На правах рукописи

ЛИВШИЦ Илья Иосифович

МОДЕЛИ И МЕТОДЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ СЛОЖНЫМИ ПРОМЫШЛЕННЫМИ ОБЪЕКТАМИ

05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
доктора технических наук

Санкт-Петербург – 2018

Работа выполнена в лаборатории безопасности информационных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук

Научный консультант	**Молдовян Александр Андреевич** доктор технических наук, профессор, главный научный сотрудник лаборатории безопасности информационных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук
Официальные оппоненты	**Кустов Владимир Николаевич** доктор технических наук, профессор Федерального государственного бюджетного образовательного учреждения высшего образования «Петербургский государственный университет путей сообщения Императора Александра I»
	Зикратов Игорь Алексеевич доктор технических наук, профессор, декан факультета Информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
	Липатников Валерий Алексеевич доктор технических наук, профессор, старший научный сотрудник Военной академии связи имени Маршала Советского Союза С. М. Буденного
Ведущая организация	Акционерное общество «Научно-производственное объединение «Эшелон»

Защита состоится «__» ноября 2018 г. в ____ час. 00 мин. на заседании диссертационного совета Д.002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, Санкт-Петербург, В.О., 14 линия, 39.

С диссертацией можно ознакомиться в библиотеке Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, http://www.spiiras.nw.ru.

Автореферат разослан «____» августа 2018 г.

Ученый секретарь
диссертационного совета Д.002.199.01
канд. технических наук Зайцева Александра Алексеевна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. В настоящее время увеличивается количество атак злоумышленников, направленных не столько на данные, сколько на элементы систем управления (СУ) и технологические процессы различных критичных объектов. Соответственно, значительно увеличилась актуальность общей проблемы создания интегрированных систем менеджмента (ИСМ) как компонент СУ для обеспечения безопасности объектов, именуемых сложными промышленными объектами (СлПО). В этой связи повысилась актуальность обеспечения информационной безопасности (ИБ) для потребителей, т.к. современный уровень развития информационных технологий (ИТ) позволил обеспечить больший охват производственных процессов, поддержку лиц, принимающих управленческие решения (ЛПР), реализацию процедур аудита СлПО. Применение ИТ призвано снизить сложность управления производственными процессами в режиме, близком к режиму реального времени (РРВ), но, вместе с тем, привнесло характерные риски в обеспечение безопасности СлПО. Известные подходы обеспечения ИБ, основанные на риск-ориентированных стандартах, предлагают набор систем менеджмента (СМ), базирующихся на цикле PDCA (цикле Деминга-Шухарта). В целях оптимизации затрат и повышения уровня обеспечения ИБ в последнее время для крупнейших СлПО реализуются проекты интегрированных СУ с включением ИСМ. Проведенный анализ выполненных проектов создания интегрированных СУ (как в РФ, так и в мире) с целью обеспечения ИБ для СлПО, а также 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.

Первое противоречие связано с тем фактом, что значительное количество разработанных стандартов (международных, государственных, отраслевых), применительно к области ИБ, обуславливает широчайшую вариативность версий и вариантов их применения для целей обеспечения безопасности СлПО. В частности, национальные стандарты ГОСТ Р не обновляются синхронно с пересмотром международных стандартов (например, ISO/IEC 27001:2013/Cor 2:2015 с дополнением 2015 г. и ГОСТ Р ИСО/МЭК 27001-2006). У отраслевых стандартов наблюдается более серьезное запаздывание – 2 и более поколения (например, ISO 31000:2018 и СТО Газпром 4.2-3-003-2009 «Анализ и оценка рисков»).

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 существенно ограничивает (и даже исключает) роль ЛПР в формировании «разумного подхода» к выбору и ограничению критериев. Соответственно, возникает риск неверного определения целей создания ИСМ как компоненты единой интегрированной СУ для СлПО и функциональной неполноты при формировании области распространения ИСМ (*scope*) и процессов ИБ. Для обеспечения заданного уровня ИБ необходимо совместно решать несколько противоречивых задач, в частности – перечень критериев ИБ, ограниченность ресурсов (в частности, технических средств, бюджета, времени и квалифицированного персонала).

Третье противоречие вызвано несогласованным снижением ЛПР издержек в процессах жизненного цикла (ЖЦ) и требованиями формирования контекста (*context*) ИСМ для формирования «управляющих условий» для минимизации потерь от рисков ИБ в СлПО. Данное противоречие также обусловлено динамикой изменений, присущих всем СлПО, тем более, функционирующих 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) объективно подтверждают этот факт – ЛПР ожидает снижение издержек без учета требований к ИСМ как важной компоненты интегрированных СУ.

Четвертое противоречие связано с проблемой соответствия множественным общим законодательным требованиям (*compliance*) и конкретным требованиям обеспечения безопасности 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 режимах, близких к РРВ.

Преодоление указанных противоречий между текущим состоянием теории и требованиями практики обеспечения ИБ для СлПО требует решения ряда задач научного характера, направленных на развитие теории ИБ как системы взаимосвязанных идей, основанных на классических трудах в области кибернетики и системного анализа. Главная цель – это обеспечение безопасности, учитывающее перспективные подходы и позволяющее формировать целостное представление о закономерностях, принципах и тенденциях обеспечения ИБ для СлПО. В представленной диссертационной работе изложены научно обоснованные методические подходы и технические решения (в том числе, аудиты ИБ), применение которых вносит вклад в повышение уровня ИБ для СлПО нашей страны.

Степень разработанности проблемы. Научные разработки автора, представленные в настоящем исследовании, сформировались, прежде всего, на базе научных работ В.И. Воробьева, И.А. Зикратова, И.В. Котенко, В.М. Крикуна, В.Н. Кустова, В.А. Липатникова, П.А. Лонциха, А.С. Маркова, А.А. Молдовяна, В.Д. Ногина, И.Б. Саенко, Б.В. Соколова, Р.М. Юсупова и др., а также зарубежных ученых Р. Кини, Х. Райфа, С. Кобле, Д. Мако, И. Такахара, М. Месаровича, И. Пригожина, Р. Хартенштайна, Э. Деминга, Н. Винера, Д. Чаума, Б. Шнайера и др.

Анализ современных работ свидетельствует, что наряду с имеющимися существенными достижениями в области обеспечения ИБ в соответствии с требованиями международных стандартов (ISO, IEC, NIST, IATA), государственных стандартов (ГОСТ Р и ГОСТ РВ) и отраслевых требований (СТО БР ИББС, СТО Газпром СОИБ), в настоящее время недостаточно разработаны методические подходы к обеспечению ИБ для СлПО. Известны научно-методические подходы ФСТЭК и ФСБ к построению моделей угроз и защиты государственных информационных ресурсов, а также ключевых систем информационной инфраструктуры (КСИИ). Основной акцент существующих методических документов сделан на формирование статической модели нарушителя, фиксированного перечня деструктивных действий (ДД), угроз безопасности информации (УБИ), экспертной оценки реализации и уровня значимости УБИ для объектов защиты (ОЗ). За исключением отдельных нормативных актов (Приказ ФСТЭК России № 31, ГОСТ Р 57580.1-2017), практически не применяется менеджмент рисков и процедура учета остаточных рисков.

В работах Р.М. Юсупова и др. широко освещается расширенная концепция ИБ, под которой, в отличие от «стандартной базы» ISO/IEC, понимается следующая «триада»: защита информации, защита от информации и добывание информации о намерениях и возможностях противоборствующей стороны в информационной сфере. Данная «триада», к сожалению, не рассматривается подробно в нормативных документах ФСБ, ФСТЭК, МЧС и ЦБ РФ, и, соответственно, не предложены решения для обеспечения ИБ в полном ЖЦ для СлПО. В современных автоматизированных системах управления (АСУ) СлПО (например, Siemens, Yokogawa, Hirschmann) обрабатывается только информация о состояниях отдельных элементов, но не всего ОЗ в целом. Обеспечение ИБ при создании АСУ является до сих пор сложной задачей, решение которой также затрудняется невысокой «информационной культурой» персонала. В частности, по данным Positive Technology за 2017 г. количество подключенных к сети интернет критических систем возросло в 1,5 раза. Решения класса GRC (Governance, Risk and Compliance), предложенные известными разработчиками (например, SAP, Oracle, RVision и пр.), пока не находят широкого применения в силу высокой стоимости, фрагментарного охвата функций ИБ и обязательного участия многочисленного персонала (ИТ-экспертов, аудиторов, аналитиков) для внедрения.

В работах Ю.А. Арбузова, В.Г. Лим, В.Н. Химич рассмотрены вопросы обеспечения ИБ в АСУ предприятий ТЭК. Предложена методология построения модели угроз и приведен алгоритм формирования модели УБИ в АСУ для объектов ТЭК. В работах М.В. Кремкова и А.В. Корнеева систематизированы наиболее характерные внутренние производственные и технические риски, имеющие место в работе предприятий ТЭК, а также даны рекомендации по своевременному учёту и управлению рисками при отражении кибернетического нападения. Отметим, что термин «*кибербезопасность*» был определен в Рекомендации МСЭ-Т X.120 (утвержденной в 2010 г.), и при этом были выделены такие задачи, как обеспечение доступности, целостности и конфиденциальности.

В то же время, как показывает анализ работ научно-практических конференций, существенную проблему представляет методический и последующий технологический разрыв между средствами (мерами) обеспечения ИБ (*controls*, СрЗИ), функционирующими в режимах, близких к РРВ, с одной стороны, и базовыми возможностями существующих СУ для комплексной оценки уровня ИБ (конкретно – процессы аудита), с другой стороны. Эту проблему поднимали еще Н. Винер и И. Пригожин в своих работах по теории кибернетики, но актуальность объективно сохраняется до сих пор. Например, в годовом отчете Cisco по ИБ за 2018 г. отмечается, что среднее время обнаружения УБИ (*time to detection*, TTD) сократилось до 4,6 часов, в 2017 г. этот показатель составлял 14 часов, а в 2016 г. – 39 часов.

В работах Р.М. Юсупова, Б.Г. Юдина, Б.В. Соколова отражены подходы к созданию защищенных ИС, которые предоставляют практические реализации новых направлений в науке, в частности – «технонауки» (*technoscience*), которые хорошо увязываются с общими принципами классической кибернетики, в частности, более активное применение контуров обратной связи (ОС) для усиления полезных воздействий и ускорения стабилизации защищаемого объекта (СлПО), например, процессы аудита ИБ. В то же время на практике не представлены подходы к созданию ИСМ, которые, применительно к СлПО, обеспечивают требуемый доказательный уровень обеспечения ИБ, т.к. до сих пор основной метод противодействия ДД злоумышленников заключался в «привязке» фиксированного перечня СрЗИ к УБИ, но не «настройки» процессов ИБ (например, управления инцидентами, и/или непрерывностью). Такой подход наблюдается практически для всех СУ при реализации только низкоуровневых функций обеспечения ИБ. В работах зарубежных ученых Д. Кэннона, С. Кобле, Л. Дерека, Л. Гордона, Г. Хинсона и др. отражены современные проблемы формирования метрик ИБ при обеспечении ИБ для СлПО.

Существенным недостатком современных подходов к созданию, внедрению, документированию и сопровождению ИСМ является практическое отсутствие достоверного методического аппарата, контроля адекватности процесса оценивания (аудит ИБ) и получения достоверных оценок уровня ИБ в СлПО для ЛПР в режиме, близком к РРВ. В частности, не представлена оценка результативности интегрированной СУ, которую предлагается в ряде работ (например, Р. Кини, Х. Райфа, И. Пригожин, Ф. Перегудов и др.) формировать через суперкритерии, что не всегда позволяет использовать надежный математический аппарат в режиме, близком к РРВ. Отчасти, положения теории Парето для доминирующих множеств позволяют формировать векторы принятия решения для дискретного числа альтернатив и эффективно применять для выбора оптимального множества решений ЛПР.

В то же время необходимо отметить, что до настоящего времени не предложен метод оценки векторов возможных решений при условии значительного различия их значимости (ценности) и возможных замещений – применительно к задачам обеспечения ИБ для СлПО. Наилучшей иллюстрацией данного факта является многолетняя деструктивная «работа» вируса Stuxnet, в создании которого подозреваются специальные службы ряда государств. Приблизительные задержки в развитии ядерной программы Ирана практически без какого-либо силового вмешательства составили 4 года, в результате управляемого резонанса частот были разрушены центрифуги для обогащения урана. Практически не представлены работы (за исключением исследований А.Н. Ефимова и Г. Хинсона), позволяющие предложить

гибкий и простой математический аппарат для формирования оптимального множества метрик ИБ, чувствительных к динамически изменяемым требованиям к интегрированным СУ. Очевидно, что введение в существующий математический аппарат функций риск-менеджмента и «привязки» к фазам ЖЦ (для каждого уникального СлПО) и введения ОС в цикле PDCA позволило бы ЛПР совершенствовать систему аудита ИБ и значительно поднять скорость принятия эффективного управленческого решения. Представляется перспективным реализовать совместно функции риск-менеджмента, гибких ОС, «замыкания» цикла PDCA, простого и эффективного математического аппарата в методе «мгновенных аудитов» ИБ. Этот метод предложено применять при противостоянии современным атакам.

Опубликованные работы зарубежных ученых в области ИБ свидетельствуют о внимании к методам и практикам отдельных процессов в широком перечне требований, например, управления идентификацией (работы С. Кобле, М. Хансена, Д. Чаума), управления безопасностью данных (работы А. Аквисти), управления безопасностью и чрезвычайными ситуациями (работы С. Дое), применения метрик ИБ (К. Бротби и Г. Хинсона). Тем не менее, не предложен целостный подход для комплексного противодействия современным угрозам ИБ для СлПО. В этой связи следует учесть постулат Н. Винера о методе управления с помощью информирующей ОС и локализации ошибок обратным процессом, с условием, чтобы проверка шла с такой же скоростью, что и само вычисление и предложения проф. Р. Хартенштайна о реконфигурировании управления.

