерения	О	
6	Определение атрибутов	А	
7	Определение метода измерения	МИ	
8	Определение основной меры	ОМ	
9	Определение функции измерения	Ф	
10	Определение производной меры измерения	Пр	
11	Определение аналитической модели	АМ	
12	Определение показателей	П	
13	Определение критериев принятия решения	Кр	
14	Определение результатов измерений	РИ	

Научные положения, выносимые на защиту. 1

Критериями результативности СМИБ (ИСМ) выступают показатели степени соответствия процессов ИБ установленным требованиям и также – результаты оперативного оценивания ЛПР (*management review*) заданных и фактических показателей деятельности.

Рассмотрим ИСМ в нотации «сущности – связи» (*Entity – Relationship*), определим $Z = \{E_n; R_m\}$ как множество, состоящее из E_n – множество сущностей и R_m – множество связей конкретного объекта (СлПО). С учетом базовой модели аудитов ИСМ $Z_{base} = \{E_{n\ base}; R_{m\ base}\}$. Показатели степени соответствия процессов ИБ установленным требованиям обозначим как $Z_q = \{E_q; R_q\}$. При этом Z_q может включать ограниченное множество показателей, необходимых для оценки определенных процессов ИБ (например, внутренний аудит ИБ) или только определенных метрик (например, количество инцидентов ИБ), это множество обозначим как Z'_q .

Тогда ЛПР может формализовать математическую постановку задачи применения метрик ИБ как:

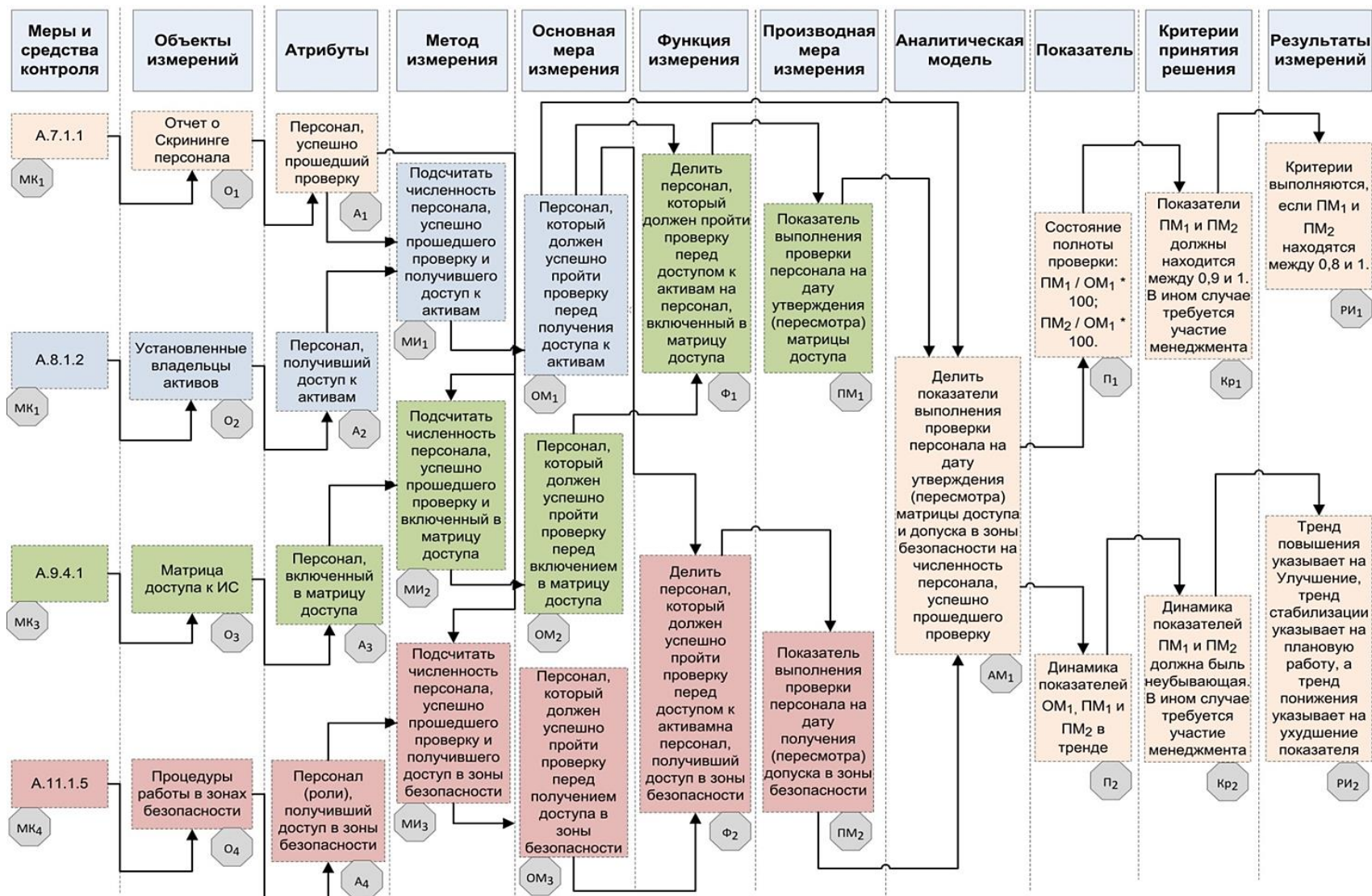
$$Q = \frac{Z_q \cap Z_{base}}{S}; \quad (R_q = R_{m\ base})$$

где:

S – затраты для применения метрик ИБ с учетом применимых требований.

Множество Q может быть формализовано в различных представлениях современных ТС (удобных для получения оперативных значений применяемых метрик, например, из систем DLP, SIEM, IDS/IPS и пр.).

Научные положения, выносимые на защиту. 1



Пример расчета метрик ИБ по новому методу



Научные положения, выносимые на защиту. 2

Второе научное положение – метод проведения аудита ИСМ для СлПО.

