Председателю диссертационного совета
Д 002.199.01
д.т.н., члену-корреспонденту РАН
Юсупову Р.М.

ОТЗЫВ

на автореферат диссертации Лившица Ильи Иосифовича «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами», представленной на соискание ученой степени доктора технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

В настоящее время объективно увеличилось количество деструктивных действий злоумышленников, направленных на технологические процессы и системы управления промышленных объектов, что обуславливает **актуальность** общей проблемы исследования и создания интегрированных систем менеджмента как части систем управления для обеспечения безопасности сложных промышленных объектов. В диссертационном исследовании Лившица И.И. показаны новые подходы для решения проблемы обеспечения информационной безопасности в условиях развития информационных технологий в области реализации процедур аудита информационной безопасности сложных промышленных объектов.

В диссертационном исследовании Лившица И.И. выявлен ряд системных **противоречий** между текущим состоянием теории и требованиями практики обеспечения информационной безопасности для сложных промышленных объектов. В работе отмечено, что их успешное преодоление требует решения ряда задач научного характера, направленных на развитие теории информационной безопасности как системы взаимосвязанных идей, основанных на классических трудах в области кибернетики и системного анализа.

Цель диссертационного исследования Лившица И.И. определена как снижение длительности и стоимости аудита информационной безопасности за счет использования новых моделей и методов аудита интегрированных систем менеджмента, реализующих оперативное формирование количественной оценки уровня обеспечения информационной безопасности в сложных промышленных объектах, выбор и применение наилучшего множества средств (мер) обеспечения информационной безопасности для обработки выявленных рисков.

Достижение указанной выше цели потребовало решения ряда **задач**, которые охватывают несколько комплексных и взаимоувязанных исследований. В частности выполнены исследование системных требований, предъявляемых к процессам обеспечения информационной безопасности в сложных промышленных объектах, исследование системных требований, предъявляемых при создании современных интегрированных систем менеджмента для защиты ценных активов, исследование аспектов применения риск-ориентированного подхода при обеспечении информационной безопасности для сложных промышленных объектов, исследование иерархической структуры показателей (метрик) информационной безопасности, исследование практической применимости предложенных методов обеспечения информационной безопасности в составе интегрированных систем менеджмента для сложных промышленных объектов для различных отраслей промышленности.

Основными **результатами** диссертационного исследования Лившица И.И., имеющими научную новизну и выносимыми на защиту, являются: обобщенные модели интегрированной системы менеджмента для обеспечения безопасности сложных промышленных объектов и базовая модель аудита интегрированной системы менеджмента, а так же три разработанных метода: метод проведения аудита интегрированной системы менеджмента для сложных промышленных объектов, метод исследования динамики сертификации по международным стандартам ISO

для сложных промышленных объектов и метод многошаговой оптимизации процесса аудита информационной безопасности в интегрированной системе менеджмента для сложных промышленных объектов.

Представленные в диссертационном исследовании Лившица И.И. методы и модели аудита информационной безопасности для сложных промышленных объектов **реализованы** как функционально завершенный элемент в системе мероприятий комплекса обеспечения информационной безопасности, что подтверждается несколькими актами о внедрении.

Практическая значимость проведенных Лившицем И.И. исследований состоит в улучшении методов оценки (аудита) информационной безопасности для сложных промышленных объектов, основанных на применении оптимального множества риск-ориентированных стандартов в составе интегрированной системы менеджмента, что обеспечивает эффективное противодействие деструктивным действиям злоумышленников, достижение требуемого уровня информационной безопасности, минимизацию потерь при возникновении ситуаций риска информационной безопасности, присущих сложным промышленным объектам, а также повышение степени соответствия законодательным требованиям.

По автореферату можно сделать следующие **замечания**:

1. В автореферате не определены явно возможность адаптации представленных в работе моделей и методов для определенного широкого класса сложных промышленных объектов с системой управления «жесткого реального времени». Предполагается, что помимо стандартов серии ISO/IEC могут быть применены «целевые» стандарты IEC серии 61508 и 61511.

2. В автореферате не приводится оценка достоверности и полноты данные, на основе которых осуществлялся расчёт показателей, относящихся к третьему защищаемому положению: методу определения динамических зависимостей сертификации ISO. Предполагается, что это объективная статистика ISO, но только ссылки на сайт отчета недостаточно для научных исследований.

3. На рис. 2 (стр 14) рис. 9 (стр. 29) в предложенных моделях аудитов информационной безопасности не указаны широко используемые в России стандарты ГОСТ Р ИСО серии 15408, а также не отражено взаимодействие с Банком данных угроз безопасности информации ФСТЭК России.

4. В тексте отсутствует пояснение, каким образом и с какими ограничениями новые предложенные модели и методы были использованы при выполнении экспериментальных исследований (см. таблицу 6, стр. 30).

Указанные замечания носят рекомендательный характер и не снижают общего положительного впечатления от работы Лившица И.И.

Основные **публикации** по теме диссертационного исследования, впервые содержащие защищаемые научные положения, выполнены в рецензируемых научных изданиях, в том числе: в 38 журналах, рекомендованных ВАК Российской Федерации, в 15 изданиях, индексируемых Scopus и/или Web of Science, а также в иных рецензируемых научных специализированных изданиях.

Представленная диссертационная работа, судя по автореферату, **удовлетворяет** требованиям ВАК Российской Федерации, предъявляемым к докторским диссертациям по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», а ее автор – Лившиц Илья Иосифович **заслуживает** присуждения ученой степени

доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Начальник сектора системной интеграции Центра защиты информации, кандидат технических наук

Белкин Тимур Григорьевич

27.09.2018

Подпись Белкина Т.Г. удос

Начальник отдела кадров

Валькова Е.А.

Почтовый адрес: 197376 г. Санкт-Петербург ул. Ак. Павлова, д. 14а

Телефон: +7(812) 295-1097

Факс: +7(812) 438-7560

E-mail: nii@nii-vektor.ru

http://www.nii-vektor.ru/