В опубликованных работах также не рассматриваются процессы проектирования ИСМ (как компоненты интегрированной СУ) с позиции обеспечения экономического баланса между стоимостью защищаемых активов (*asset*) в составе СлПО с гарантированным уровнем обеспечения ИБ (заданным ЛПР), с одной стороны, и стоимостью внедренных технических средств (мер) ИБ в СлПО, с другой стороны. В известных случаях демонстрируется только фиксированный набор средств (мер) ИБ, рекомендованный ФСТЭК (Приказы № 31, 235, 239) и/или ФСБ (Приказ № 796) для типовых решений – например, объектов ТЭК и удостоверяющих центров. В существующей практике (Марков А.С., Цирлов В.Л.) широко применяются стандарты ISO/IEC серии 15408 (на базе «Общих критериев»), а также новые модифицированные варианты, в частности, cPP (*common process performance*), призванные упростить и значительно ускорить процедуры объективной независимой оценки технических систем (ТС). Обобщая вышеизложенное, **научная проблема** представленной диссертационной работы формулируется как проблема разрешения противоречий между состоянием теории ИБ (в частности, неполноты определения требований к аудиту ИБ) и современными требованиями практики по обеспечению ИБ в 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:

- моделей (***M = { M | 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 аудиту ИБ), ***R*** (собственных свойств ТС), ***K*** *(*мер и средств обеспечения ИБ), ***T*** (совокупности требований в аспекте ИБ для СлПО) и ***G*** (совокупности ДД и выявленных рисков);
- методов (***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 $M: (A \to A', R \to R', K \to K', T \to T', G \to G')$, 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 $\| N - N' \| \to \Delta N_{min}$

$$m: C \xrightarrow{0} N$$

Актуальность и степень разработанности темы определяют **цель диссертационного исследования**: снижение длительности и стоимости аудита ИБ за счет использования новых моделей и методов аудита ИСМ, реализующих оперативное формирование количественной оценки уровня обеспечения ИБ в СлПО, выбор и применение наилучшего множества средств (мер) обеспечения ИБ для обработки выявленных рисков. Достижение поставленной цели потребовало решения следующих **задач** для обеспечения требуемого уровня ИБ в СлПО:

1. 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 как компоненты интегрированной СУ для различных отраслей промышленности;
2. 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;
3. Исследование, анализ и создание иерархической структуры показателей (метрик) ИБ в процессах обеспечения ИБ, в том числе, аудита ИБ, предназначенных для формирования и оценивания требований ИБ в СлПО;
4. 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;
5. Исследование практической применимости предложенных методов обеспечения ИБ в составе ИСМ для СлПО для различных отраслей промышленности.

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

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

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

Цель исследования достигается решением научной проблемы исследования существующих подходов при разработке, документировании, внедрении и независимой оценке (аудите ИБ) в ИСМ и разработкой новых методов для обеспечения ИБ в СлПО.

Теоретической базой исследования являются работы Р.М. Юсупова, И.Б. Саенко, Б.В. Соколова, А.А. Молдовяна в области обеспечения комплексной безопасности и теории управления. Развитие существующих подходов в области ИБ основано на предложенном ранее автором методе оценки (аудите) СМИБ на основе модифицированного метода анализа иерархий (МАИ). Дальнейшее развитие этого подхода применительно к поставленной научной проблеме нашло практическую реализацию при создании базовой модели аудита ИСМ и дополнительными новыми методами оптимизации процесса аудита.

Научные положения, выносимые на защиту. Решение задач диссертационного исследования позволило разработать и обосновать ряд научных положений, которые выносятся на защиту.

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 СлПО, заключающаяся в широком применении системы численных показателей (метрик) ИБ для оценки результативности ИСМ как компоненты интегрированной СУ 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 РРВ.

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 аудитом ИБ по частоте и предоставляет ЛПР оценку роста уровня обеспечения ИБ в СлПО как показатель результативности (*effectiveness*) ИСМ и соответствия применимым требованиям.

Третье научное положение – метод исследования динамики сертификации по международным стандартам ISO для СлПО. Предложен новый метод исследования показателей динамики сертификации, основанный на публичных статистических данных ISO, устанавливающий оценку влияния «лидеров» разного ранга и учитывающий приоритеты отраслей в соответствии с международными кодами экономической деятельности EAC. Новый метод позволяет оценить «входные» динамические изменения потребностей бизнеса, выраженные в изменении предпочтений ЛПР по составу внедряемых СМ, прошедших независимый аудит в составе ИСМ и формировать прогнозные оценки.

Четвертое научное положение – метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО, который, в отличие от известных стандартов ISO и ISO/IEC, обеспечивает координацию, распределение ресурсов и оперативное информирование ЛПР по оценке результативности аудита ИСМ. Предложенный метод обеспечивает научно обоснованное и целенаправленное функционирование ИСМ как компоненты интегрированной СУ, и отличается от существующих методов циклическим непрерывным оцениванием ИБ на основе оптимальной системы численных показателей (метрик) ИБ.

Научная новизна представленной диссертационной работы состоит в следующем. Впервые в целостном функциональном представлении сформулирован научно-методический аппарат для обеспечения аудита ИБ для СлПО, основанный на современном комплексном риск-ориентированном подходе, специальных моделях и методах выполнения аудита ИБ. Результатом исследования нескольких смежных научных областей (теории управления, теории множеств и теории принятия решений), явилось развитие понятийного аппарата теории обеспечения ИБ для СлПО, а также разработка новых моделей и методов аудита ИБ, позволяющих формировать оптимальный перечень метрик ИБ и выполнять количественную оценку уровня обеспечения ИБ. Новизна комплекса моделей и методов заключается в формировании функционально завершенной структуры для выполнения аудита ИБ в ИСМ.

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 генерировать 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 разработана иерархическая система показателей (метрик) ИБ, позволяющая, в отличие от применяющейся аттестации или ежегодного фиксированного аудита, формировать и учитывать при принятии решения ЛПР метрики (оценки ИБ) в режиме, близком к РРВ.

Новизна второго научного положения заключается в том, что впервые для планирования и оценки (аудита) ИСМ для СлПО предложен метод «мгновенных аудитов», учитывающий меру адекватности выполнения применимых требований ИБ «не вообще», а в

той мере, которая достаточна для достижения в срок поставленной цели аудита. 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, по сравнению с существующими методами, контролировать динамику изменения оценки уровня обеспечения ИБ («динамической перестройки» критериев аудита). Важным преимуществом нового метода является акцентирование именно на получении численных оценок, а не простого «соответствия» или «несоответствия». Предложенный метод позволяет дополнительно исправлять ошибки, присущие сложному процессу аудита.

Новизна третьего научного положения заключается в том, что в отличие от публикующихся периодических обзоров (содержащих общую статистику), предложен новый метод исследования динамики сертификации по международным стандартам ISO. Представленный метод содержит математический аппарат, позволяющий оценивать зависимости степени развития разных организаций (например, по кодам отраслей EAC) 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, представленные в публичных статистических данных ISO в соответствии с предложенным методом, позволяют проследить взаимосвязь с общим «успехом» по конкретной отрасли для «лидеров» разных рангов. Представленный метод универсален, реализует обобщенный подход к оценке и определяет «лидеров» по кодам EAC вне каких-либо ограничений.

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 оперативного информирования ЛПР в части обеспечения ИБ, в случае выявления такой необходимости, а не только фиксированные ежегодные встречи в рамках выполнения анализа 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 различных типов защищаемых активов СлПО, а также новые законодательные и/или отраслевые нормативные требования.

Теоретическая значимость диссертационного исследования состоит в обосновании возможности применения новых моделей и методов обеспечения ИБ на основании независимой оценки (аудита) ИБ в СлПО, созданных в соответствии с требованиями современных риск-ориентированных стандартов; определении новых критериев выбора множества требований, оптимальных для конкретного СлПО; определении новых условий формирования оптимального множества критериев оценки (метрик) ИБ и развитии научного аппарата независимой оценки ИБ в ИСМ (как компоненты интегрированной СУ) для СлПО.

Теоретическое значение имеют следующие научные результаты.

Первое научное положение позволяет расширить границы применимости теории обеспечения ИБ для СлПО, отличительными свойствами которой являются:

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

Второе научное положение позволяет реализовать в методе «мгновенных аудитов» ИСМ для СлПО важные методические аспекты:

1. Раздельные интерфейсы для внешних и внутренних заинтересованных сторон (*stakeholders*), реализующие предоставление информации с заданной частотностью;
2. Включение контуров гибкой ОС по всем типам аудита позволяет повысить уровень обеспечения ИБ и оперативно агрегировать всю необходимую информацию для ЛПР;
3. Вовлечение в принятие «разумных решений» ЛПР, которое может являться и коллегиальным органом управления, в том числе, с участием внешних заинтересованных сторон.

Третье научное положение позволяет обеспечить в методе исследования динамики сертификации по стандартам ISO необходимую информацию для поддержки принятия «разумных решений» ЛПР при обеспечении ИБ в ИСМ для СлПО благодаря:

1. Формированию на основании публичной достоверной статистики ISO оценок приемлемости выбора: по составу ИСМ, по необходимости внешней оценки (аудита) для функций обеспечения стабильного роста, безопасности и устойчивости бизнес-процессов, защиты ценных активов (в том числе, нематериальных, *goodwill*);
2. Определению коэффициентов зависимости (корреляции) для отраслей «лидеров» по рангам, рассчитываемых для произвольного количества отраслей промышленности.

Четвертое научное положение включает систему методов многошаговой оптимизации аудита ИБ в ИСМ (как компоненты интегрированной СУ) и позволяет реализовать гибкий подход к выполнению аудита ИБ в зависимости от фазы ЖЦ для СлПО.

Выдвинутые теоретические положения подтверждены практикой в процессе выполнения диссертационного исследования и открывают новые перспективы для работ в области управления ИБ, в частности, аудита ИБ.

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, минимизацию потерь при возникновении ситуаций риска ИБ, присущих СлПО, а также повышение степени соответствия законодательным требованиям (*compliance*). Представленные методы и модели аудита ИБ для СлПО реализованы как функционально завершенный элемент в системе мероприятий комплекса обеспечения ИБ. Результаты диссертационного исследования получили **практическую реализацию** в следующих предметных областях:

1. **Информационные технологии**. В компании ИТСК (РФ) реализован комплекс новых методов аудита ИБ с учетом иерархической системы критериев модели ИСМ.
2. **Воздушный транспорт**. В международных аэропортах Алматы и Астаны (Республика Казахстан) реализован комплекс новых моделей и методов аудита ИБ в составе ИСМ в соответствии с требованиями международных стандартов ISO и дополнительных отраслевых требований IATA (ISAGO).
3. **Системная интеграция**. В группе компаний «Газинформсервис» (РФ) реализован комплекс новых моделей и методов аудита ИБ при создании ИСМ, в том числе, для группы компаний «Газпром нефть».
4. **Образование.** В международной компании AQS (Азербайджан) реализованы новые принципы обучения аудиторов (ведущих аудиторов) ИБ, основанные на разработанных методах проведения аудита ИБ, в том числе, с учетом требований международных стандартов ISO.
5. **Банковское дело**. В Акционерном коммерческом банке «Рускобанк» (РФ) реализован комплекс новых методов проведения аудита ИБ, в том числе, с учетом требований ISO и СТО БР ИББС.
6. **Управление коммунальными объектами критической инфраструктуры.** В ГУП «Водоканал Санкт-Петербурга» (РФ) реализован комплекс новых методов проведения аудита ИБ для СМИБ в составе ИСМ с учетом требований, предъявляемых к СлПО.

Достоверность и обоснованность полученных результатов подтверждается:

- широким обсуждением на всероссийских и международных научных и научно-практических конференциях;
- доказанным положительным эффектом от ряда внедрений результатов представленного диссертационного исследования;
- сопоставление результатов с известными аналогичными исследованиями за длительный период (Reuters, Deloitte, Ernst&Young, McKinsey, PwC, Cisco, SAP);
- сопоставление с публичными данными национальных («Эшелон», ФСТЭК, Positive Technology) и международных аналитических обзоров сертификации (ISO);
- корректностью применения апробированного в научной практике исследовательского и аналитического аппарата;
- строгостью математических соотношений, использованных для моделей и методов оценки (аудита) ИБ;
- результатами независимых оценок (аудита) ИСМ в рассматриваемых предметных областях («Русский Регистр», TUV, Lloyd, BSI, DNV);
- публикацией результатов диссертационного исследования в рецензируемых научных изданиях, в том числе, индексируемых Scopus и/или Web of Science.

Основное содержание диссертационной работы и сопутствующие результаты выполненных исследований опубликованы в печати. Научные результаты получены лично автором и непосредственно связаны с его научно-практической деятельностью, в том числе, при выполнении им проектов в области ИБ на территории РФ и стран СНГ.

Апробация и реализация результатов диссертации проводилась в виде личных докладов на ведущих международных и всероссийских научных и научно-технических конференциях, в том числе ежегодных: DCCN, FRUCT, «Комплексная защита информации», «ИБ АСУТП КВО», IT&MQ&IS и пр.

Результаты диссертации реализованы при выполнении ряда крупных проектов, в том числе, комплексных и совместных аудитах на предприятиях ТЭК (РФ), авиационного комплекса (Казахстан), ИТ (РФ), в образовательных учреждениях (Азербайджан, Белоруссия, РФ), в кредитных организациях (РФ) и пр.

Публикации. Основные результаты диссертационного исследования, впервые содержащие защищаемые научные положения, нашли отражения в **38** статьях, опубликованных в научных журналах, рекомендованных ВАК РФ, в **15** изданиях, индексируемых Scopus и/или Web of Science, в **2** рецензируемых учебных пособиях, а также в **12** публикациях в иных рецензируемых научных специализированных изданиях.

Личный вклад автора в основных публикациях с соавторами кратко характеризуется следующим образом: [1 – 4, 14] представлен новый подход к учету рисков ИБ и выполнению аудита ИБ в ИСМ; в [6 – 8] представлен новый подход к выполнению аудита ИБ в ИСМ; в [5, 9] предложен новый метод «мгновенных аудитов» ИБ; в [10 – 12, 18] предложены новые метрики ИБ для выполнения аудита в ИСМ; в [13, 16, 30] представлены подходы к выбору активов СлПО и оценке безопасности ИТ; в [28] представлена новая оценка доступности ТС при выполнении аудита ИСМ; в [35, 36] представлены новые методы для определения результативности ИСМ.

Структура и объем диссертации. Диссертационная работа включает: введение, **6** глав, заключение, перечень сокращений, перечень терминов и определений, список литературы и приложения. Объем диссертации: **407** страниц, в том числе список литературы на **29** страницах, **88** рисунков и **70** таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, проведен анализ исследуемой научной проблемы и обоснован подход к ее решению, сформулированы цель и задачи диссертационного исследования, определена научная новизна и практическая значимость результатов, сформулированы основные научные положения, выносимые на

защиту, аргументированы обоснованность и достоверность полученных результатов, а также приведены сведения об их реализации и апробации.

Первая глава диссертации посвящена исследованию направлений развития теоретических и методологических аспектов теории ИБ и постановке задач, направленных на разрешение выявленных противоречий между состоянием теории и требованиями практики при планировании и проведении аудита ИБ в ИСМ для СлПО. Глава 1 содержит материалы исследований, относящиеся к первому защищаемому положению. Новая постановка задачи для выбора ЛПР предпочтений сформирована (в нотации теории надежности и эффективности ТС, предложенной Воробьевым С.Н., Егоровым Е.С., Торбиным В.У.) с учетом формальных контрольных процедур, базирующихся на измерениях.