На основе выявления наиболее значимых потребностей ЛПР, предложен новый метод проведения «мгновенных аудитов» ИБ в ИСМ для СлПО. Новый метод, в отличие от известных методов аудита, позволяет учесть расширенный перечень критериев аудита (например, требований регуляторов и/или отраслевой специфики) и отличается применением численных показателей (метрик) ИБ с учетом специфики обеспечения безопасности различных видов СлПО.

Предложенный метод реализует новый принцип управления аудитами ИБ по частоте и предоставляет ЛПР оценку уровня защищенности СлПО как показатель результативности (*effectiveness*) СМИБ (ИСМ) и соответствия применимым требованиям.

- ✓ Исходные данные: критерии аудита, требования оценки уровня ИБ; **А, Т в (1).**
- ✓ Ограничения: ресурсы (временные, персонал, состав мер защиты, бюджет); **К, G, R в (1).**
- ✓ Основные шаги:
 - Формирование постановки задачи высшего руководства
 - Формирование критериев и метрик для выполнения «мгновенных аудитов» ИБ.
 - Анализ качества состава отобранных «элитных» элементов
 - Интерпретация результатов, изменение правил ротации и изменение частоты.
- ✓ Вывод: Повышение достоверности оценки ИБ достигается сокращением периода проведения и длительности аудита ИБ и динамичным изменением перечня критериев.

Научные положения, выносимые на защиту. 2

Для отбора наилучшей в смысле решения поставленной задачи совокупности критериев ИБ предлагается применять базовые положения теории «элитных групп» (предложенной ранее проф. А.Н. Ефимовым).

В новом предложенном методе экспертам рекомендуется элементы y_i выбирать случайно, что является, во-первых, требованием стандартов (ISO 19011, 17021 и 27006) по формированию «выборки аудита» (“*audit sample*”) и, во-вторых, должно исключить на практике случаи «подгонки» множества элементов Y под заранее заданный результат α .

Для этого в базовую формулу внесен новый компонент γ – вероятность включения в «элитную» группу ранее не использованных элементов Y_i . Таким образом, распределение качества Y в определенной «элитной» группе может характеризоваться плотностью распределения:

$$F_{Elite\ New}(y) = \left\{ \gamma \frac{\beta}{F(\alpha)} f(y): y < \alpha; (1 - \gamma) \frac{1 - \beta}{1 - F(\alpha)} f(y): y \geq \alpha \right\}$$

где:

α – показатель качества;

β – вероятность отбора в элитную группу «сорных» элементов;

γ – **вероятность отбора в элитную группу ранее не использованных элементов;**

$F_{EliteNew}(y)$ – функция распределения качества y в исходной группе;

$f(y)$ – соответствующая плотность распределения.

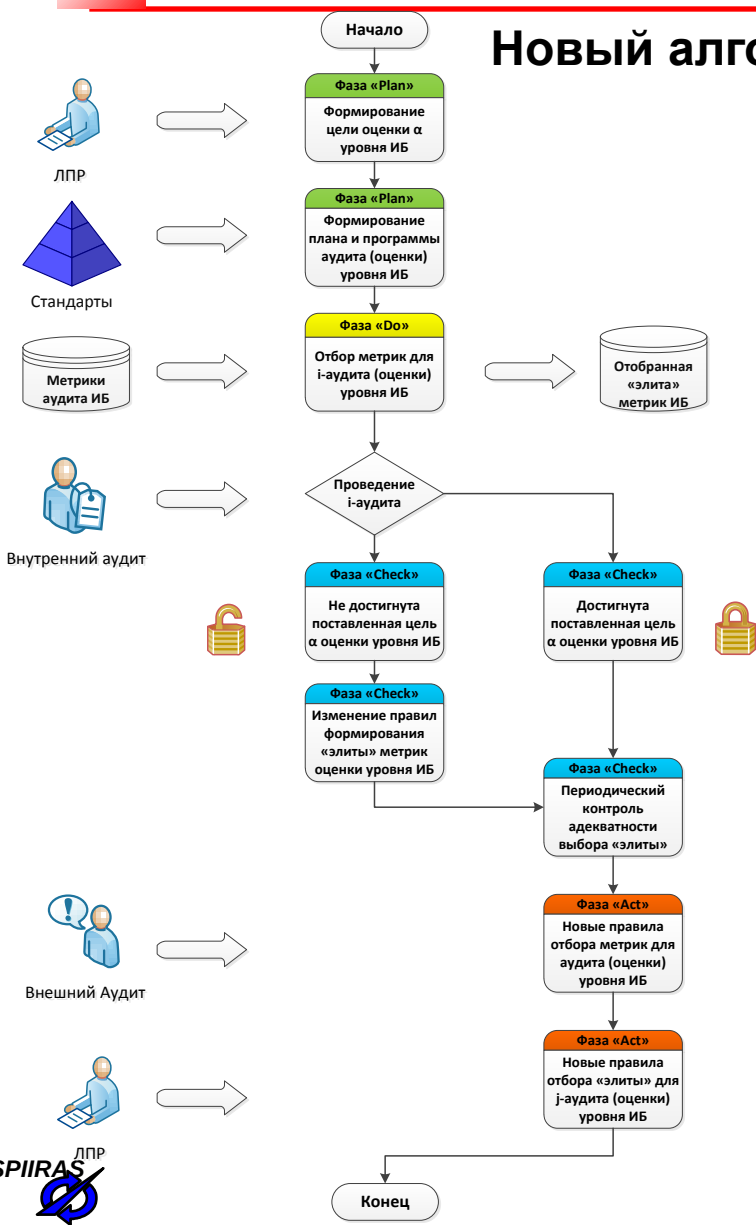
Научные положения, выносимые на защиту. 2

Новый алгоритм применения «элитных групп» для СМИБ

Для развития базовой теории «элитных групп» для применения в целях управления аудитами ИБ в представленном алгоритме введены новые функции в строгом соответствии с циклом PDCA (циклом Деминга-Шухарта).

