УДК 004.056

РАЗРАБОТКА МЕТОДА МНОГОФАКТОРНОЙ ОПТИМИЗАЦИИ РИСКОВ ДЛЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Алексеев В.Р.
Научный руководитель – Профессор Лившиц И.И.
Санкт-Петербург, Университет ИТМО

Аннотация
В объектах критической информационной инфраструктуры (КИИ) используются различные методы защиты информации (в соответствии с Федеральным Законом №187-ФЗ). Для современных систем КИИ требуется оптимизация данных методов. В данной работе представлены варианты оптимизации методов защиты объектов КИИ на примере многофакторной оптимизации и повышения надежности.

Введение

Эффективность информационных систем (вычислительная и измерительная техника, автоматизированные системы управления, системы хранения, преобразования и передачи информации и др.) и программных комплексов в системах объектов критической информационной инфраструктуры во многом определяется уровнем защищенности информации от несанкционированного доступа. доступ и воздействие на него, а также достоверность информации, которая обрабатывается в этих системах и комплексах. Эти особенности напрямую связаны с проблемами безопасности и надежности информационных систем.

Целью данной работы является повышение конфиденциальности и целостности системы безопасности КИИ. Для достижения данной цели были поставлены задачи анализа возможных улучшений системы КИИ, анализа ограничений нововведений, запрещенных (или ограниченных) законодательством и стандартами, а также разработки метода внедрения многофакторной оптимизации и повышения надежности системы.

Основная часть

Реализация решений на основе таких методов, как оптимизация с использованием математических моделей и повышение надежности систем безопасности, требует изучения аспектов кибербезопасности для оценки соответствующих мер по обеспечению безопасности объектов критической информационной инфраструктуры. В данной работе представлены и проанализированы с точки зрения кибербезопасности аналитика для моделей многофакторной оптимизации и анализ системы безопасности объектов КИИ.

Предлагаемые решения основаны на мировых стандартах и локальных государственных законах Российской Федерации, а также приказах ФСТЭК России. Здесь они рассматриваются и объединяются в новый безопасный и экономичный метод на основе теоретико-множественных моделей мониторинга и управления информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления, а также телекоммуникационными сетями, используемыми для организации их взаимодействия. Меры кибербезопасности необходимы для защиты государственных учреждений, российских юридических лиц, владеющих информационными системами (ИС), информационно-телекоммуникационными сетями (ИТС), автоматизированными системами управления (АСУ), функционирующими в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской и других сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергетики, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности проанализированы и

оценены с точки зрения затрат на выполнение и с учетом ошибок безопасности, которые может возникнуть.
Предложенное решение позволяет реализовать экономичный метод для конкретного организационного решения объекта КИИ. Данный анализ направлен на решение проблемы безопасности по принципу проектирования, когда меры кибербезопасности должны быть рассмотрены и реализованы, начиная с первых этапов развития инфраструктуры.

Выводы

Внедрение решений, основанных на используемых в КИИ технологиях, таких как идентификация и аутентификация, управление доступом, ограничение программной среды и т.д. требует изучения аспектов информационной безопасности для оценки соответствующих мер по обеспечению безопасности критической информационной инфраструктуры. В данной работе представлена и проанализирована разработка оптимизированных методов использования многофакторной оптимизации и повышения надежности системы для систем КИИ с точки зрения кибербезопасности. Предлагаемые решения основаны на Федеральном Законе №187-ФЗ, приказе ФСТЭК №239, а также стандартах ISO/IEC 27032 и ГОСТ Р МЭК 61508. Этот анализ направлен на решение проблемы безопасности по принципу проектирования, когда меры кибербезопасности должны быть рассмотрены и реализованы, начиная с первых этапов развития инфраструктуры.

Алексеев В.Р. (автор) Подпись

Лившиц И.И. (научный руководитель) Подпись