Обозначим:

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

Тогда модель проблемной ситуации описывается как:

$$\langle \mathbf{U, A, G, Y, H, W, \Psi, K, \Omega, \theta'} \rangle \qquad (1)$$

Для решения проблемы принятия решения ЛПР требуется определить, уточнить и оценить состав общей информации о проблемной ситуации ($\mathbf{\theta'}$), как важнейший элемент формирования оперативных и эффективных управленческих решений для ЛПР, основанных на объективных достоверных данных. В качестве ограничений предложено рассмотреть: сроки ожидания ЛПР, допустимые затраты, принципиальная возможность реализации всей системы сбора информации о проблемной ситуации $\mathbf{\theta'}$ и сложность практической реализации ряда элементов, которые рассмотрены подробнее в диссертации. На рисунке 1 представлена обобщенная модель ИСМ для обеспечения безопасности СлПО.

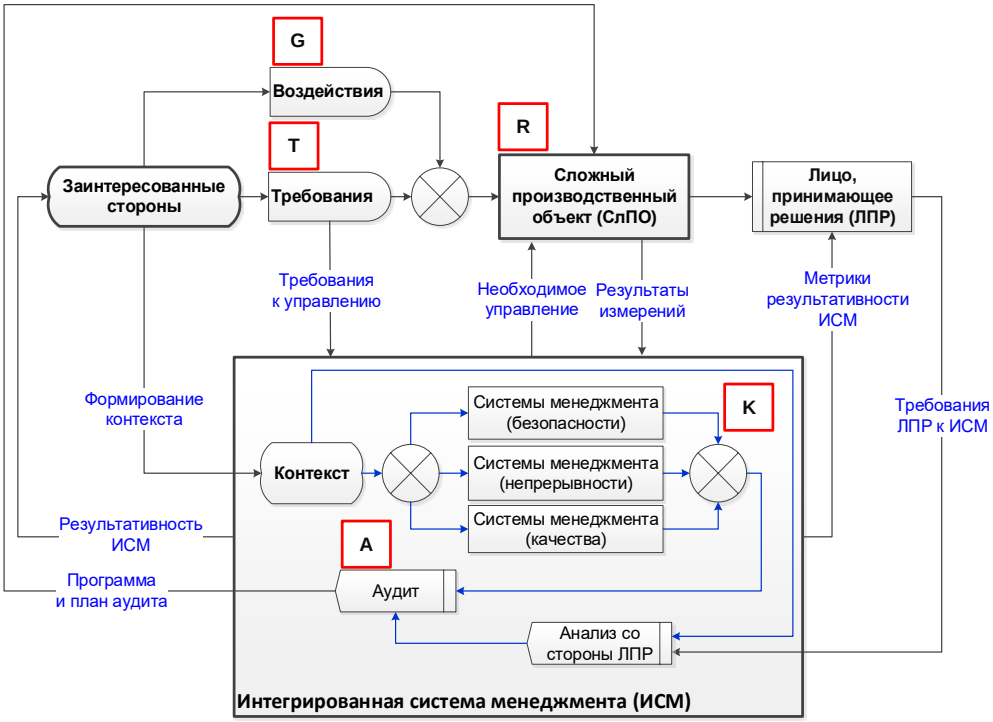

Рисунок 1 – Обобщенная модель ИСМ для обеспечения безопасности СлПО

С учетом применения риск-ориентированных стандартов в ИСМ представляется важным гарантировать «замыкание» цикла PDCA при управлении ИБ для СлПО и формирование контекста СлПО как «открытой системы» в терминах И. Пригожина. В соответствии с применяемой выше нотацией, предложена новая модель проблемной ситуации. На основании имеющейся дополнительной уточненной информации $\boldsymbol{\theta'_N}$ и результатов «контрольного» оценивания (аудита) ИБ СлПО необходимо определить модель предпочтений ЛПР – **Ω**, приведенную в (1). Отметим, что наличие **A** в (1) означает, что часть значений неопределенных факторов будет обязательно установлена (например, требования проведения аудита ИБ заданы регуляторами), а другая часть будет определена в процессе решения новых самостоятельных задач (например, формирования оптимального перечня средств (мер) и обеспечения ИБ, рекомендованных ЛПР к внедрению в процессе аудита ИБ).

Во многих практических случаях априорное значение коэффициента эффективности **К** приводит к формированию множества «нехудших альтернатив». Это может означать в конкретном случае для СлПО, что по результатам аудита ИБ могут быть сформированы несколько достойных альтернатив, но мера выбора из «нехудших» единственной – задача решается ЛПР посредством модели **Ω** (модели предпочтений ЛПР). Общая постановка задачи моделирования предпочтений представлена в виде:

$$\langle \mathbf{D}, \theta'_N ; \Omega_D \rangle \qquad (2)$$

где:

D = {U, A, G, Y, W, K}

θ'_N – дополнительная уточненная информация о проблемной ситуации.

Предлагается уточнить перечень требований к аудиту ИБ, расширить и уточнить состав дополнительной информации о проблемной ситуации θ'_N за счет новых факторов и представить задачу формирования множества стратегий ЛПР в новом виде:

$$\langle \theta_{A0}, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, A_N, U_N \rangle \qquad (3)$$

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 (1-й, 2-й и 3-й стороной);

θ_3 – информация об инцидентах ИБ (например, DLP, SIEM, SOC);

θ_4 – информация о новом «контексте» ИСМ;

θ_5 – информация о новых предпочтениях ЛПР;

θ_6 – информация об изменениях ФЗ (например, ФЗ-187 «ГосСОПКА»);

A_N – адаптивное множество значений определенных и неопределенных факторов;

U_N – адаптивное уточненное множество стратегий ЛПР.

На основании постановленной задачи предложена базовая модель аудита ИСМ, которая содержит все требуемые сущности для выполнения аудита ИБ (критерии, объект, наблюдения аудита и пр.) и позволяет генерировать оценки уровня обеспечения безопасности. Отметим, что переход от обобщенной модели ИСМ к модели «конкретной ситуации» является сложным, особенно, когда речь идет об анализе больших и сложных ТС (в том числе – СлПО), а в ряде случаев применяются только эвристики, т.к. многие элементы явно не заданы. На рисунке 2 представлена базовая модель аудита ИСМ, необходимая как концептуальная база для описания подходов к поставленной задаче. В этой модели, как части обобщенной модели ИСМ (см. рисунок 1), детально отражена возможность сопоставлять планируемые и реальные состояния интегрированной СУ для СлПО (как ОО). При этом реализуется «замкнутый» цикл аудита (в смысле гарантированного выполнения всех обязательных процедур аудита ИБ). Для конкретной задачи управления ИБ в интегрированной СУ для СлПО «замкнутый» цикл аудита означает гарантированное достижение результатов всех фаз цикла PDCA, выявления причин несоответствий и результативное выполнение всех запланированных корректирующих действий в срок. Объективные результаты любых аудитов ИСМ, в т.ч. статистика инцидентов ИБ, являются

достоверными и объективными данными, которые могут быть приняты как апостериорные оценки свойств фактически реализованной системы безопасности для СлПО.

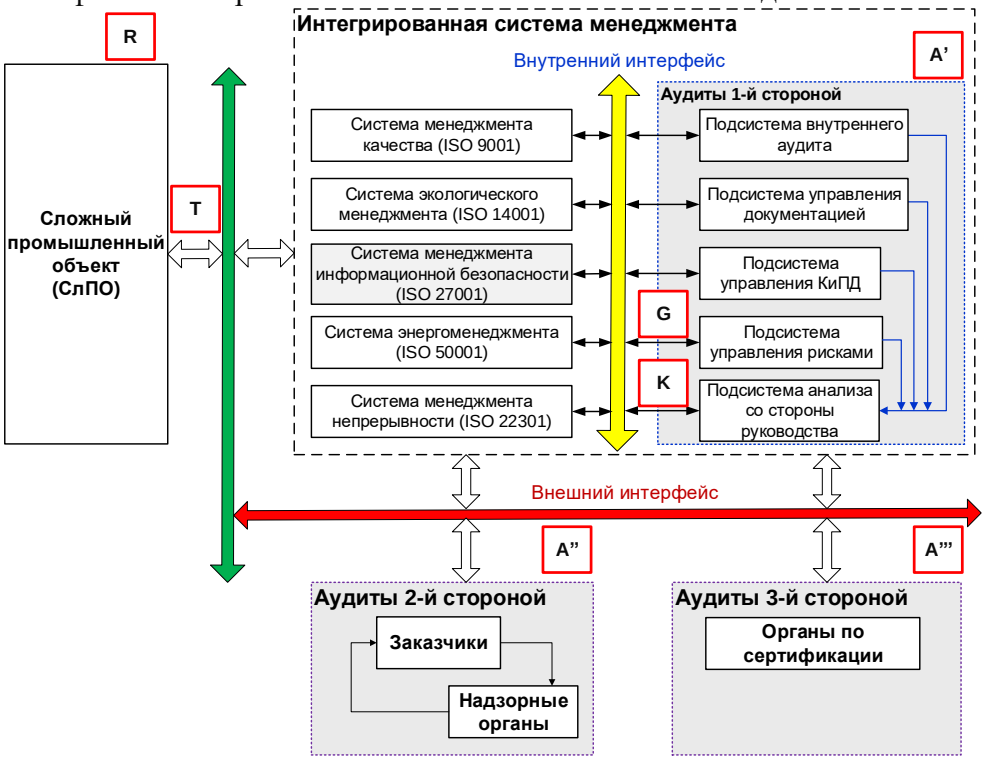

Рисунок 2 – Базовая модель аудита ИСМ

При этом ЛПР имеет возможность сколь угодно уточнять (на основе полученных данных) оценки фактического состояния безопасности СлПО, например, по процессам, в том числе, сопоставляя затраты и величину ущерба (если имел место инцидент ИБ). Таким образом, может быть предложена следующая математическая оценка риска ИБ для СлПО как математическое ожидание двух слагаемых (прямого и косвенного ущерба соответственно):

$$\boldsymbol{R_t = M_t\left(R_t^1 + R_t^2\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} S^1{}_{ij} \cdot V^1{}_{ij} + \sum_{i=1}^{n}\sum_{j=1}^{m} S^2{}_{ij} \cdot V^2{}_{ij}}$$

где:

i – возможные ДД для конкретного СлПО (с учетом возможности реализации),

j – возможные сценарии реализации ДД для конкретного СлПО,

S^1_{ij} – величина прямого ущерба при реализации риска возможных ДД,

S^2_{ij} – величина косвенного ущерба при реализации риска возможных ДД,

V_{ij} – вероятность реализации риска возможных ДД.

На основании рассмотренных практик аудита ИБ в СлПО представлен новый метод определения численных показателей (метрик) ИБ. В диссертации отмечается, что с целью снижения издержек (это одна из приоритетных задач бизнеса и форма оценки результативности службы ИБ) могут быть применены метрики, например, на базе ISO/IEC (ГОСТ Р ИСО/МЭК) серии 27004. ЛПР может получать необходимые данные для принятия эффективных управленческих решений для обеспечения требуемого уровня безопасности СлПО только при наличии ИСМ, оперирующих достоверными оценками. Критериями результативности ИСМ выступают показатели степени соответствия процессов ИБ установленным требованиям, а также результаты оперативного оценивания ЛПР (*management review*) заданных и фактических показателей деятельности.

Для оценки степени достижения целей ИБ (т.е. оценки результативности) рекомендуется применять метрики ИБ, которые обеспечивают поддержку принятия решений ЛПР на соответствующих уровнях иерархии. Пример расчета метрик ИБ для 4-х выбранных средств (мер) обеспечения ИБ показан на рисунке 3.

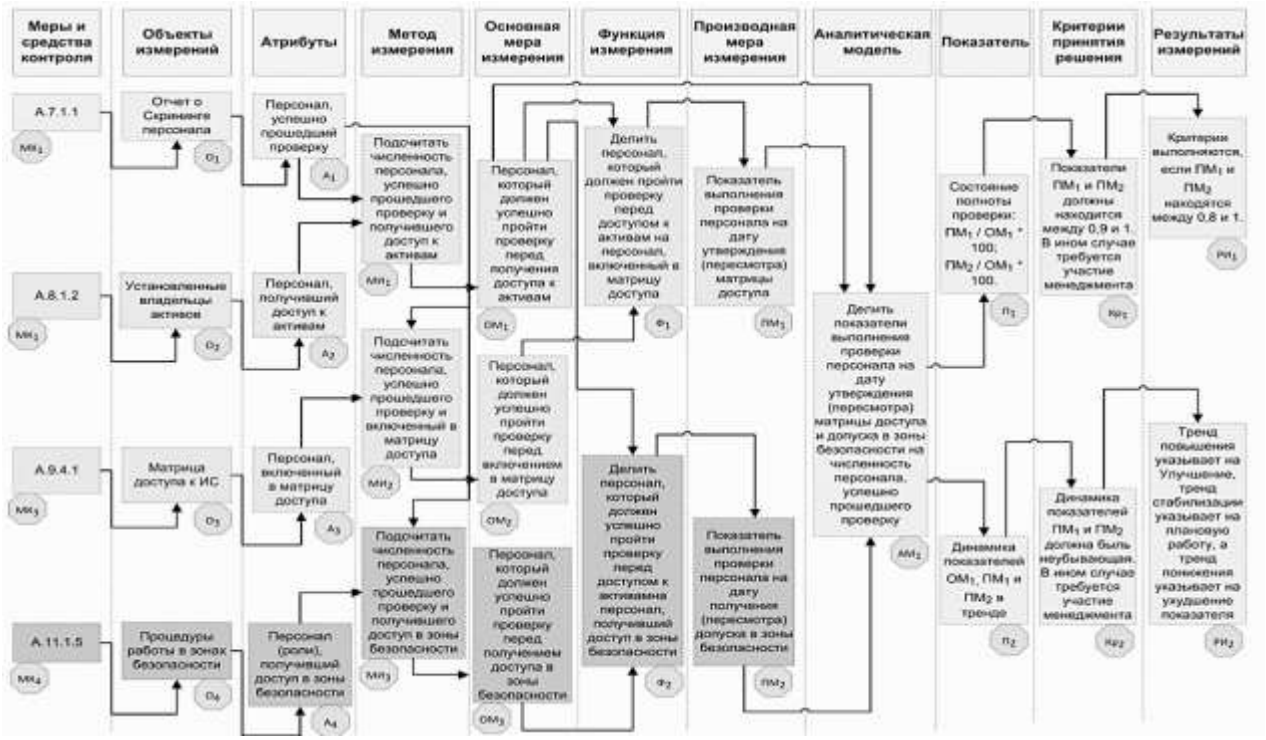

Рисунок 3 – Пример расчета метрик ИБ

Вторая глава посвящена вопросам уточнения множества ограничений (в т.ч. законодательных) для базовой модели аудита ИСМ для СлПО. Исследование показало, что одной из важнейших задач является точное определение объекта аудита – СлПО. Следующее исследование касается изучения критериев (требований) аудита ИБ для СлПО (помимо указанных в Главе 1 диссертации), прежде всего – применимого законодательства, которое охватывает (но не ограничивается): Федеральные законы (ФЗ-187, ФЗ-256), Распоряжение Правительства (например, 1314-Р), приказы ФСТЭК России (№ 31, № 235, № 239), Методические рекомендации МЧС по инвентаризации критически важных объектов (КВО). Выявлено, что в настоящее время на законодательном уровне РФ не в полной мере определены механизмы взаимодействия и ответственность субъектов, прямо или косвенно участвующих в обеспечении безопасности КИИ: органов государственной власти, служб безопасности, разработчиков решений в области ИБ.