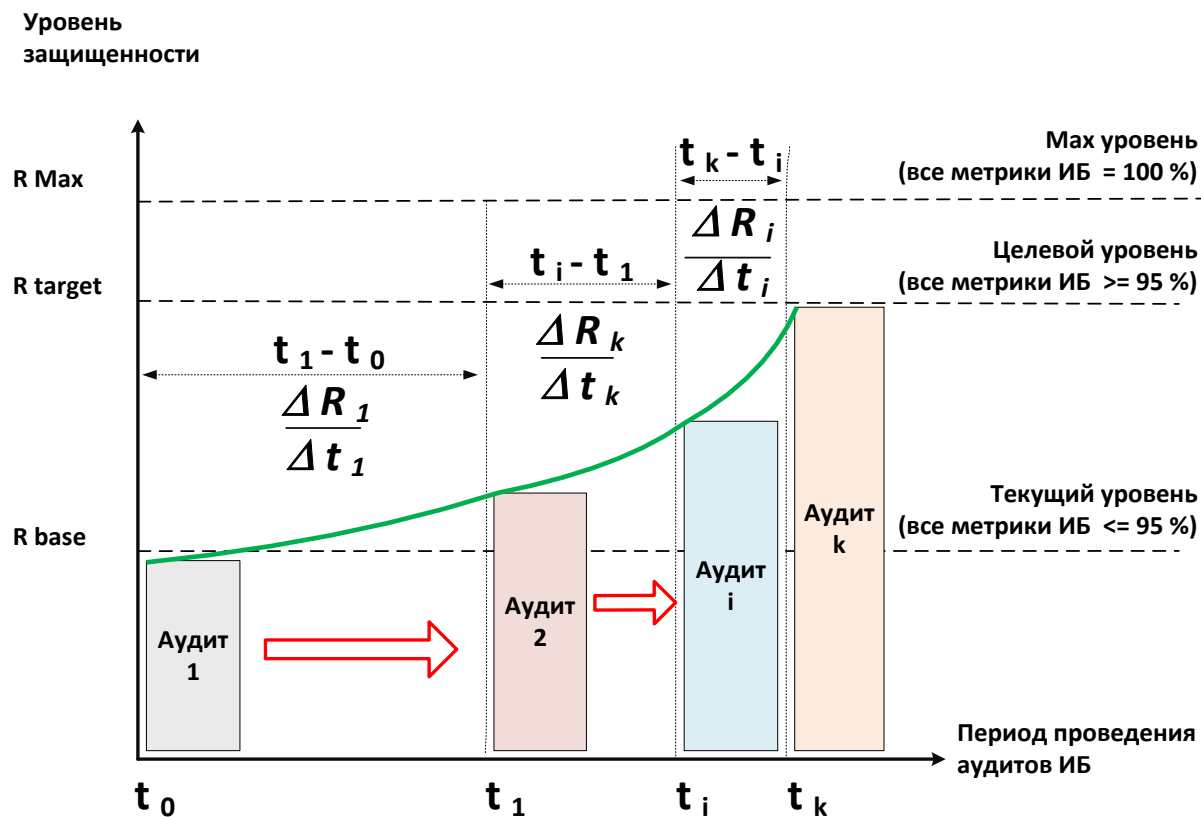
Рекомендуется принять во внимание для аудита ИБ ряд принципиально новых обстоятельств:

- Необходимо ориентироваться прежде всего на долю «элитных» элементов, удовлетворяющих $y_i \geq \alpha$, но ранее не отобранных для аудита в течении одного полного замкнутого цикла программы аудита;
- Необходимо отслеживать характер изменения «качества» каждого отобранного «элитного» элемента при k-аудите, при наличии достаточных ресурсов – всей совокупности «элитных» элементов, в т.ч. «резерва» множества Y ;
- Необходимо формировать правила выбора, ротации и отсева «элитных» элементов (на практике это означает пересмотр метрики ИБ по итогам, например, системы аудита ИБ).



Научные положения, выносимые на защиту. 2

Реализация метода «мгновенных аудитов» для оценки защищенности ценных активов с требуемой частотой может быть продемонстрирована как сокращение периода (увеличение частоты) проведения аудита ИБ при использовании.



Отметим, что оперативные данные, формируемые при реализации метода «мгновенных аудитов» обеспечивают оценку компонентов θ_1 и θ_2 из (4), предоставляя ЛПР опосредованно и данные для определения компонент A_N и U_N .



Научные положения, выносимые на защиту. 3

Третье научное положение – метод исследования динамики сертификации по международным стандартам ISO для СлПО.

Предложен новый метод исследования показателей динамики сертификации по международным стандартам, основанный на достоверных публичных статистических данных ISO, и устанавливающий новый порядок формирования и оценки влияние «лидеров» разного ранга.

Предложенный метод учитывает приоритеты ведущих отраслей в соответствии с международными кодами экономической деятельности ЕАС и позволяет оценить динамические изменения потребностей бизнеса, выраженные в изменении предпочтений по составу перечня внедряемых стандартов, успешно прошедших внешний (независимый) аудит ИСМ.

Научные положения, выносимые на защиту. 3

Динамика сертификации по выбранным стандартам ISO

Стандарт	2010 г.	2011 г.	2012 г.	2013 г.	2014 г.
В мире					
ISO 9001	100	-3,51%	1,65%	2,96%	0,77%
ISO 14001	100	4,13%	8,68%	5,97%	7,46%
ISO 27001	100	11,06%	13,05%	13,62%	7,53%
ISO 50001		100,00%	351,72%	115,83%	40,45%
В Европе					
ISO 9001	100	-13,33%	2,26%	3,37%	-0,38%
ISO 14001	100	-1,89%	10,61%	6,43%	3,98%
ISO 27001	100	10,19%	20,61%	24,63%	9,56%
ISO 50001		100,00%	427,20%	108,08%	38,39%
В РФ					
ISO 9001	100	-78,63%	-6,16%	-5,80%	-3,94%
ISO 14001	100	-44,03%	-0,27%	16,70%	-0,71%
ISO 27001	100	-56,94%	-12,90%	77,78%	4,17%
ISO 50001		100,00%	700,00%	212,50%	224,00%

