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»

Происходящее в настоящее время увеличение количества атак злоумышленников, направленных на технологические процессы различных критичных объектов, значительно значимость и **актуальность** общей проблемы создания интегрированных систем менеджмента как компонента систем управления для обеспечения безопасности сложных промышленных объектов. Автор в диссертационном исследовании показывает проблему обеспечения информационной безопасности в условиях, когда современный уровень развития информационных технологий позволил обеспечить больший охват производственных процессов, и, в том числе, реализацию процедур аудита сложных промышленных объектов.

В этой связи в диссертационном исследовании Лившица И.И. выявлен ряд системных **противоречий** и отмечено, что преодоление определенных противоречий между текущим состоянием теории и требованиями практики обеспечения информационной безопасности для сложных промышленных объектов 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 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 поставленной цели потребовало решения ряда **задач** для обеспечения требуемого уровня информационной безопасности:

1. Исследование системных требований, предъявляемых к процессам обеспечения информационной безопасности в сложных промышленных объектах и выявление закономерностей между изменениями требований регуляторов, стандартов (международных, отраслевых) и объективными потребностями создания интегрированных систем менеджмента как компоненты интегрированной системы управления для различных отраслей промышленности;
2. Исследование системных требований, предъявляемых при создании современных интегрированных систем менеджмента, для защиты ценных активов и анализ аспектов применения риск-ориентированного подхода при обеспечении информационной безопасности для сложных промышленных объектов, а также методов формирования оптимального перечня критериев для оценки результативности интегрированных систем менеджмента;
3. Исследование, анализ и создание иерархической структуры показателей (метрик) информационной безопасности в процессах обеспечения информационной безопасности, в том числе, аудита информационной безопасности, предназначенных для формирования и оценивания требований информационной безопасности в сложных промышленных объектах;
4. Разработка и обоснование методов обеспечения информационной безопасности в составе интегрированных систем менеджмента, с

учетом минимизации издержек по защите перечня активов и, в частности, увеличения стоимости нематериальных активов в составе сложных промышленных объектах;

5. 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:

1. Обобщенная модель интегрированной системы менеджмента для обеспечения безопасности сложных промышленных объектов, базовая модель аудита интегрированной системы менеджмента и система численных показателей (метрик) информационной безопасности для выполнения аудита интегрированной системы менеджмента.
2. Метод проведения аудита интегрированной системы менеджмента для сложных промышленных объектов.
3. Метод исследования динамики сертификации по международным стандартам ISO для сложных промышленных объектов.
4. Метод многошаговой оптимизации процесса аудита информационной безопасности в интегрированной системе менеджмента для сложных промышленных объектов.

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.

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.

По автореферату можно сделать следующие замечания:

1. Не представлено детальное обоснование формирования набора применяемых метрик в предложенном методе (см. рисунок 3, стр. 15);
2. Отсутствует анализ результативности и параметров быстродействия по модифицированной формуле Apdex в ходе проводимого экспериментального исследования (см. формулу 11, стр. 30);
3. В тексте отсутствует пояснение, каким образом новые предложенные модели и методы были использованы при выполнении экспериментальных исследований (см. таблицу 6, стр. 30);
4. В автореферате отсутствуют сведения о комплексных стоимостных показателях, используемых для оценки ущерба активам сложных промышленных объектов при выполнении «мгновенных» аудитов информационной безопасности (стр. 19-20).

Указанные замечания носят рекомендательный характер и не снижают общего положительного впечатления от работы. Основные результаты диссертационного исследования, впервые содержащие защищаемые научные положения, нашли отражения в 38 статьях, опубликованных в научных журналах, рекомендованных ВАК Российской Федерации, 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.

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».

Главный специалист по защите информации,
доктор технических наук, профессор

в Михаил Никитич

Подпись Бобова М.Н. уд
Начальник отдела кадро

).В.Кобзарь

12.10.2018

Открытое акционерное общество «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления»

Почтовый адрес:
220114, Республика Беларусь, г. Минск, пр. Независимости, д. 117
Телефон: (+375 17) 267-44-55, Факс: (+375 17) 267-24-50,
E-mail: agat@agat.by