Механизмы государственного лицензирования, надзора и контроля в этой сфере не в полном объеме закреплены законодательными актами, и в результате эти функции не в полной мере эффективны (например, документы КСИИ ФСТЭК с 2007 г. не прошли регистрацию в Минюсте, и в мае 2018 г. выведены из оборота). На данный момент можно констатировать отсутствие единых норм и системного подхода при построении системы защиты КИИ. По итогам предпринятого исследования под термином СлПО понимается «технический объект, имеющий систему управления, несанкционированное изменение штатного режима функционирования которого, связанное с нарушением свойств ИБ, может привести к угрозе техногенных катастроф с необратимыми последствиями».

Проведено исследование терминологии, применяемой при выполнении аудита ИБ в ИСМ для СлПО. В диссертации представлены множественные существенные различия в определениях из действующих нормативных документов РФ по тематике ИБ, например, «*доступность информации*», «*угроза безопасности информации*», «*целостность информации*» и пр. Дальнейшее исследование посвящено методам категорирования рисков СлПО, в частности, рассмотрены существующие методы на базе ISO (ГОСТ Р) серии 15288, ISO (ГОСТ Р) серии 31000, ГОСТ 51901, РД 08-120-96, NIST SP 800-53 и ряда научных разработок (в частности, ФГУП «НТЦ «Промышленная безопасность», «НПП «ИСТА-Системс» и ФГУ ВНИИ ГОЧС, NIST, ISO, IATA). Помимо «классических» методов оценки рисков, рассмотрены дополнительно отраслевые документы ICAO: Doc 9859 и Doc 8973/8.

Для эффективного управления СлПО, ЛПР должно учитывать множество факторов, способных оказать значительное воздействие на режимы функционирования, например:

- $\boldsymbol{\eta_1}$ – внешние негативные воздействия на СлПО (в том числе, ДД),
- $\boldsymbol{\eta_2}$ – последствия инцидентов ИБ (ремонт или простой оборудования АСУТП),
- $\boldsymbol{\eta_3}$ – внутренние события, например, невыполнение запланированных мероприятий ИБ,
- $\boldsymbol{\eta_4}$ – непредвиденные события, например, отказ в техническом обслуживании и пр.

Математическая модель такого процесса может быть представлена в виде:

$$\mathbf{R_t}\left(\mathbf{PR_j}\right) = \boldsymbol{f}\left(\boldsymbol{\alpha}^{\boldsymbol{\eta i}}_{\mathbf{PRj}}, \boldsymbol{\eta_i}(\mathbf{PR_j})\right)$$

где:

$\mathbf{R_t\,(PR_j)}$ – совокупное влияние множества факторов $\boldsymbol{\eta_i}$ на процесс PR_j,

$\boldsymbol{\eta_i}$ $\mathbf{(PR_j)}$ – воздействие фактора $\boldsymbol{\eta_i}$ на процесс ИБ PR_j,

$\boldsymbol{\alpha}^{\boldsymbol{\eta i}}_{\mathbf{PRj}}$ – весовой коэффициент воздействия фактора $\boldsymbol{\eta_i}$ на процесс ИБ PR_j

Тогда с учетом требований обеспечения безопасности СлПО на всех этапах ЖЦ можно определить влияние конкретных факторов для аудита каждого процесса ИБ в ИСМ. Пример размещения влияния факторов ($\boldsymbol{\eta_1}$ – $\boldsymbol{\eta_m}$) с учетом известных процессов (PR_1 – PR_m) применительно к фазам цикла PDCA показан в таблице 1.

Таблица 1 – Влияние факторов для аудита процессов ИБ по фазам PDCA

Фактор	**Фаза PDCA (перечень процессов по фазам)**			
	PR_1	**PR_2**	**…**	**PR_m**
$\boldsymbol{\eta_1}$	η_1 (PR_1)	η_1 (PR_2)		η_1 (PR_m)
$\boldsymbol{\eta_2}$	η_2 (PR_1)	η_2 (PR_2)		η_2 (PR_m)
…	…	…	…	…
$\boldsymbol{\eta_n}$	η_n (PR_1)	η_n (PR_2)		η_n (PR_m)

Отметим, что определение $\alpha^{\eta i}_{PRj}$ может выполняться по классическому методу МАИ (Т.Саати) или по модифицированным методам на базе МАИ, например, на основе разработанной модели СМИБ, ранее предложенной автором. В диссертации отмечается, что для эффективного управления рисками ИБ необходимо обеспечить поддержку ЛПР со стороны внешних заинтересованных сторон с целью выявления, идентификации, управления и контроля событий ИБ, потенциально способных повлиять на достижение целей организации. Пример реализации процесса управления рисками ИБ в СлПО для одной ключевой фазы «Plan» цикла PDCA в интегрированной СУ показан в диссертации.

Дополнительно отметим важность для формирования эффективных ОС внешней информации, в частности: проведение учений по отражению атак СлПО (учения «Кибер-Антитеррор-2016», проведенные на Лукомльской ГРЭС в Белоруссии и учения «Ростелеком» в 2017 г. в РФ). Достоинства и недостатки различных методов оценки уровня обеспечения ИБ изложены в диссертации. С учетом выполненных исследований сформирована структура критериев оценки уровня ИБ на объектах ТЭК, включающая 3 иерархических уровня:

1. Базовые (например, на базе ISO/IEC или ГОСТ Р ИСО/МЭК серии 27001, 22301 и пр.)
2. Дополнительные (например, на базе ГОСТ Р 51901 и пр.).
3. Специальные (например, ISAGO, FMEA, HAZOP и пр.)

Следующее исследование посвящено анализу процессов формирования требований ИБ и оценивания на их базе уровня обеспечения безопасности СлПО. Выполнено исследование, отражающее важность обеспечения национального ИТ-суверенитета РФ. Известно, что революция в области ИТ, произошедшая в конце XX века, имела весьма интересное свойство: вопросы ИБ практически полностью утратили самостоятельность и стали органичной и неотъемлемой частью ИТ. Однако в настоящее время даже при реализации программы «ГосСОПКА», по мнению ряда экспертов, возникают серьезные проблемы, например, отсутствие собственного доверенного ПО: как общесистемного (операционных систем, СУБД), так и прикладного (например, для моделирования), собственной элементной базы и телекоммуникационного оборудования. Соответственно, необходимо создавать в

России национальную полноформатную, сбалансированную и самодостаточную индустрию ИТ. Для достижения этой цели «доверенные» национальные ИТ должны быть «пронизаны» функциями безопасности от базиса до самого верхнего слоя (например, по модели ISO/OSI).

В третьей главе представлены материалы исследований, относящиеся ко второму защищаемому положению. Проблема выполнения измерений (как процесс оценки) для больших и/или сложных систем рассматривалась в классических трудах Н. Винера, Р. Кини, Х. Райфа, И. Пригожина. Рассматривая объект ИСМ, подразумевается открытая система, которая постоянно осуществляет обмен (в частности – информационный) с внешней средой. Иначе говоря, ИСМ, как компонента интегрированной СУ, и создается для эффективного противодействия ДД на защищаемый СлПО. ДД могут быть описаны в пространстве параметров (на практике – метрик), по которым ЛПР объективно судит о состоянии защищаемого СлПО в каждый требуемый момент времени по результатам аудита ИБ.

Результаты измерений результативности средств (мер) обеспечения ИБ следует определять и доводить до сведения заинтересованных сторон (внутренних или внешних), соответственно, требуется механизм контроля передачи информации на разные интерфейсы. Базовая модель такой системы контроля представлена на рисунке 2. В диссертации представлены различные категории метрик ИБ, унифицированных к типу защищаемых активов (*asset management*) организаций. Для разделения метрик ИБ на категории предлагается использовать следующие критерии:

- Простые метрики могут быть получены напрямую специалистами службы ИБ через технические средства или по результатам анализа мероприятия ИБ (например, при анализе «логов» систем SIEM, DLP, IPD/IDS, WAF, NGFW и пр.);
- Сложные метрики вычисляются на основании простых метрик и требуют привлечения дополнительно специалистов иных служб (например, оценка стоимости защищаемых активов требует данных от финансово-экономических подразделений);
- Комплексные метрики вычисляются на основании сложных метрик и требуют привлечения высшего руководства, ответственного за безопасное выполнение бизнес-процессов. Кроме того, учитывая прямое отношение комплексных метрик к защищаемым активам (в том числе, оценку ущерба), для анализа и расчета данной категории метрик ИБ должен допускаться ограниченный ряд руководителей.

Для отбора наилучшей, в смысле решения поставленной задачи, совокупности метрик ИБ, предлагается применять новые расширенные положения теории «элитных групп» (предложена проф. А.Н. Ефимовым). В базовом варианте имеется совокупность элементов счетного множества $\mathbf{Y}$ (в новом варианте предложено специфицировать множество метрик ИБ). Свойство каждого элемента выражается определенной критериальной величиной $\mathbf{y_i}$, находящейся в диапазоне $\mathbf{0 \le y \le 1}$, и известно, что чем больше значение достигает $\mathbf{y_i}$, тем лучше. В частности, это требование точно соответствует задаче оценки конкретного атрибута – чем лучше его «абсолютная» оценка, тем лучше, и тем выше общая оценка измерения результативности ИСМ в интегрированной СУ.

Известна цель: $\mathbf{0 \le \alpha \le 1}$ и известно требование – достижение цели с условием, чтобы некоторый показатель качества был не ниже заданной величины $\mathbf{\alpha \le 1}$. Задача формируется как отбор из исходного множества $\mathbf{Y}$ заданного количества элементов для достижения поставленной цели с установленным ЛПР показателем качества. В множестве $\mathbf{Y}$ могут присутствовать элементы $\mathbf{y_i}$, для которых выполняется $\mathbf{y_i \ge \alpha}$ (называемые «элитные» элементы) и $\mathbf{y_i \le \alpha}$ (называемые «сорные» элементы). В новом методе предлагается элементы $\mathbf{y_i}$ выбирать случайно, что является, во-первых, требованием стандартов ISO серии 19011 и 17021 по формированию «выборки аудита» (*audit sample*) и, во-вторых, должно исключить на практике случаи «подгонки» множества элементов $\mathbf{Y}$ под заранее заданный результат $\mathbf{\alpha}$. Для этого в базовую формулу внесен новый важный компонент $\mathbf{\gamma}$ – вероятность включения в «элитную» группу ранее не использованных элементов $\mathbf{y_i}$. Таким образом, предложенное

новое распределение качества **Y** в определенной «элитной» группе может характеризоваться новой плотностью распределения:

$$F_{Elite\ New}(y) = \left\{ \gamma \frac{\beta}{F(\alpha)}\ f(y): y < \alpha; (1-\gamma) \frac{1-\beta}{1-F(\alpha)}\ f(y): y \geq \alpha \right\} \qquad (4)$$

где:

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

α – показатель качества;

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

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

f (y) – соответствующая плотность распределения.

Если в силу ряда причин, элементы отобранной «элитной» группы (4) могут выбывать, но требуется сохранить «представительность» данной группы (например, для целей измерения в процессе аудита ИБ определенных процессов ИБ), то необходимо решать задачу повторного выбора элементов из оставшейся базовой совокупности **Y**. Алгоритм применения «элитных групп» для целей измерений результативности ИСМ показан на рисунке 4.

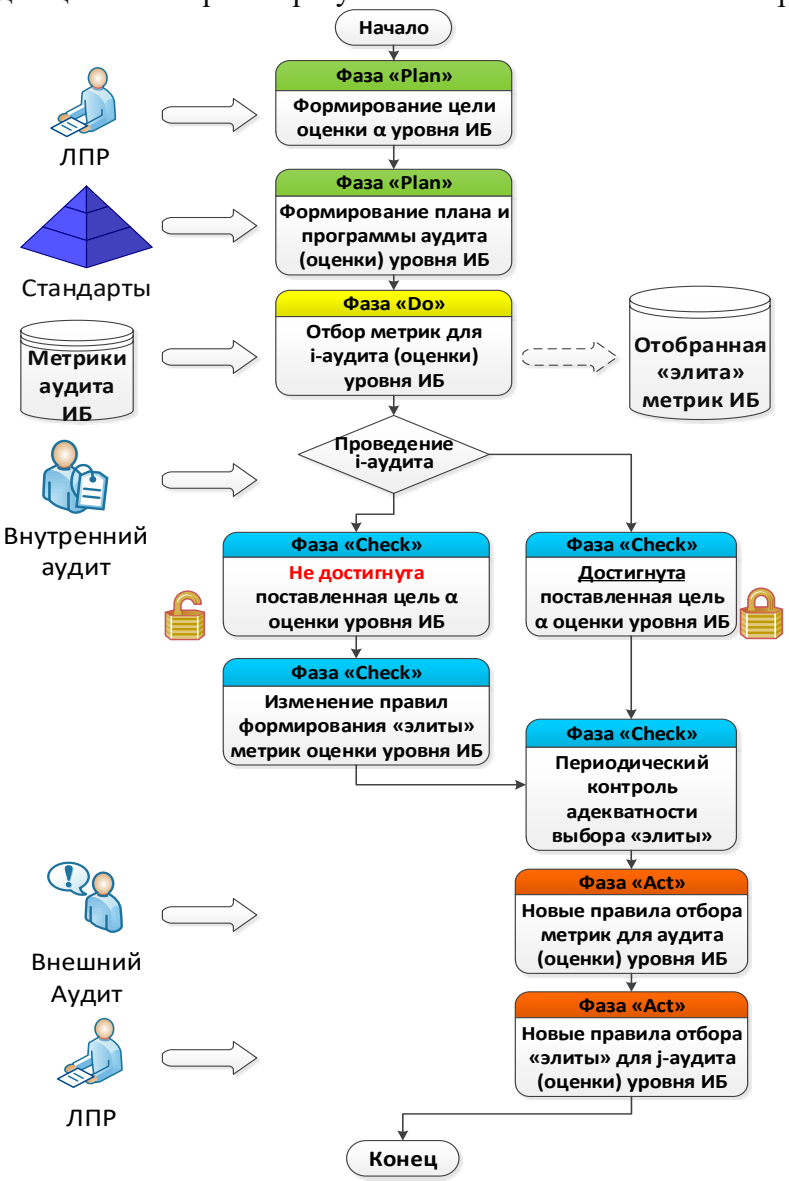

Рисунок 4 – Алгоритм применения «элитных групп» для ИСМ

Для дальнейшего развития базовой теории «элитных групп» и применения в целях управления аудитом ИБ в представленном алгоритме введены новые функции:

- необходимо ориентироваться, прежде всего, на долю «элитных» элементов, «удовлетворяющих» требованию $\mathbf{y_i \geq \alpha}$, но ранее не отобранных для аудита в течение одного полного замкнутого цикла программы аудита;
- необходимо отслеживать характер изменения «качества» каждого отобранного «элитного» элемента, а 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 метрик ИБ по итогам, например, определенного внутреннего аудита в ИСМ как компоненты интегрированной СУ.