Научные положения, выносимые на защиту. 3

Результаты определения «лидеров рангов» по сертификации ISO

Стандарт	ЕАС	Наименование отрасли (Industrial sector)	Ранг		
			1	2	3
9001	17	Basic metal & fabricated metal products			
	19	Electrical and optical equipment			
	28	Construction			
	29	Wholesale & retail trade, repairs of motor vehicles			
	18	Machinery and equipment			
14001	28	Construction			
	17	Basic metal & fabricated metal products			
	19	Electrical and optical equipment			
	29	Wholesale & retail trade, repairs of motor vehicles			
	14	Rubber and plastic products			
27001	33	Information technology			
	35	Other Services			
	28	Construction			
	31	Transport, storage and communication			
	19	Electrical and optical equipment			



Научные положения, выносимые на защиту. 3

Новый метод основан на изучении несколько наборов данных (результаты статистики сертификации по международным стандартам ISO), которые могут быть точно (однозначно) определены по итогам значений аргумента t (в конкретном примере – 5 лет). Таким образом, мы обладаем данными о некоторой реализации случайного процесса на длительном интервале достоверных наблюдений.

Для исследования удобно рассматривать реализацию случайного процесса как множество дискретных сечений (счетное множество). Соответственно, исследуемый процесс можно считать процессом с дискретным временем и дискретным состоянием, т.к. в любой момент t полагаем множество его состояний конечным (счётным).

Для рассматриваемого случайного процесса $X(t)$, известно, что сечение $X(t)$ при любом фиксированном значении аргумента t представляет собой случайную величину, которая имеет следующий закон распределения:

$$F(t, x) = P \{ X(t) < x \}$$

Эта функция является функцией 2-х аргументов, и это одномерный закон распределения. Из работ Е.С. Вентцель известно, что более точные и исчерпывающие характеристики при необходимости может обеспечить для инженерных приложений двумерный закон распределения, функция 4-х аргументов.

Научные положения, выносимые на защиту. 3

Оценка независимости двух случайных величин выполняется по формуле:

где:

$$Corr(\eta, \gamma) = \frac{Cov(\eta, \gamma)}{\sigma(\eta) \cdot \sigma(\gamma)}$$

σ – стандартное (среднее квадратическое) отклонение

Cov – ковариация между двумя дискретными случайными величинами.

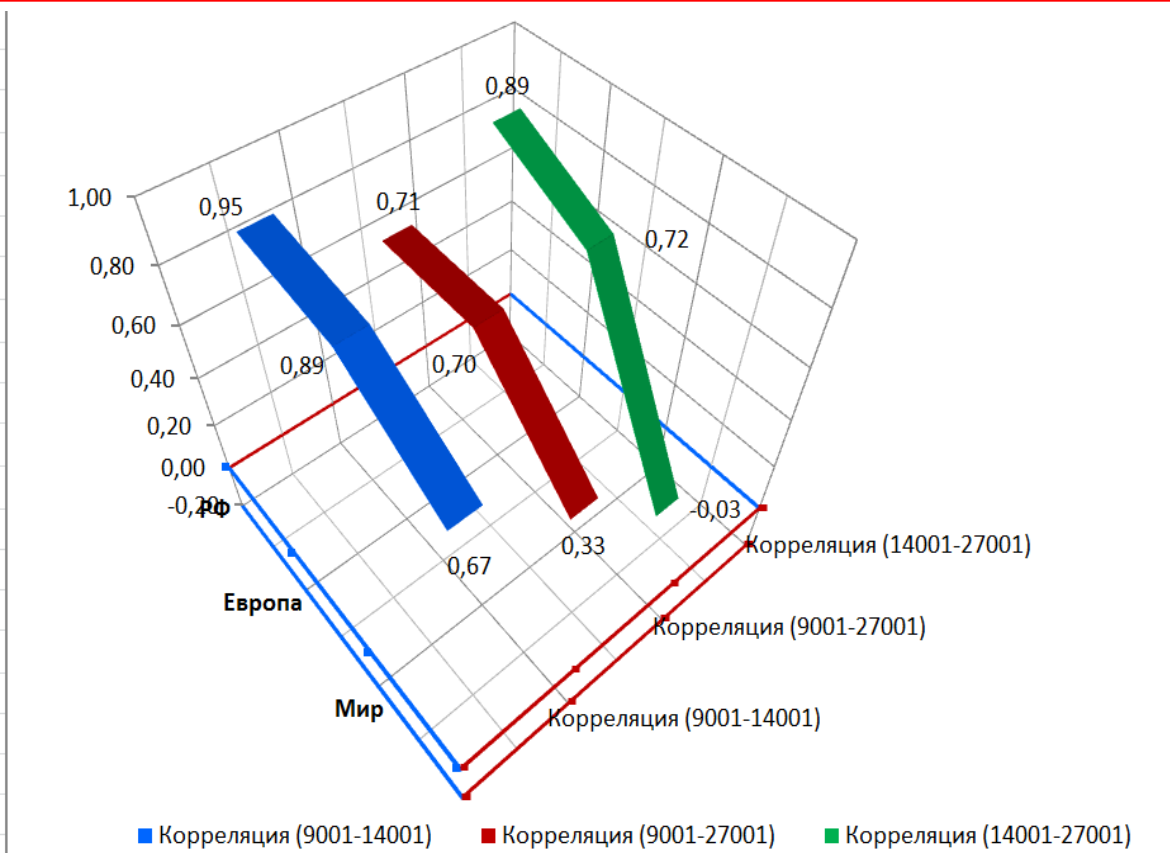
Ковариация Cov определяется по формуле:

$$Cov(\eta, \gamma) = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} P_{ij} (X_i - E(\eta)) \cdot (Y_j - E(\gamma))$$

где: E – математическое ожидание.