Оценку результативности средства (меры) обеспечения ИБ, выбранных на основании дополненной теории «элитных групп» в рамках программы измерений, следует непосредственно связывать с функционированием «конкретной реализации» ИСМ. Практическая ценность нового метода «мгновенных аудитов» основана на известных фактах, что 96% успешных взломов можно было избежать, если бы был внедрен ряд мер ИБ, т.к. более 75% атак использовали уже известные уязвимости, которые могли бы быть «закрыты» регулярными «патчами» безопасности. При этом отмечается, что 85% произошедших вторжений были обнаружены спустя месяцы (среднее время обнаружения – 5 мес.).

В этой ситуации предлагается применять не только технический подход (СрЗИ), но предложить новый метод «мгновенных аудитов» ИБ. Методической базой нового метода «мгновенных аудитов» является семейство стандартов ISO/IEC (ГОСТ Р ИСО/МЭК) серии 27001 и 19011, дополненное множеством метрик ИБ для формирования количественной оценки. В частности, рекомендуется применять дополнительно метрики обеспечения ИБ из стандартов ISO/IEC (ГОСТ Р ИСО/МЭК) серии 20000 (для управления ИТ-услугами, например – SLA) и серии 22301 (для управления непрерывностью бизнеса, например – RTO, RPO). Для успешного решения отраслевых задач ИБ необходимо принять во внимание дополнительно и отраслевые стандарты, в частности, IATA (ISAGO). Управление «частотностью аудита» позволяет в интегрированной СУ более оперативно контролировать динамику процесса изменений уровня обеспечения ИБ («динамическая перестройка» критериев аудита). Важным преимуществом предложенного метода является акцент именно на получение численных оценок, а не общего «соответствия» или «несоответствия».

Метод «мгновенных аудитов» предполагает реализацию принципа выполнения аудита ИБ с частотой, зависящей от предыдущего состояния «слева» уровня обеспечения ИБ объекта. Наибольшее значение для целей аудита ИБ играет метод опережающего управления, как указано в классическом примере Н. Винера. Кроме того, для эффективного обеспечения ИБ необходимо уменьшить период выявления, анализа и «закрытия» несоответствий, и успешная реализация этого процесса представляется значительно быстрее, чем выбор, закупка, доставка, установка и настройка новых и новых СрЗИ. При этом, во-первых, выполняются все требования стандартов ISO по обеспечения ИБ, во-вторых, дополнительно выполняются бизнес-требования ЛПР (не желающих ждать целый год для приведения оценки ИБ к требуемому уровню) и, в-третьих, решаются вопросы оперативного противодействия современным УБИ (время «замыкания» PDCA-цикла стремится к нулю).

Для формирования оценки уровня обеспечения ИБ по результатам аудита в течении всего ЖЦ интегрированной СУ для СлПО предлагается применять предел функции слева. Это позволяет оценить требуемый интервал, на котором допустимо (по времени) могут быть выполнены необходимые изменения в интегрированной СУ, и, следовательно, обосновать необходимость и целесообразность проведение нового аудита ИБ. Заметим, что близкие рекомендации даны в стандарте ISO 22301 (например, требуется обеспечить RTO << MTPD). Рассмотрим действительную функцию переменных:

$$\boldsymbol{y = f\,(x_1, x_2, x_3, \ldots, x_n),}$$

где, например, первые 4 переменные описывают атрибуты аудита ИБ:

- $\boldsymbol{x_1}$ – частота проведения аудита, определяемая как отношение количества всех проведенных аудитов в ИСМ к наблюдаемому периоду;

- x_2 – объем программы аудита, определяемый как отношение количества охваченных процессов к общему количеству процессов ИСМ;
- x_3 – метрика достижения уровня обеспечения ИБ, определяемая как мера результативности R_{base} / R_{Max};
- x_4 – метрика выполнения корректирующих действий по итогам выполненных аудитов ИБ, запланированных на наблюдаемый период.

Для одной изменяемой переменной x_1 (например, частоты проведения аудита ИБ) оценим практическое значение частной производной (при неизменности иных переменных), получаем оценку скорости роста уровня обеспечения ИБ:

$$\frac{\partial}{\partial x_1} = \frac{\Delta R_k}{\Delta t k}.$$

Реализация метода «мгновенных аудитов» для оценки роста уровня обеспечения ИБ ценных для бизнеса активов с требуемой частотой может быть продемонстрирована как сокращение периода (увеличение частоты) проведения аудита ИБ (см. рисунок 5).

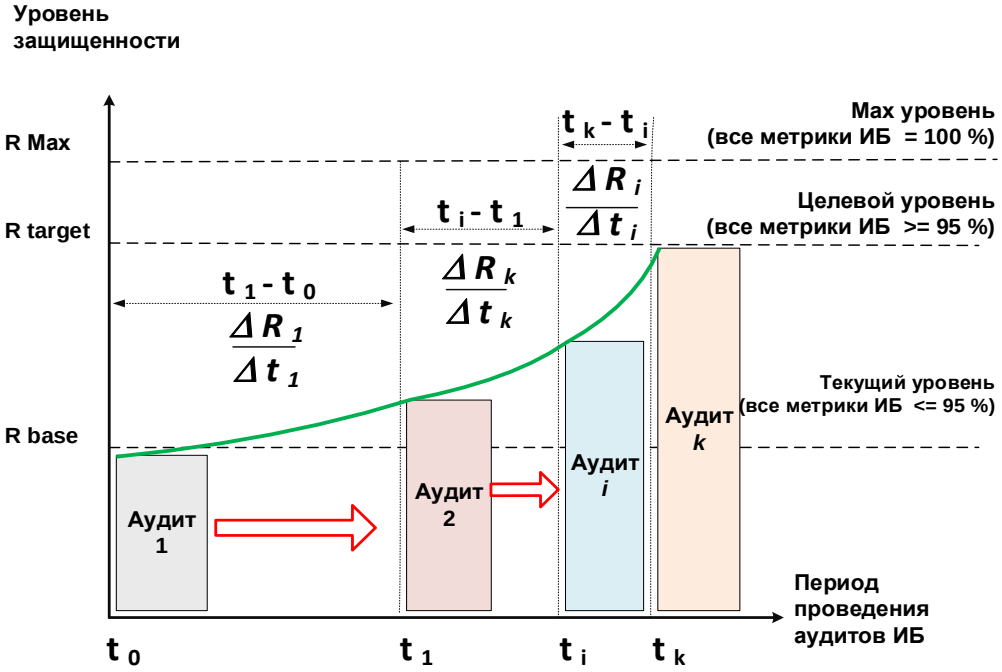

Рисунок 5 – Пример увеличения скорости роста уровня обеспечения ИБ

В указанном примере для одной переменной x_1 продемонстрировано увеличение скорости роста уровня обеспечения ИБ $\frac{\Delta R_k}{\Delta t k}$ при известных переменных процесса аудита ИБ. Отметим, что оперативные данные, формируемые при реализации метода «мгновенных аудитов», обеспечивают оценку θ_1 и θ_1 из (3), предоставляя ЛПР опосредованно и данные для определения A_N и U_N из (3).

В четвертой главе представлены материалы исследований, относящиеся к третьему защищаемому положению. Представляет интерес создание нового метода для получения достоверных статистических данных о динамике применения международных стандартов ISO за длительный интервал наблюдений, что позволит ЛПР принимать рациональные решения еще в начале ЖЦ интегрированной СУ для СлПО. Для выбора факторов необходимо оперировать достоверной информацией, которая может быть проверена независимыми исследователями. В диссертации ставится задача исследования динамики сертификации различных организаций (по кодам отраслей EAC) по наиболее применимым международным стандартам ISO. Предложено формировать данные о реализации случайного процесса на базе статистики ISO за семилетний период наблюдения. В исследовании рассматриваются реализации случайного процесса как множество дискретных сечений, а сам процесс полагаем процессом с дискретным временем и дискретным состоянием. Для рассматриваемого случайного процесса применим одномерный закон распределения:

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

В работах Е.С. Вентцель показано, что более точные и исчерпывающие характеристики дает (в том числе, для инженерных приложений) двухмерный закон распределения, функция четырех аргументов. Для оценки независимости (или зависимости) двух случайных величин применяется известная формула (5):

$$Corr(\eta,\gamma) = \frac{Cov(\eta,\gamma)}{\sigma(\eta) \bullet \sigma(\gamma)} \qquad (5)$$

где:

σ – стандартное (среднее квадратическое) отклонение

Cov – ковариация между двумя дискретными случайными величинами.

Ковариация Cov из (5) определяется по известной формуле (6):

$$Cov(\eta,\gamma) = \sum_{i=1}^{\infty}\sum_{j=1}^{\infty} Pij(Xi - E(\eta)) \bullet (Yj - E(\gamma)) \qquad (6)$$

где:

E – математическое ожидание.

Обработанные данные по динамике сертификации ISO для аналитических разрезов (в мире, в Европе и в РФ) по данным за 7 лет представлены в таблице 2. На основании формулы (5) определяется корреляция для различных выборок (по стандартам ISO серии 9001, 14001 и 27001 соответственно) по всему установленному периоду наблюдений, для необходимости формирования «целевой» аналитики вводится новая сущность «лидер ранга».

Таблица 2 – Динамика сертификации по выбранным стандартам ISO

Стандарт	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
В мире							
ISO 9001	–	-6,19%	0,74%	0,55%	1,31%	-0,21%	6,94%
ISO 14001	–	1,46%	7,17%	4,99%	8,35%	7,67%	8,34%
ISO 27001	–	11,06%	13,05%	10,11%	6,48%	19,70%	20,90%
ISO 50001	–		387,15%	115,83%	40,18%	77,16%	68,68%
В Европе							
ISO 9001	–	-13,33%	2,26%	-2,33%	-1,13%	-3,12%	2,72%
ISO 14001	–	-1,89%	10,51%	3,54%	2,86%	0,57%	0,70%
ISO 27001	–	10,19%	20,61%	24,66%	8,94%	20,58%	19,97%
ISO 50001	–		427,20%	108,08%	38,39%	83,71%	68,46%
В РФ							
ISO 9001	–	-78,63%	-6,16%	-5,80%	-4,68%	-18,99%	-44,04%
ISO 14001	–	-44,03%	-0,27%	16,70%	-2,67%	-6,62%	-10,29%
ISO 27001	–	-56,94%	-12,90%	77,78%	-10,42%	27,91%	12,73%
ISO 50001	–		700,00%	212,50%	224,00%	45,68%	47,46%

Результаты определения коэффициентов корреляции по «лидерам» различных рангов представлены в таблице 3.

Таблица 3 – Определение коэффициентов корреляции по рангам

Код ЕАС	**Ранг**	**Коэффициенты корреляции**		
		9001 – 14001	**14001 – 27001**	**9001 – 27001**
19	1	-0,115	-0,878	0,056
28	1	-0,769	-0,121	0,477
17	2	-0,270	0,338	0,633
29	2	-0,422	0,091	0,087
18	3	-0,261	0,058	0,888
14	3	-0,236	0,672	0,301
33	3	-0,318	-0,389	0,664
35	3	0,580	0,329	0,552
31	3	0,608	0,377	0,720

На основании применения нового метода исследования динамики сертификации по итогам анализа данных из таблицы 3 можем определить:

1. Для «лидеров 3-го ранга» только для пары 9001-27001 наблюдается положительная корреляция с низким (для отраслей EAC 14 и 35), средним (для отраслей EAC 31 и 35) и высоким (для отрасли EAC 18) признаком по шкале Чеддока соответственно. Остальные пары сравнения дают различную по направленности корреляцию.
2. Для «лидеров 2-го ранга» для пары 9001-27001 наблюдается положительная корреляция с низким (для отрасли EAC 29) и средним (для отрасли EAC 17) признаком по шкале Чеддока соответственно. Для пары 14001-27001 наблюдается положительная корреляция с низким (для всех отраслей EAC) признаком по шкале Чеддока соответственно. Для пары 9001-14001 наблюдается различная по направленности корреляция.
3. Для «лидеров 1-го ранга» только для пары 9001-27001 наблюдается положительная корреляция с низким (для отрасли EAC 19) и средним (для отрасли EAC 28) признаком по шкале Чеддока соответственно. Остальные пары сравнения дают различную по направленности корреляцию.
4. Для пары ISO 9001 – 27001 для всех «лидеров» в целом показана без исключения только положительная корреляция и важно, что успех сертификации по указанной паре стандартов мало зависит от специфики конкретных отраслей (т.е. объективно доказано, что требованиям ИБ привержены не только лишь «специфические» ИТ-компании).

Отметим, что оперативные данные, формируемые при реализации метода исследования динамики сертификации по стандартам ISO обеспечивают оценку $\boldsymbol{\theta_{A0}}$, $\boldsymbol{\theta_4}$ и $\boldsymbol{\theta_5}$ из (3), предоставляя ЛПР опосредованно и данные для определения $\mathbf{A_N}$ и $\mathbf{U_N}$ из (3).

В пятой главе представлены материалы исследований вопросов оптимизации системы внутреннего аудита, относящиеся к четвертому защищаемому положению. В диссертации подробно рассмотрены существующие «классические» системы аудита (в частности ISO, ISAGO, СТО БР ИББС, СТО Газпром СОИБ). С учетом выполненного анализа предложен новый метод оптимизации аудита ИБ, основанный на следующих основных принципах:

1. Вводится понятие интегральной оценки (ИО) ИБ для ОЗ, которая включает определенный групповой показатель оценки всех вынесенных на аудит ИБ процессов – R_{ISMS}. Этот групповой показатель определяется с помощью частных показателей – R_{PR}, с учетом их весовых коэффициентов в зависимости от важности процесса в организации ИБ для конкретного ОЗ в интегрированной СУ.
2. После проведения начального аудита ИБ по каждому проверяемому процессу количественно оценивается его степень соответствия заданным критериям аудита (применимым требованиям), а также его влияние на ИО ИБ конкретного ОЗ.
3. Последующие аудиты ИБ проводятся по новому методу, использующему гибкий подход: наиболее детально подвергаются проверке те процессы, по которым на предыдущем аудите выявлены существенные несоответствия (в нотации ISO 17021 – *major*), и которые имеют наибольший приоритет в ИО ИБ для конкретного ОЗ.
4. Частота и детальность, которая должна быть дифференцирована для различных проверяемых процессов, также связывается с ИО. Например, определенные группы процессов, имеющие приоритетное значение для ЛПР, подвергаются аудиту чаще.
5. Объем проверки и частота аудита каждый раз определяется в зависимости от приближения функции ИО ИБ для ОЗ к установленному целевому показателю – R_{target} ($\lim R_{target} \rightarrow 1$) для оценки уровня обеспечения ИБ каждого конкретного ОЗ.