Код ЕАС	Ранг	Коэффициенты корреляции		
		9001 – 14001	14001 – 27001	9001 – 27001
19	1	0,442	-0,314	0,472
28	1	-0,851	0,415	0,111
17	2	0,646	0,808	0,875
29	2	0,667	0,404	0,667
18	3	0,440	0,779	0,864
14	3	0,475	0,439	0,369
33	3	0,769	0,641	0,973
35	3	0,902	0,957	0,981
31	3	0,892	0,967	0,936

Научные положения, выносимые на защиту. 3



Дополнительно
определены
коэффициенты
корреляции по
3-м регионам:

1. Россия
2. Европа
3. Мир

Аналитический разрез	Коэффициенты корреляции		
	9001 – 14001	14001 – 27001	9001 – 27001
РФ	0,946	0,892	0,709
Европа	0,895	0,719	0,696
Мир	0,666	-0,030	0,331



Научные положения, выносимые на защиту. 3

На основании применения нового метода исследования динамики сертификации по международным стандартам ISO определим:

- Для «**лидеров 3-го ранга**» для всех пар сравнения стандартов наблюдается корреляция с низким (для отраслей ЕАС 14 и 18) и высоким признаком (по шкале Чеддока 0,3 и 0,8 соответственно). Эта группа в целом показывает положительную корреляцию по всем парам сравнения.
- Для «**лидеров 2-го ранга**» для всех пар сравнения стандартов наблюдается корреляция со средним (для отрасли ЕАС 29 и 17) и высоким признаком (по шкале Чеддока свыше 0,4 и 0,8 соответственно). Эта группа в целом показывает положительную корреляцию по всем парам сравнения.
- Для «**лидеров 1-го ранга**» для всех пар сравнения стандартов (кроме пары ISO 9001 – 27001) наблюдается различная по знаку корреляция. Эта группа в целом показывает разнонаправленную корреляцию по тем парам сравнения, где есть стандарт ISO 14001.
- Для пары ISO 9001 – 27001 для всех «**лидеров**» без исключения показана только положительная корреляция, и внимание к сертификации по указанной паре стандартов мало зависит от специфики конкретных отраслей (т.е. объективно, требованиям ИБ привержены не только ИТ-компании).

Оперативные данные, формируемые при реализации метода исследования динамики сертификации по стандартам ISO обеспечивают оценку компонентов θ_{A0} , θ_4 и θ_5 из (4), предоставляя ЛПР опосредованно и данные для определения компонент A_N и U_N .



Научные положения, выносимые на защиту. 4

Четвертое научное положение – метод многошаговой оптимизации процесса аудита ИСМ для СлПО.

Предложен новый метод многошаговой оптимизации процесса аудита ИСМ для СлПО, который, в отличие от известных стандартов ISO серии 19011, 17021 и 27006, позволяет обеспечить координацию, распределение ресурсов и оперативное информирование в части результатов аудита и выполнения корректирующих мероприятий в ИСМ для ЛПР.

Предложенный новый метод заключается в научно обоснованном и целенаправленном применении функционально завершенной подсистемы ИБ в составе ИСМ, и отличающийся от существующих методов циклической непрерывной оценкой результативности ИБ на основе оптимальной системы численных показателей (метрик) ИБ с возможностью быстрой коррекции программы аудита ИСМ.

Новая задача оптимизации заключается в ускорении процесса выбора оптимальной системы численных показателей (метрик) ИБ при анализе результативности каждого цикла аудита, в отличие от классического анализа только по завершению полностью всей программы аудита.



Научные положения, выносимые на защиту. 4

Предложен новый метод многошаговой оптимизации процесса аудита ИСМ для СлПО состоит из 2-х циклов оптимизации программы аудита ИСМ, отличающихся следующими новациями:

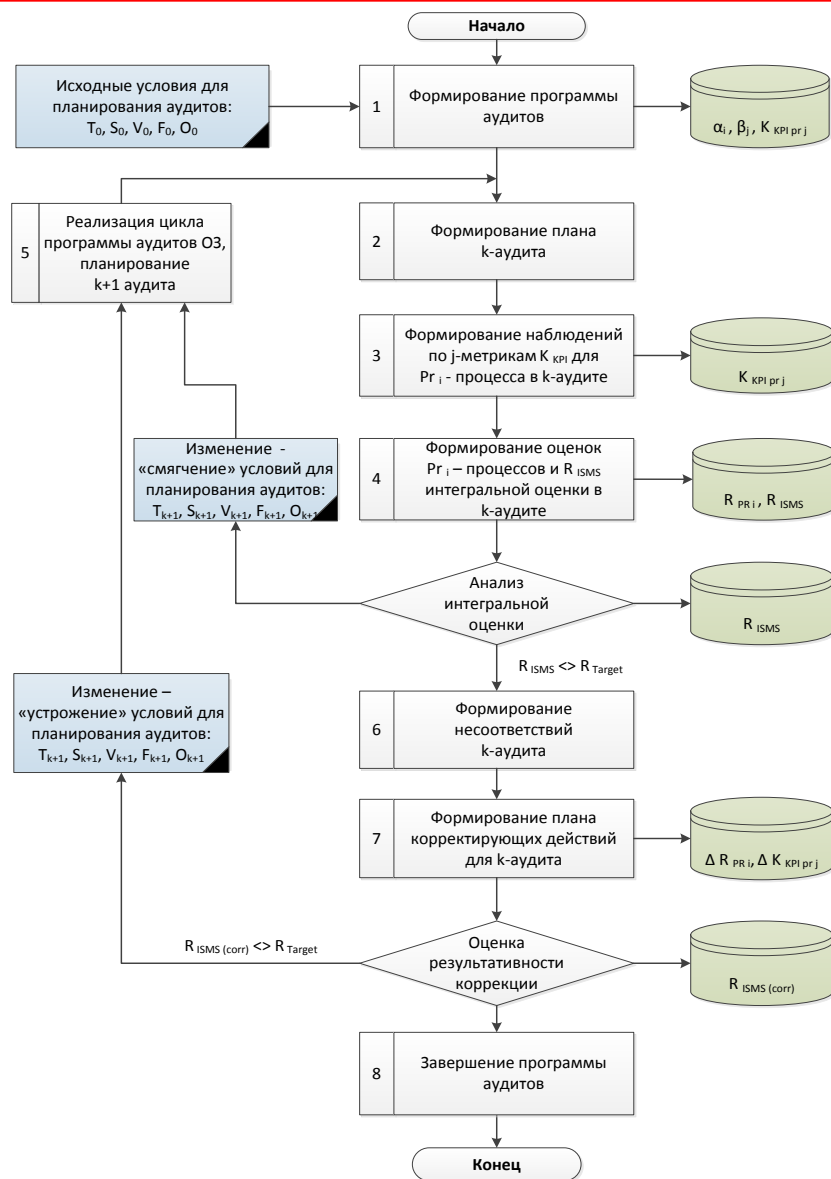
- **Базовым оптимизационным циклом**, который характеризует эффективное выполнение аудита ИСМ в терминах оценки результативности для каждого PR_i – процесса ИБ и каждой KPI_j – метрики ИБ, а также определяет циклы оптимизации ресурсов в программе аудита: глубины, размера аудиторской выборки, количества привлекаемых аудиторов (технических экспертов) и пр.
- **Быстрым блоком оценки результативности мер коррекции** (корректирующих действий) в текущем k -м аудите, затрагивающих изменения – как следующего процесса, так и следующего в программе $(k+1)$ -го аудита. Также обеспечивается быстрый переход к оценке показателей результативности СМИБ – R_{ISMS} в k -м аудите и $(k+1)$ -м аудите для постоянной и оперативной оптимизации всей программы аудита.