Дополнительно отметим важность внедрения нового стандарта по управлению активами – ISO 55000, т.к. многие активы (в «классическом» понимании ISO серии 27001 – *“asset”)* не включены в управление (процедуры СТО Газпром СОИБ не оперируют такими активами, как «персонал», «здания» и пр.). В максимально удачном случае аудиты ИБ должны «доказать», что выбрано оптимальное для установленных требований ЛПР множество стандартов (см. Главу 4 диссертации), и аудит ИБ выполняется результативно.

Также крайне ценно обеспечить для ЛПР (как заказчику любого аудита, *auditee*) получение нового «качества» интегрированной СУ для СлПО – эмерджентности, как свойства внутренней целостности (устойчивости, безопасности, управляемости и пр.), как «добавленной стоимости» аудита.

Для оценки степени соответствия подсистемы обеспечения ИБ в составе ИСМ интегрированной СУ установленным требованиям в новом предложенном методе используются универсальные частные и групповые показатели ИБ, что снимает ряд противоречий. Например, для целей проведения аудита ИСМ в аспекте обеспечения ИБ предлагается применять показатель результативности R_{ISMS}, вычисляемый в каждом цикле k-го аудита по новой аддитивной формуле с учетом весовых коэффициентов – **α** и показателя результативности каждого конкретного процесса ИБ – $R_{PR\,i}$:

$$R_{ISMS} = \varphi \sum_{i=1}^{n} \alpha_i * R_{PR\,i} \qquad (7)$$

где φ – степень охвата, определяемая как отношение r – количества процессов, оцениваемых в каждом цикле k-го аудита к n – общему количеству идентифицированных процессов в ИСМ:

$$\varphi = \frac{r}{n}$$

при этом:

$$\sum_{i=1}^{n} \alpha_i = 1 \qquad (8)$$

Показатель результативности каждого конкретного процесса ИБ – $R_{PR\,i}$, в свою очередь, вычисляется по новой аддитивной формуле с учетом весовых коэффициентов – **β** и показателей – метрик ИБ для каждого конкретного процесса ИБ – R_{KPI}:

$$R_{PR\,i} = \mu \sum_{j=1}^{m} \beta_j * K_{KPI\,j} \qquad (9)$$

Где μ – степень достоверности оценки результативности каждого конкретного процесса ИБ $R_{PR\,i}$, оцениваемая в зависимости от вида аудита данного процесса, например:

$$\mu = \begin{cases} 0{,}6 - \text{для аудита } 1 - \text{й стороной} \\ 0{,}7 - \text{ для аудита } 2 - \text{й стороной} \\ 0{,}9 - \text{для аудита } 3 - \text{й стороной} \end{cases}$$

при этом:

$$\sum_{j=1}^{m} \beta_j = 1 \qquad (10)$$

Сумма весовых коэффициентов частных показателей ИБ, используемых при вычислении группового показателя ИБ, должна быть равной 1, что обеспечивает нормирование всех показателей в аддитивных формулах (8) и (10). Показатель результативности R_{ISMS} должен быть в пределе равен 1. В процессе аудита ИСМ постоянное измерение «невязки» текущего для k-го аудита R_{ISMS} измеряется как рассогласование с целевым показателем $R_{ISMStar}$, и крайне важно обеспечить его минимум.

Следовательно, задача оптимизации может быть отнесена к типу задач статической оптимизации для процессов управления, протекающих в установившемся режиме. Необходимо реализовать оптимизационную модель для процесса аудита ИСМ в условиях детерминированных ограничений и задачи многомерной дискретной условной оптимизации:

$$F\,(y) \rightarrow max$$

где:

$F\,(y) \in R^m$,

$f\ (y)\ \in\ R^1$

$f\ (y)$ – целевая функция $\boldsymbol{m}$-мерного векторного аргумента $\boldsymbol{y}$:

$y = (y_1, y_2, y_3, \dots y_m)$

Область допустимых значений: $y\ \in\ D\ \subset R^m$.

Переменные $\boldsymbol{m}$-мерного векторного аргумента $\boldsymbol{y}$ могут быть для значимого территориально-распределенного СлПО с внедренной ИСМ как компоненты интегрированной СУ, например, следующими:

- T– длительность аудита ИБ (час.);
- S– плановая стоимость аудита ИБ (руб.);
- O – перечень посещаемых объектов в ходе аудита ИБ;
- V– объем аудита ИБ (количество подразделений на объекте);
- F– перечень функциональных вопросов (чек-лист) в ходе аудита ИБ;
- R_{ISMS} – оценка результативности аудита ИБ.

Рассмотрим пример решения варианта оптимизационной задачи с установленными ограничениями (II-го рода, в виде неравенства):

$$\left.\begin{gathered} R_{ISMS}\ (S,T,F,V,O) \to max \\ S < 1000 \\ T < 8 \\ F < 200 \\ V < 10 \\ O < 10 \\ R_{ISMS}\ < 1 \\ S > 0, T > 0, F > 0, V > 0, O > 0, R_{ISMS}\ > 0 \end{gathered}\right\}$$

Данная постановка оптимизационной задачи в текстовой нотации формулируется как выбор параметров процесса аудита ИСМ, при котором достигается максимальная оценка результативности (R_{ISMS}) аудита при заданных ограничениях плановой стоимости аудита ИБ (S), длительности аудита ИБ (T), количества посещаемых объектов (O), проверяемых подразделений (V) и перечня функциональных вопросов (F). Некоторые примеры решения оптимизационной задачи приведены в диссертации. По итогам оценки всех аудитов ИБ, заполняется следующая матрица – с учетом процессов ИБ – PR_1, аудита ИБ – k-аудита и метрик ИБ – $KPI_{11.}$ (таблица 4).

Таблица 4 – Схема размещения результатов аудита процессов ИБ

Аудит / **Процесс**	**1**	**2**	**…**	**k**
PR_1	KPI_{11}	KPI_{12}		KPI_{1k}
PR_2	KPI_{21}	KPI_{22}		KPI_{2k}
…	…	…	…	…
PR_i	KPI_{i1}	KPI_{i2}		KPI_{ik}

На основании известных национальных стандартов (в частности, ISO 19011, 27006), отраслевых стандартов (СТО ИББС БР и пр.) предложен новый метод многошаговой оптимизации процесса аудита ИСМ для СлПО, который позволяет оптимизировать систему распределения ресурсов и оперативного доведения результатов аудита ИСМ как компоненты интегрированной СУ до ЛПР. Предложенный метод заключается в научно обоснованном и целенаправленном оперативном функционировании подсистемы ИБ в составе ИСМ, отличающийся от существующих методов циклической непрерывной количественной оценкой результативности ИСМ на основе оптимальной системы численных показателей (метрик) ИБ. Предложенный метод состоит из 2-х циклов оптимизации программы аудита ИСМ, отличающихся следующими новациями:

1. Базовым оптимизационным циклом, который характеризует эффективное выполнение аудита ИСМ в терминах оценки результативности для каждого PRi – процесса ИБ и каждой KPIj – метрики ИБ, а также определяет циклы оптимизации ресурсов в

программе аудита: размера аудиторской выборки, количества привлекаемых аудиторов (технических экспертов) и пр.

2. 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 R_{ISMS} в k-м аудите и (k+1)-м аудите для постоянной и оперативной оптимизации всей программы аудита.

Рассмотрим базовый оптимизационный цикл программы аудита ИСМ, построенный с учетом формальных требований стандартов ISO, ISAGO, СТО Газпром СОИБ и СТО БР ИББС, и дополненных новыми элементами (рисунок 6).

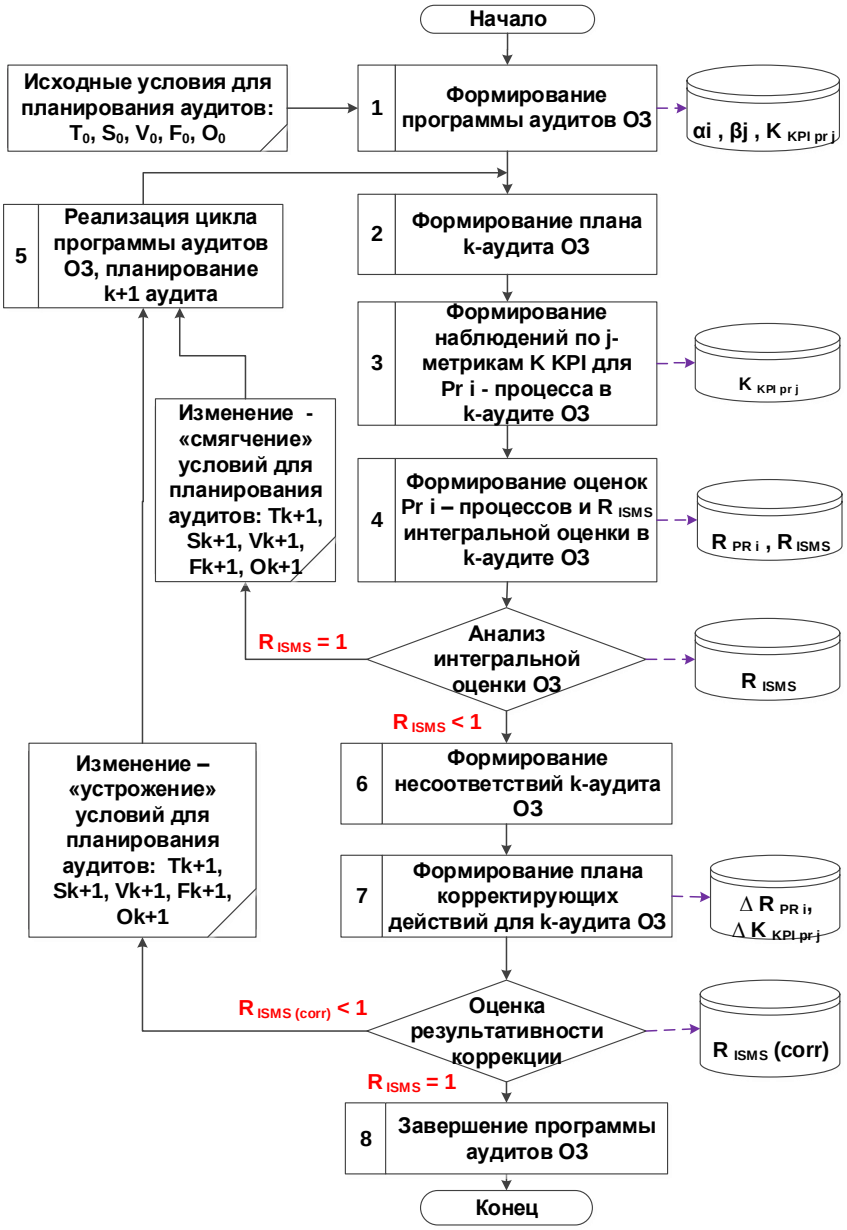

Рисунок 6 – Базовый оптимизационный цикл программы аудита ИСМ

Описание базового оптимизационного цикла программы аудита ИСМ представлено в диссертации (Глава 5). Рассмотрим далее детализацию базового оптимизационного цикла программы аудита ИСМ с учетом формальных требований стандартов по аудиту (ISO, ISAGO, СТО БР ИББС и пр.), дополненных новыми системными элементами (рисунок 7):

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

Описание быстрого блока оценки результативности программы аудита ИСМ представлено в диссертации (Глава 5). Отметим, что оперативные данные, формируемые при реализации методов оптимизации программы аудита ИСМ, обеспечивают оценку θ_{A0}, θ_2, θ_4 и θ_5 из (3), предоставляя ЛПР опосредованно и данные для определения A_N и U_N из (3).

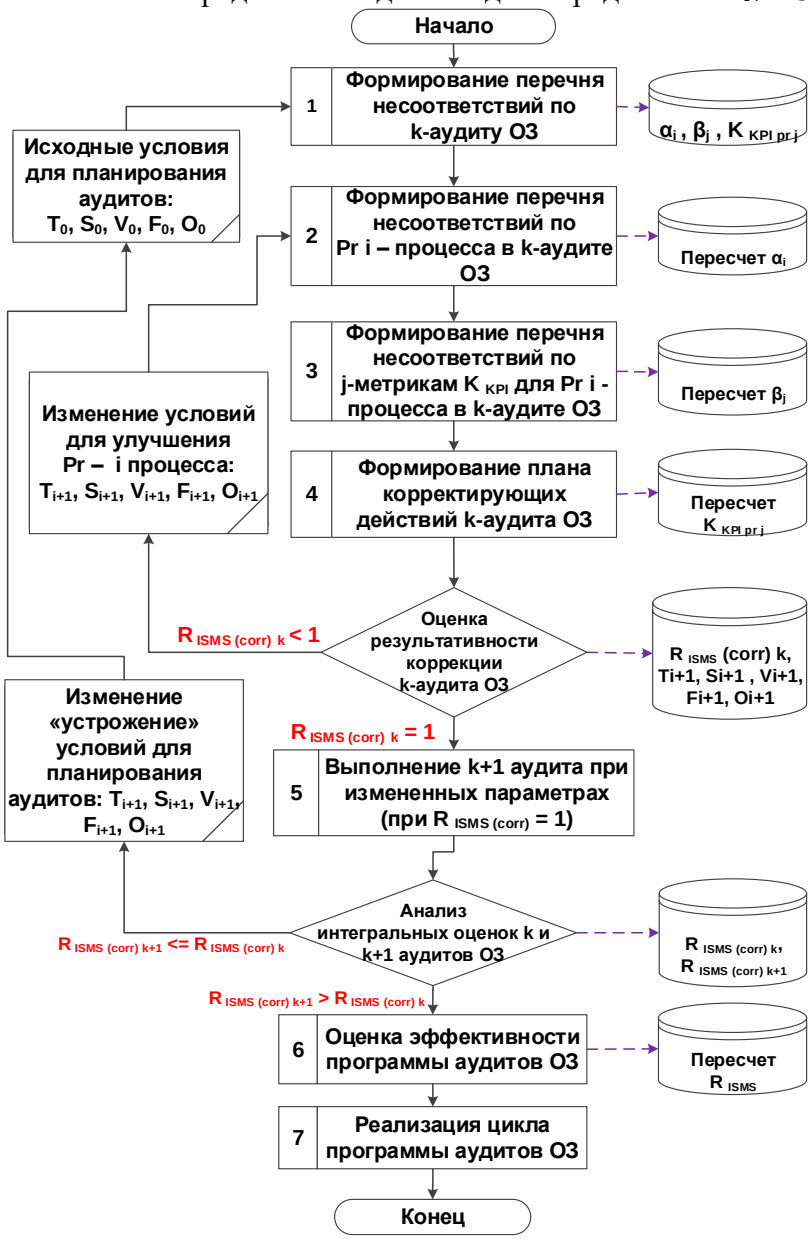

Рисунок 7 – Детализация базового оптимизационного цикла программы аудита ИСМ

Представленные выше теоретические и научно-практические положения нуждаются в оценке практического применения с целью подтверждения корректности предположений и возможности практического использования моделей и методов аудита ИСМ как компоненты интегрированной СУ для СлПО и последующего анализа результатов апробации. **Этому посвящена 6 глава**. В качестве инструмента практической апробации предлагается метод имитационного моделирования на основе предложенной модели ИСМ для АК (подробнее рассматривается в диссертации). Особенностями АК являются приоритет требований авиационной безопасности (как показал ряд авиационных происшествий: в 2014 г. в аэропорту «Внуково», в 2015 г. в аэропорту Казани, в 2016 г. в аэропорту Брюсселя и Киева, в 2018 г. в аэропорту Хитроу), сохранности воздушных судов и груза. Для обеспечения функционирования АК применяются современные интегрированные СУ, в состав которых входят СМ, соответствующие международным стандартам (в т.ч. ISAGO, ISO). Управление и оптимизация деятельности АК может быть выполнено на основе полученных оценок

(метрик) в ИСМ, как компоненты интегрированной СУ. Для этих целей необходимо, во-первых, проектировать ИСМ на базе современных риск-ориентированных стандартов, во-вторых, сформировать требования к процессам АК в измеримых метриках, в-третьих, обеспечить аудит в АК. Отметим, что в АК применимы требования к аудиту всех типов (1-й, 2-й и 3-й стороной).