Оперативные данные, формируемые при реализации методов оптимизации программы аудита ИСМ, обеспечивают оценку компонентов θ_{A0} , θ_2 , θ_4 и θ_5 из (4), предоставляя ЛПР опосредованно и данные для определения компонент A_N и U_N .

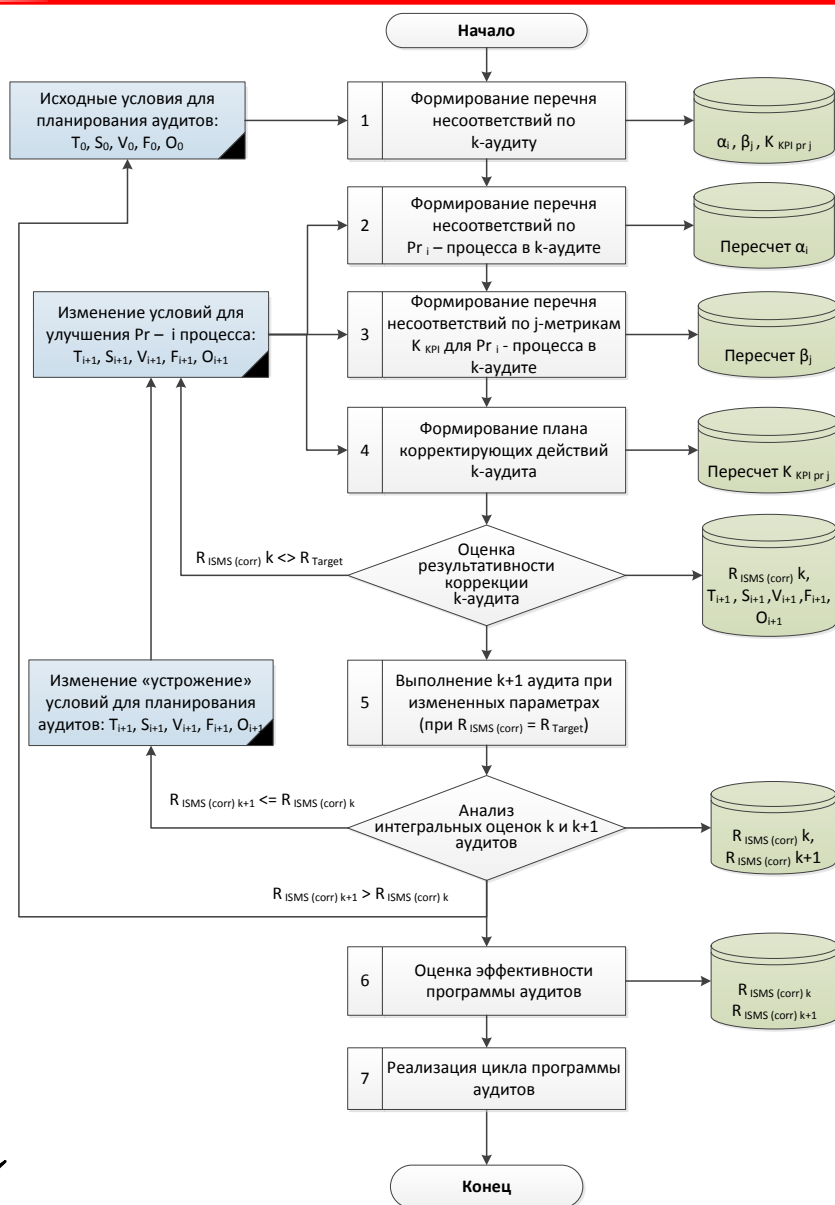
Научные положения, выносимые на защиту. 4