Выбор именно данного объекта АК для моделирования обусловлен:

- длительным непрерывным периодом наблюдения за данным типом объекта – 4 года (с 2012 по 2015 гг. включительно);
- независимым моделированием для увеличения объективности одновременно для двух похожих объектов исследования (единого отраслевого назначения) – АК в Алматы (код ИКАО – ALA) и АК в Астане (код ИКАО – TSE);
- строгим соблюдением непредвзятости (*impartiality*) при проведении аудита, сформированы полностью независимые группы для проведения аудита ИСМ;
- обсуждением результатов моделирования после завершения полностью принятого 3-х летнего цикла аудита и получения раздельных объективных свидетельств.

Численная оценка результативности по представленной модели ИСМ соответствует численной оценке уровня обеспечения безопасности (см. формулы (7) – (10)). Приведем примеры объектов измерений в различных СМ:

- результативность реализованных средств (мер) обеспечения ИБ;
- состояние активов, защищенных средствами (мерами) обеспечения ИБ;
- степень удовлетворения заинтересованных сторон (потребителей).

Для целей обеспечения комплексной безопасности АК могут использоваться различные источники данных, например:

- результаты анализа риска и оценки риска;
- отчеты о внутренних и / или внешних аудитах;
- сообщения об инцидентах АК.

Для выполнения имитационного моделирования применяется программная среда MPriority версии 1.0 (авторы: Абакаров А.Ш., Сушков Ю.А.). Данная система содержит диалоговые средства, позволяющие получать полную информацию о проведенных попарных сравнениях и оперативно устранять возможные несогласованности в матрицах попарных сравнений. Применение среды моделирования MPriority учитывает предыдущий опыт и основано на предложенном автором в 2012 г. методе оценки (аудита) СМИБ на основе модифицированного МАИ. Для выполнения имитационного моделирования в среде MPriority приняты следующие исходные данные (подробно изложено в диссертации):

1. Объект: модель аудита ИСМ для СлПО – АК.
2. Количество уровней модели (всего – 5):
   - уровень цели,
   - уровень функциональных подсистем (всего – 4),
   - уровень типов аудита ИСМ (всего – 3),
   - уровень ключевых процессов ИБ (всего – 6),
   - уровень альтернатив (всего – 5).
3. Формулы расчета результативности ИСМ ((7) – (10)).

Требуется определить результативность ИСМ по представленной модели, принимая во внимание текущие параметры:

1. Цель определена как: оценка результативности ИСМ.

   Общая структура модели ИСМ для СлПО АК показана на рисунке 8.

   Всего в представленной модели отражены 4 функциональные подсистемы (СМ), 4 уровня иерархии и 5 возможных альтернатив – стандартов ISO и ISAGO (IATA).
2. Предположим, выполнены все типы аудита:
   - Аудиты 1-й стороной (в объеме 100%),
   - Аудиты 2-й стороной (в объеме 30%),

- Аудиты 3-й стороной (в объеме 100%).

Предположим, результативность по каждому типу аудита составляет, соответственно: 0,9; 0,8 и 1 (как аргументы согласно формулам (7) – (10)). Весовые коэффициенты (**β**) для данного уровня иерархии определяются по методу МАИ в системе MPriority.

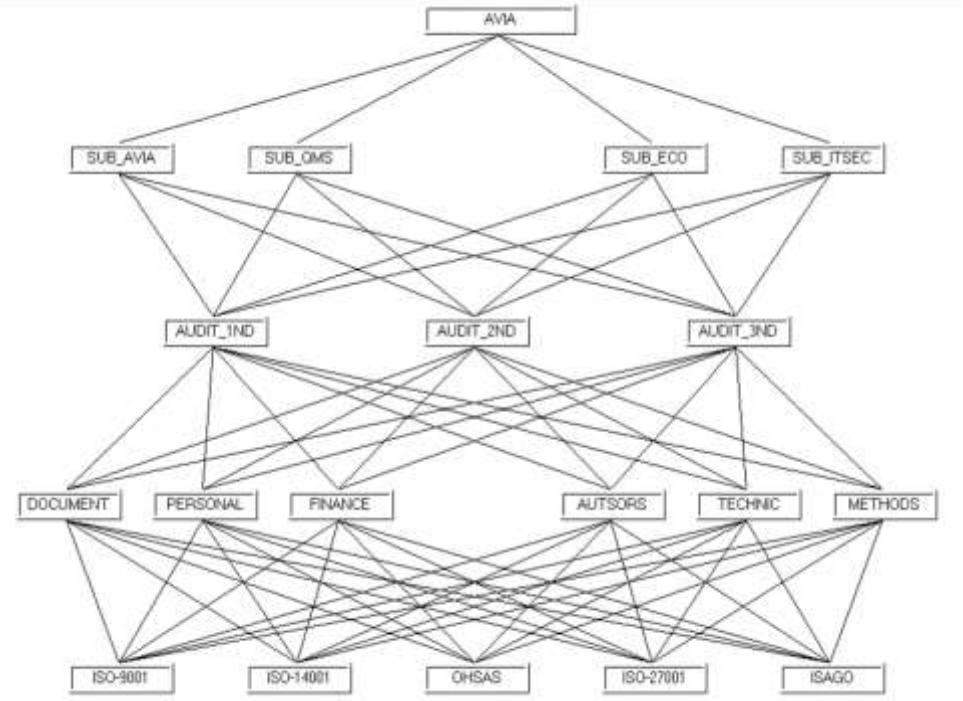

Рисунок 8 – Общая структура модели ИСМ для СлПО АК

3. Предположим, выявлены несоответствия по всем функциональным подсистемам:
   - По ***Sub_Avia*** *(все типы аудита);*
   - По ***Sub_QMS*** *(аудиты 1-й и 3-й стороной);*
   - По ***Sub_ECO*** *(аудиты 1-й и 3-й стороной);*
   - По ***Sub_ITSec*** *(аудиты 1-й и 3-й стороной).*
4. Предположим, выявлены несоответствия для каждого типа аудита по каждой из функциональных подсистем соответственно:
   - По $A_{1\text{-}ND}$ соответственно 0,8; 0,8; 0,75 и 0,7.
   - По $A_{2\text{-}ND}$ соответственно 0,7; 1; 1; и 1.
   - По $A_{3\text{-}ND}$ соответственно 0,8; 0,6; 0,7 и 0,7.
5. Предположим, $\boldsymbol{\mu} = 0{,}9$ по формуле (9).

С учетом полученных по МАИ коэффициентов (**α** и **β**) выполним расчет по формулам (7) – (10) модели аудита ИСМ для АК. В модели учтены все 4 подсистемы (***Sub_Avia, Sub_QMS, Sub_ECO, Sub_ITSec***) и 3 атрибута, агрегированные по различным видам аудита (***1-ND, 2_ND, 3_ND***, соответственно, 1-й, 2-й и 3-й стороной). Расчет результативности подсистем по модели ИСМ для АК представлен по агрегированным 3-м параметрам:

$$P_{ПС\ Sub\_Avia} = \boldsymbol{\mu}\,(\beta_{11} A_{1\text{-}ND} + \beta_{21} A_{2\text{-}ND} + \beta_{31} A_{3\text{-}ND})$$
$$P_{ПС\ Sub\_QMS} = \boldsymbol{\mu}\,(\beta_{12} A_{1\text{-}ND} + \beta_{22} A_{2\text{-}ND} + \beta_{32} A_{3\text{-}ND})$$
$$P_{ПС\ Sub\_ECO} = \boldsymbol{\mu}\,(\beta_{13} A_{1\text{-}ND} + \beta_{23} A_{2\text{-}ND} + \beta_{33} A_{3\text{-}ND})$$
$$P_{ПС\ Sub\_ITSec} = \boldsymbol{\mu}\,(\beta_{14} A_{1\text{-}ND} + \beta_{24} A_{2\text{-}ND} + \beta_{34} A_{3\text{-}ND})$$

и, соответственно:

$$P_{ИСМ} = \boldsymbol{\varphi}\,(\alpha_{Avia} P_{ПС\ Sub\_Avia} + \alpha_{QMS} P_{ПС\ Sub\_QMS} + \alpha_{ECO} P_{ПС\ Sub\_ECO} + \alpha_{ITSec} P_{ПС\ Sub\_ITSec})$$

Получаем по (9):

$P_{ПС\ Sub\_Avia}$ = 0,9 * (0,11 * 0,8 + 0,25 * 0,7 + 0,64 * 0,8) = 0,9 * 0,78 = 0,7.

$P_{ПС\ Sub\_QMS}$ = 0,9 * (0,10 * 0,8 + 0,22 * 1 + 0,68 * 0,6) = 0,9 * 0,71 = 0,66.

$P_{ПС\ Sub\_ECO}$ = 0,9 * (0,14 * 0,75 + 0,28 * 1 + 0,58 * 0,7) = 0,9 * 0,7 = 0,63.

$P_{ПС\ Sub\_ITSec}$ = 0,9 * (0,14 * 0,7 + 0,22 * 1 + 0,64 * 0,7) = 0,9 * 0,77 = 0,69.

Предположим, φ = 0,9 и получаем в итоге по (7):

$$Р_{ИСМ} = 0,51*0,7 + 0,13*0,66 + 0,07*0,63 + 0,29*0,69 = 0,68$$

В диссертации используется следующая шкала зрелости ИСМ (таблица 5):

Таблица 5 – Шкалы зрелости ИСМ

Уровень	Зрелость ИСМ	Основные характеристики ИСМ	Значение $Р_{ИСМ}$
0	Отсутствует	· Реализация отдельных требований	$0,1 \geq Р_{ИСМ} > 0$
1	Определенная	· Реализация всех требований СМ · ИСМ документирована	$0,25 \geq Р_{ИСМ} > 0,1$
2	Управляемая	· ИСМ документирована · Поддерживается цикл PDCA	$0,5 \geq Р_{ИСМ} > 0,25$
3	Установленная	· Реализация всех требований в ИСМ · ИСМ сертифицирована	$0,75 \geq Р_{ИСМ} > 0,5$
4	Предсказуемая	· ИСМ сертифицирована · Управление по целям	$0,8 \geq Р_{ИСМ} > 0,75$
5	Оптимизируемая	· ИСМ прошла 1 цикл сертификации · Определены цели улучшения	$Р_{ИСМ} > 0,8$

По таблице 5 при $Р_{ИСМ}$ = 0,68 уровень зрелости равен 3, степень зрелости ИСМ – «Установленная». В представленном расчете с помощью системы моделирования MPriority получаем оценку приоритетов существующих стандартов (ISO, ISAGO, ГОСТ) для целей обеспечения безопасности СлПО в АК (рисунок 9).

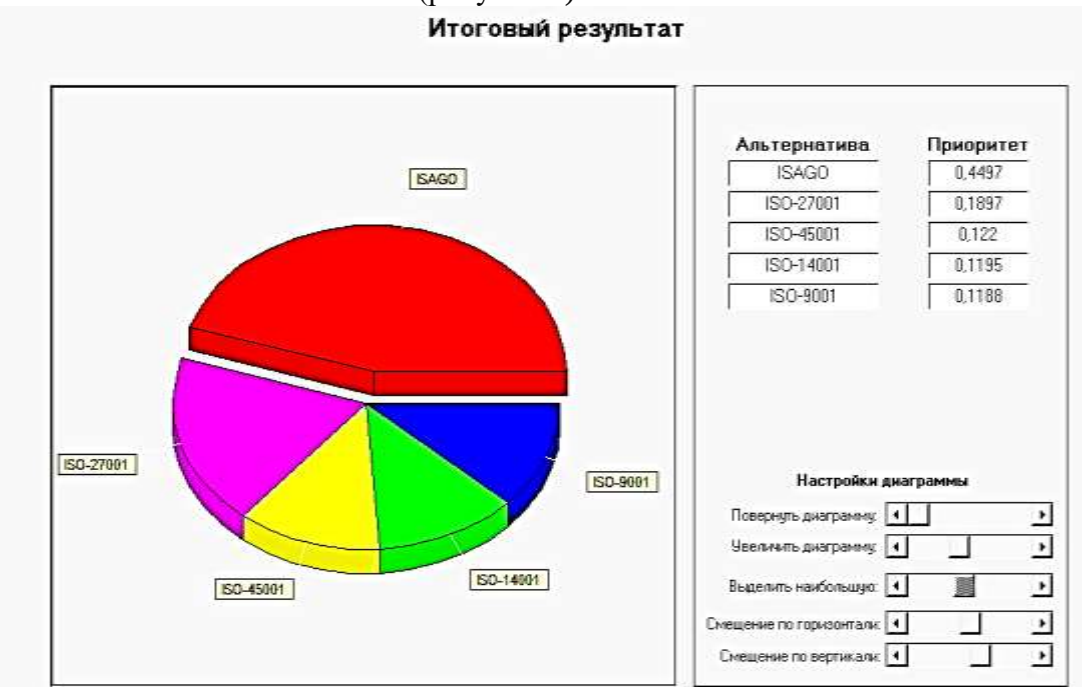

Рисунок 9 – Расчет приоритетов для целей обеспечения безопасности СлПО в АК

В диссертации рассмотрена проблема оценки производительности системы моделирования. Необходимость оценки производительности важна в том случае, если ЛПР не имеет возможности ждать сколь угодно долго результатов реального аудита ИСМ как компоненты интегрированной СУ для СлПО и/или предпочитает выполнить работу с экспертной группой (сессию моделирования). Также может потребоваться одновременно обеспечить для ЛПР оценку нескольких предполагаемых сценарных вариантов построения системы аудита ИСМ (без физического изменения самого СлПО как объекта моделирования). В качестве методики для оценки производительности системы имитационного моделирования предлагается новая модификация методики Apdex. Известные недостатки базовой формулы методики Apdex рассмотрены подробно в

диссертации. Для применения методики Apdex с целью оценки производительности системы имитационного моделирования СлПО внесены новации:

$$I_{Apdex\ New} = \frac{f(Nt) * NT + f(Nq) * NQ}{N} \qquad (11)$$

где:

$I_{ApdexNew}$ *– 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.*

На основании новой формулы (11) в диссертации подробно рассмотрен состав операций для оценки производительности системы имитационного моделирования СлПО на примере АК (объекты: АК Алматы и АК Астаны) и представлено сопоставление оценок.