Базовый

оптимизационный цикл программы аудита ИСМ



Научные положения, выносимые на защиту. 4



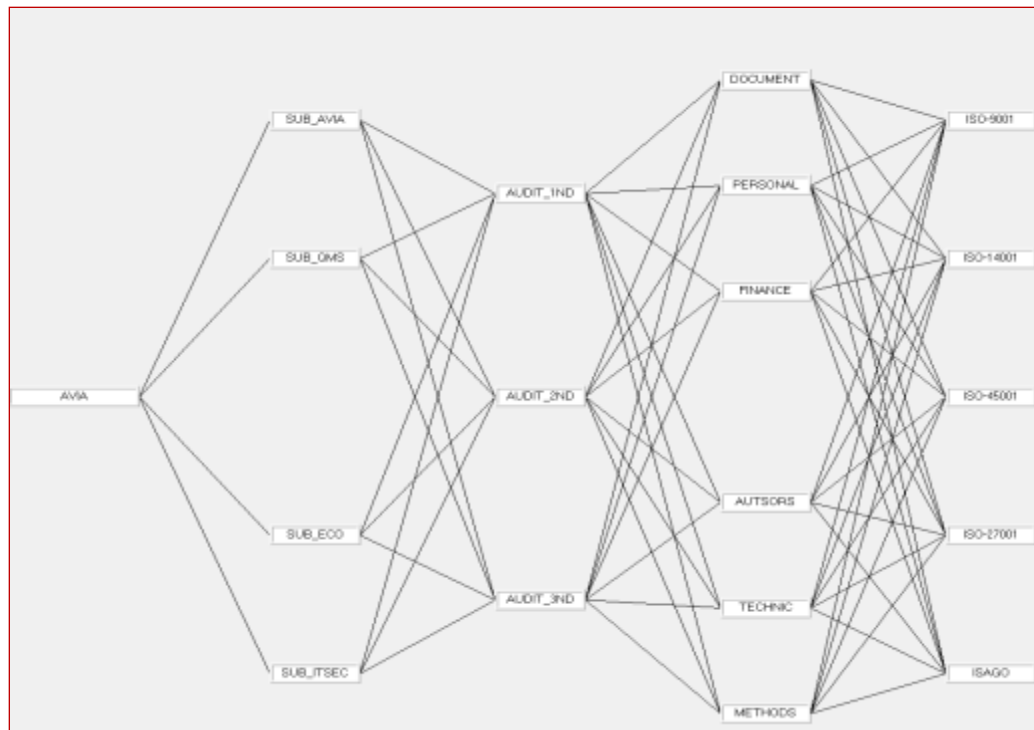
Детализация базового оптимизационного цикла программы аудита ИСМ

Рассмотрим далее детализацию базового оптимизационного цикла программы аудита ИСМ с учетом формальных требований стандартов по аудиту (ISO, ISAGO), дополненных новыми компонентами:

- Блок быстрого перехода при $R_{ISMS (corr)} < R_{ISMS tar.}$
- Блок быстрого перехода при $R_{ISMS (corr) k+1} < R_{ISMS (corr) k}$

Апробация по модели ИСМ для аэропортовых комплексов

По разработанной модели ИСМ для АК выполнено имитационное моделирование в среде MPriority на примере двух однотипных и независимых объектов: АК Астана (TSE) и АК Алматы(ALA).



Работа эксперта

Применение поправочных коэффициентов объекту

SUB_AVIA

	1	2	3	Приоритет
1. AUDIT_1ND	1	1/3	1/5	0.1047
2. AUDIT_2ND	3	1	1/3	0.2582
3. AUDIT_3ND	5	3	1	0.6309

СЗ: 3.0395
 ИО: 0.0192
 МО: 0.0331

Применить
 Закрыть
 Отмена

Улучшение согласованности исходных данных

	1	2	3	Сумма
1. AUDIT_1ND	0	3,4	5,16	8,56
2. AUDIT_2ND	0,53	0	3,4	3,93
3. AUDIT_3ND	1,88	0,53	0	2,41

Список нарушенных условий транзитивности:
 Информация о нарушении транзитивности - отсутствует

Закрыть

Модель в среде моделирования MPriority



Итоговый результат в среде моделирования MPriority

Оценка производительности системы имитационного моделирования

Для оценки производительности системы имитационного моделирования предложена новая методика на базе Apdex.

$$I_{Apdex\ New} = \frac{f(Nt) * NT + f(Nq) * NQ}{N}$$

где:

- $I_{Apdex\ New}$ – новая оценка (индекс производительности) Apdex,
 $f(Nt)$ – вероятность получения ЛПР ответа к целевому времени T и $4T$,
 $f(Nq)$ – вероятность получения ЛПР ответа свыше времени $4T$,
 NT – кол-во выполнений операций с временем отклика от 0 до $4T$,
 NQ – кол-во выполнений операций с временем отклика свыше $4T$,
 N – общее количество выполнений данной операции.

Операция	T, сек.	N	Nt	VNt	Nq	VNq	Apdex base	Оценка (база)	Apdex new	Оценка (новая)
Формирование цели ЛПР	30	20	18	0,997	2	0,003	0,95	Отлично	0,90	Хорошо
Формирование функциональных подсистем	120	47	38	0,997	9	0,003	0,90	Хорошо	0,81	Удовл.
Формирование ключевых процессов ИБ	300	48	28	0,997	20	0,003	0,79	Удовл.	0,58	Неприемлемо
Формирование мер и средств контроля ИБ	600	94	65	0,997	29	0,003	0,85	Хорошо	0,69	Неприемлемо
Формирование альтернатив	120	20	18	0,997	2	0,003	0,95	Отлично	0,90	Хорошо
Расчет по системе MPriority	10	100	94	0,997	6	0,003	0,97	Отлично	0,94	Хорошо
Проверка согласованности МПС, ошибок транзитивности	600	90	49	0,997	41	0,003	0,77	Удовл.	0,54	Неприемлемо
Представление результатов ЛПР	120	20	17	0,997	3	0,003	0,93	Хорошо	0,85	Хорошо



Научная новизна защищаемых положений. 1

Новизна первого научного положения – заключается в том, что впервые предложены обобщенная модель ИСМ для обеспечения безопасности СлПО и базовая модель аудита ИСМ, которые, в отличие от известных моделей, содержат все базовые сущности для выполнения аудита и совместно с новой системой численных показателей (метрик) ИБ для выполнения аудита ИБ позволяют формировать численные оценки уровня обеспечения ИБ.

Новая модель аудита ИСМ предполагает использование единого множества метрик, но на разных интерфейсах (для внутреннего и для внешних потребителей). Также введено воздействие на объект оценки (ОО), которое реализуется через подсистему анализа со стороны ЛПР.

Дополнительно проведена структуризация предмета исследования и выполнено дальнейшее развитие иерархической системы показателей (метрик) ИБ, позволяющей, в отличие от применяющейся формальной аттестации или ежегодных фиксированных аудитов, формировать и учитывать при принятии решения ЛПР метрики (оценки ИБ) в режиме, близком к РВВ.



Научная новизна защищаемых положений. 2

Новизна второго научного положения – заключается в том, что впервые для планирования и оценки (аудита) ИСМ (А) для СлПО предложен метод «мгновенных аудитов», учитывающий адекватность выполнения применимых требований ИБ (Т) «не вообще», а в той мере, которая достаточна для достижения в значительно короткий срок поставленной цели аудита (R).

Известно, что процесс аудита предполагает получение объективных оценок на основании свидетельств аудита, которые могут быть проверены независимыми экспертами.

Новый метод с учетом управления «частотностью аудита», объективно, позволяет более оперативно контролировать динамику процесса оценки уровня защищенности («динамической перестройки» критериев аудита).

Важным преимуществом нового метода является акцентирование именно на получении численных оценок, а не простого «соответствия» (*conformity*) или «несоответствия» (*non-conformity*).

Предложенный метод позволяет дополнительно исправлять ошибки, присущие сложному процессу аудита, методом локализации обратным процессом (G), как показано в известной классической работе Н. Винера.



Научная новизна защищаемых положений. 3

Новизна третьего научного положения – заключается в том, что в отличие от публикуемых периодических обзоров (содержащих общую статистику), предложен новый метод исследования динамики сертификации по международным стандартам ISO.

Представленный метод содержит математический аппарат, позволяющий оценивать зависимость степени развития разных организаций (например, по кодам отраслей ЕАС) от динамики сертификации ISO. Реализован корреляционный анализ для оценки динамики рассмотренных зависимостей, так как не все отрасли подтверждают равные тенденции (динамику сертификации).

Дополнительно определяется коэффициент зависимости (корреляции) относительных величин – для определенных отраслей, ранжированных по новой введенной метрике «лидер». В частности, впервые оценки СМИБ, представленные в публичных статистических данных ISO в соответствии с представленным методом, позволяют проследить взаимосвязь с общим «успехом» по конкретной отрасли для «лидеров» разных рангов.

Представленный метод универсален, реализует обобщенный и объективный подход к оценке и определяет «лидеров» вне каких-либо ограничений – по кодам ЕАС.



Научная новизна защищаемых положений. 4

Новизна четвертого научного положения – заключается в том, что в отличие от известных процессов выполнения аудита ИСМ для СлПО, предлагается новое решение задачи многошаговой оптимизации процесса обеспечения ИБ на всем интервале ЖЦ СлПО.

Представленный новый метод оптимизации предусматривает проведение мониторинга результативности аудита в режиме, близком к РРВ, и оперативное информирование ЛПР в части обеспечения ИБ, в случае выявления такой необходимости, а не только фиксированные ежегодные встречи в рамках выполнения анализа СМИБ (ИСМ).

Использование нового метода позволяет оптимизировать ресурсы для выполнения аудита (оценок) уровня обеспечения ИБ по этапам ЖЦ СлПО с учетом происходящих изменений.

В частности, учитываются изменения перечня применяемых (рекомендованных) СрЗИ, предпочтения ЛПР, появления новых УБИ в отношении защищаемых активов СлПО, а также новые законодательные и/или отраслевые нормативные требования.



Практическая ценность полученных результатов

Практическая ценность полученных результатов – состоит в улучшении методов оценки (аудита) ИБ для СлПО, основанных на применении оптимального множества риск-ориентированных стандартов в составе ИСМ, что обеспечивает:

- эффективное противодействие ДД злоумышленников,
- достижение требуемого уровня ИБ,
- снижение издержек в процессе разработки и внедрения ИСМ,
- минимизацию потерь при возникновении ситуаций риска ИБ, присущих СлПО,
- повышение степени соответствия комплексу законодательных требований (*compliance*).

Представленные методы и модели аудита ИБ для СлПО реализованы как функционально завершённый элемент в системе мероприятий комплекса обеспечения ИБ.



Перечень публикаций, содержащих описание защищаемых положений

Защищаемые положения	Перечень публикаций
Обобщенная модель ИСМ для обеспечения безопасности ИСМ, базовая модель аудита ИСМ и система численных показателей (метрик) ИБ для выполнения аудита ИСМ	БАК – 9 Scopus – 3 Рецензируемые журналы – 6 Конференции – 11
Метод проведения «мгновенных аудитов» ИСМ для СлПО	БАК – 15 Scopus – 4 Рецензируемые журналы – 7 Конференции – 10
Метод исследования динамики сертификации по международным стандартам ISO для СлПО	БАК – 6 Scopus – 2 Рецензируемые журналы – 4 Конференции – 8
Метод многошаговой оптимизации процесса аудита ИСМ для СлПО	БАК – 10 Scopus – 3 Рецензируемые журналы – 5 Конференции – 9



Публикации. Практическая апробация

- Основные результаты исследования опубликованы в научной печати:
 - Свыше 40 публикации в журналах, внесенных в список изданий, рекомендованных ВАК;
 - Свыше 30 докладов в трудах международных и российских научных и научно-практических конференций;
 - 14 публикаций в изданиях, индексируемых Scopus / Web of Science;
- Результаты исследования внедрены:
 - Транспортный комплекс:
 - Международный аэропорт Астаны (TSE);
 - Международный аэропорт Алматы (ALA).
 - Информационные технологии: «Информационно-сервисная технологическая компания (ИТСК);
 - Системная интеграция в области ИБ: («Газинформсервис»);
 - Кредитные и финансовые организации: («Рускобанк»);
 - Управление объектами критичной инфраструктуры: ФГУП «Водоканал Санкт-Петербурга»
 - Образование:
 - ФГАОУВО НИУ ИТМО (кафедра ПБКС);
 - Международная компания AQS (Азербайджан).



Уважаемый председатель Ученого совета!

Уважаемые члены Ученого совета!

Уважаемые коллеги!

Благодарю вас за внимание!

Пожалуйста, ваши вопросы!