Примеры реализации полученных научных результатов в практической деятельности для СлПО различной отраслевой принадлежности наглядно демонстрируют достижение цели диссертационного исследования и возможность их применения для повышения уровня «зрелости» ИСМ для обеспечения стабильности функционирования СлПО (см. таблицу 6).

Таблица 6 – Результаты, подтверждающие достижения цели исследования

Предприятие	**Акт внедрения**	**Параметр**	**Значение**
Международный аэропорт Алматы (Казахстан)	Да	Затраты на систему внутренних аудитов ИБ	Снижены на 5%
Международный аэропорт Астаны (Казахстан)	Да	Затраты на систему внутренних аудитов	Снижены на 4%
ИТСК (РФ)	Да	Затраты на систему внутренних аудитов ИБ	Снижены на 2%
АКБ «Рускобанк» (РФ)	Да	Уровень соответствия ИБ требованиям СТО БР ИББС	Достигнут уровень 4
AQS (Азербайджан)	Да	Результативность обучения аудиторов	Повышена на 15%
ГУП «Водоканал Санкт-Петербурга» (РФ)	Да	Результативность обучения аудиторов	Значительно
«Газинформсервис» (РФ)	Да	Длительность выполнения аудитов СОИБ	Снижена на 4 месяца

ЗАКЛЮЧЕНИЕ

В диссертационной работе **решена** крупная важная научно-техническая проблема, заключающаяся в создании теоретических основ формирования перспективных подходов и применения новых методов обеспечения ИБ в интегрированных СУ для СлПО, созданных для снижения длительности и стоимости аудита ИБ, формирования количественной оценки уровня обеспечения ИБ в СлПО, применения наилучшего множества мер (средств) обеспечения ИБ для парирования выявленных рисков в СлПО. Решение данной проблемы имеет научную и практическую ценность для обеспечения безопасности СлПО, в том числе получены научные результаты, составляющие **итоги** диссертационного исследования:

1. Проведено исследование системных требований, предъявляемых к процессам обеспечения ИБ в СлПО и определены закономерности между системными изменениями требований регуляторов, применимыми стандартами (международными, национальными, отраслевыми) и объективными потребностями создания ИСМ как компоненты интегрированной СУ для различных отраслей промышленности;
2. Проведено исследование системных требований, предъявляемых при создании современных ИСМ, предназначенных для защиты ценных активов СлПО, в частности,

нематериальных активов (*goodwill*), с учетом риск-ориентированного подхода при обеспечении ИБ для СлПО;

3. Проведено исследование и анализ с целью создания иерархической структуры численных показателей (метрик) ИБ в процессах обеспечения ИБ, предназначенных для формирования требований к ИСМ как компоненты интегрированной СУ для СлПО;
4. Разработаны 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 как компоненты интегрированной СУ для СлПО согласно применимым требованиям.
5. Разработан метод проведения аудита ИСМ для СлПО, который, 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 аудитом ИБ по частоте и предоставляет ЛПР оценку роста уровня обеспечения ИБ в СлПО как показатель результативности (*effectiveness*) ИСМ и соответствия применимым требованиям.
6. Разработан метод исследования динамики сертификации по международным стандартам ISO для СлПО, основанный на публичных статистических данных ISO, устанавливающий оценку влияния «лидеров» разного ранга и учитывающий приоритеты отраслей в соответствии с международными кодами экономической деятельности ЕАС. Новый метод позволяет оценить «входные» динамические изменения потребностей бизнеса, выраженные в изменении предпочтений ЛПР по составу внедряемых СМ, прошедших внешний (независимый) аудит ИБ в ИСМ как компоненты интегрированной СУ для СлПО и формировать прогнозные оценки.
7. Разработан метод многошаговой оптимизации процесса аудита ИБ в ИСМ для СлПО, который, в отличие от известных стандартов ISO, обеспечивает координацию, распределение ресурсов и оперативное информирование ЛПР об оценке результативности аудита ИСМ. Предложенный метод обеспечивает научно обоснованное и целенаправленное функционирование ИСМ, и отличается от существующих методов циклической непрерывной оценкой ИБ.
8. Выполнено исследование практической применимости предложенных моделей и методов обеспечения ИБ в составе ИСМ для СлПО для различных отраслей.

Сформулированы **рекомендации** по применению результатов работы с учетом новых законодательных инициатив (например, ФЗ-187) для обеспечения безопасности объектов КИИ РФ. Научные положения, представленные в диссертации, обеспечивают методическое сопровождение процессов автоматизации формирования численных показателей (метрик) ИБ, сокращения длительности процессов планирования, выполнения и анализа результатов аудита ИБ в ИСМ для СлПО.

В качестве **перспектив** дальнейшей разработки тематики могут быть предложены:

1. Разработка модели перехода от фиксированного перечня УБИ к модели комплексного оценивания рисков в процессе реализации аудита ИБ. В прогнозируемой перспективе это позволит обеспечить «единое управленческое поле» в ИСМ для обеспечения безопасности всех процессов в современных и перспективных СУ для СлПО.
2. Разработка модели реализации комплексного аудита ИБ, которая позволила бы предоставлять оценки всех процессов в современных интегрированных СУ для СлПО в едином пространстве, а не по отдельности (управление персоналом, управление инцидентами, управление рисками и пр.), что значительно повысило бы шансы на успех в информационном противоборстве с потенциальными злоумышленниками.

Соответствие диссертации паспорту научной специальности. Отраженные в диссертации научные положения соответствуют паспорту научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» в части области исследований по 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) и п. 15 (модели и методы управления информационной безопасностью).

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации, включенные в библиографические базы Web of Science и / или Scopus

1. Livshitz I., Neklyudov A., Lontsikh P. Evaluation of IT security – genesis and its state-of-art. IOP Conf. Series: Journal of Physics: Conf. Series 1015 (2018) 042029 DOI: 10.1088/1742-6596/1015/4/042029.
2. Livshitz, I.I., Lontsikh, P.A., Lontsikh, N.P., Kunakov, E.P., Drolova, E.Y. Implementation and auditing of risk management for the oil and gas company. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085881.
3. Livshitz, I.I., Ezrahovich, A.Y., Vladimirtsev, A.V., Karasev, S.N., Drolova, E.Y. Assessment of the impact of the modern risk-oriented standards on the security of the complex industrial facilities. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085873.
4. Livshitz, I.I., Ezrahovich, A.Y., Vladimirtsev, A.V., Lontsikh, P.A., Karaseva, V.A. Risk-based thinking of ISO 9001:2015 - The new methods, approaches and tools of risk management. Proceedings of the 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2017. DOI: 10.1109/ITMQIS.2017.8085872.
5. Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Karasev, S.N. The new aspects for the instantaneous information security audit. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751920.
6. Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Karaseva, V.A. The evaluation of the electronic services with accordance to IT-security requirements based on ISO/IEC 27001. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751921.
7. Livshitz, I.I., Lontsikh, P.A., Karaseva, V.A., Kunakov, E.P., Nikiforova, K.A. Implementation of information security and data processing center protection standards. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751923.
8. Livshitz, I.I., Nikiforova, K.A., Lontsikh, P.A., Drolova, E.Y., Lontsikh, N.P. The optimization of the integrated management system audit program. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies, IT and MQ and IS 2016. DOI: 10.1109/ITMQIS.2016.7751919.
9. Livshitz, I.I., Yurkin, D.V., Minyaev, A.A. Formation of the Instantaneous Information Security Audit Concept. Distributed Computer and Communication Networks, 2016. https://doi.org/10.1007/978-3-319-51917-3_28.

10. Livshitz I., Lontsikh P., Eliseev S. The Method of Implementation of the Numerical IT-Security Metrics in Management Systems. Proceedings of the FRUCT'20 (3-7 April 2017) pp. 242 – 248. ISSN 2305-7254. DOI: 10.23919/FRUCT.2017.8071318.
11. Livshitz I., Lontsikh P., Eliseev S. The Optimization Method of the Integrated Management System Security Audit. Proceedings of the FRUCT'20 (3-7 April 2017) pp. 248 – 254. ISSN 2305-7254. DOI: 10.23919/FRUCT.2017.8071319.
12. Livshitz Ilya, Podolyanets Lada. Models of Complex Industrial Facilities Assessment Based on Risk Approach. International Review of Management and Marketing, 2016, N.6 (S5) pp. 125-135. ISSN: 2146-4405.

Статьи в ведущих научных журналах и изданиях, рекомендованных ВАК Министерства образования и науки РФ:

13. Лившиц И.И. Оценка современных условия обеспечения безопасности сложных промышленных объектов / И.И. Лившиц, А.В. Неклюдов, А.Т. Танатарова // Энергобезопасность и энергосбережение. – 2018. – № 2. – С. 5-14. DOI: 10.18635/2071-2219-2018-2-5-14.
14. Лившиц И.И. Модель интегрированной системы менеджмента для обеспечения безопасности сложных объектов / Лившиц И.И., Фаткиева Р.Р. // Вопросы кибербезопасности. – 2018. – № 1 (25). – С. 64-71. DOI: 10.21681/2311-3456-2018-1-64-71
15. Лившиц И.И. Менеджмент информационной безопасности // Стандарты и качество. – 2017. – № 9. – С. 48-52.
16. Лившиц И.И. Анализ существующих ИТ активов для обеспечения информационной безопасности / И.И. Лившиц, А.В. Неклюдов // Вопросы защиты информации. – 2017. – № 1 (116). – С. 46-57.
17. Лившиц И.И. Методика оптимизации программы аудита интегрированных систем менеджмента // Труды СПИИРАН. – 2016. – № 5. – С. 52 – 68. DOI: 10.15622/sp.48.3.
18. Лившиц И.И. Формирование метрик для измерения результативности систем менеджмента информационной безопасности / И.И. Лившиц, П.А. Лонцих // Вестник Иркутского государственного технического университета. – 2016. – № 5. – С. 65 – 72. DOI: 10.21285/1814-3520-2016-5-65-72.
19. Лившиц И.И. Практические аспекты выполнения аудитов ИБ в соответствии с требованиями стандартов СТО БР ИББС // Деньги и кредит. – 2016. –№ 2. – С.54 –58.
20. Лившиц И.И. Оценка методических подходов для формирования систем безопасности сложных промышленных объектов топливно-энергетического комплекса // Вопросы защиты информации. – 2016. – № 1. – С. 56 – 61.
21. Лившиц И.И. Методика определения активов при внедрении и сертификации СМИБ в соответствии с требованиями ГОСТ Р ИСО серии 27001 и СТО Газпром СОИБ серии 4.2 // Вопросы защиты информации. – 2015. – № 4. – С. 43 – 51.
22. Лившиц И.И. Формирование концепции мгновенных аудитов информационной безопасности // Труды СПИИРАН. – 2015. – № 6 (43). – С. 253 – 270. DOI: http://dx.doi.org/10.15622/sp.43.14
23. Лившиц И.И. Оценка защищенности объектов топливно-энергетического комплекса // Энергобезопасность и энергосбережение. – 2015.– № 5. – С. 5 – 10.
24. Лившиц И.И. Определение активов при внедрении и сертификации СМИБ // Стандарты и качество. – 2015. – № 6 (936). – С. 84 – 85.
25. Лившиц И.И. Методика выполнения комплексных аудитов промышленных объектов для обеспечения эффективного внедрения систем энергоменеджмента // Энергобезопасность и энергосбережение. – 2015. – № 3. – С. 10-15.
26. Лившиц И.И. Исследование динамики сертификации по международным стандартам ISO для целей обеспечения комплексной безопасности // Вопросы защиты информации. – 2015. – № 2. – С. 48 – 56.
27. Лившиц И.И. Анализ уязвимостей и угроз национальной платежной системы Российской Федерации // Вопросы защиты информации. – 2015. – № 1. – С. 75 – 80.

28. Лившиц И.И. Методический подход к оценке защищенности информации в телекоммуникационных системах на основе анализа их доступности / И.И. Лившиц, В.В. Маликов // Вестнік Сувязі. – 2015. – № 2. – С. 57-61.
29. Лившиц И.И. Подходы к применению модели интегрированной системы менеджмента для проведения аудитов сложных промышленных объектов – аэропортовых комплексов // Труды СПИИРАН. – 2014. – № 6. – С. 72 – 94.
30. Лившиц И.И. Исследование зависимости сертификации по международным стандартам ISO от типов организации для ведущих отраслей промышленности / И.И. Лившиц, А.А. Молдовян, А.Т. Танатарова // Труды СПИИРАН. – 2014. – № 3 (34).
31. Лившиц И.И. Применение модели СМИБ для оценки защищенности интегрированных систем менеджмента // Труды СПИИРАН. – 2013. – № 8 (31). – С. 147 – 162.
32. Лившиц И.И. Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI / ISO // Информатизация и связь. –2013.–№6.– С.62– 67.
33. Лившиц И.И. Подходы к решению проблемы учета потерь в интегрированных системах менеджмента // Информатизация и связь. – 2013. – № 1. – С. 57 – 62.
34. Лившиц И.И. Подходы к синтезу модели оценки защищенности персональных данных в соответствии с требованиями стандарта ISO/IEC 27001:2005 // Труды СПИИРАН. – 2012. – № 4 (23). – С. 80 – 92.

Рецензируемые учебные пособия

35. Лившиц И.И. Нормативное обеспечение эксплуатации средств защиты информации: учебное пособие /А.В. Красов, И.И. Лившиц, Д.В. Юркин, А.В. Малых, Ю.О. Изотова; СПбГУТ. – СПб., 2017. – 68 с.
36. Лившиц И.И. Управление качеством систем менеджмента информационной безопасности: учебное пособие / А.В. Красов, И.И. Лившиц, Д.В. Юркин, А.В. Малых; СПбГУТ. – СПб., 2016. – 75 с.