ТЕХНОЛОГИЯ ОПТИМИЗАЦИИ ПРОЕКТНЫХ И УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ПРИ СОЗДАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБЪЕКТОВ МОРСКОЙ ИНФРАСТРУКТУРЫ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

А. В. Алексеев (Санкт-Петербург)

Бурное развитие информационных технологий, как никогда ранее, побуждает исследователей и разработчиков активно внедрять современные методы моделирования сложных организационно-технических процессов, включая, прежде всего, широкий спектр методов имитационного моделирования в теорию и практику решения актуальных задач развития и укрепления научно-производственного потенциала РФ.

Среди обширного ряда возникающих научных и практических задач особое место занимают задачи моделирования глобальных процессов и функционального качества объектов моделирования, оценивания качества самих моделей, поиска наиболее результативных путей практического применение моделей и инструментальных средств их реализации при управлении процессами и объектами моделирования, принятии эффективных проектных и управленческих решений (ПУР) по результатам моделирования.

Одной из таких важнейших практических задач является количественный сравнительный анализ (квалиметрический рейтинг-анализ) современных информационных комплексов и информационно-коммуникационных систем (ИКС) в целом, представленных на рынке IT–средств и технологий.

В условиях известной насыщенности рынка подобными продуктами и всё возрастающей конкуренции поставщиков средств и услуг оптимальный выбор ИКС различного назначения представляет сегодня весьма сложную проблему, ввиду, как правило, отсутствия сопоставимых и достоверных исходных данных для сравнения вариантов выбора ИКС, а также по причине методической сложности выполнения квалиметрических многокритериальных оценок для современных сложных многофункциональных организационно-технических комплексов.

Одним из возможных и перспективных направлений решения данной проблемы, в том числе для объектов морской инфраструктуры, сложных корабельных и береговых автоматизированных комплексов и систем, является проведение рейтинг-анализа средств по технологии полимодельной квалиметрической ранговой оптимизации проектных и управленческих решений (КРОПУР) [1].

Последняя прошла успешную апробацию в целом комплексе исследований и проектов, посвящённых сравнительному количественному анализу качества (рейтинг-анализу) различных объектов, включая объекты морской инфраструктуры, обеспечения их информационной безопасности, создания средств и систем обеспечения безопасности различного назначения, в том числе обеспечения комплексной безопасности города–области–региона [2–4].

В рамках настоящих исследований с целью демонстрации возможностей технологии КРОПУР на примере решения ряда практических задач и формирования базы данных квалиметрического сравнения и мониторинга качества автоматизированных систем в защищённом исполнении (АСЗИ) были обобщены результаты выполненного рейтинг-анализа основных классов современных сертифицированных средств и систем защиты информации (СЗИ), включая:

- средства разграничения доступа; средства межсетевого экранирования; VPN-средства;
- средства сканирования и анализа информационной безопасности;

- средства мониторинга–управления информационной безопасностью;
- средства защиты от вредоносных кодов (антиспамовые, антивирусные, средства);
- системы шифрования–дешифрования данных;
- операционные системы в защищённом исполнении;
- программно-аппаратные комплексы и системы в защищённом исполнении;
- системы электронной цифровой подписи и др.

При этом в составе сравниваемых СЗИ рассматривались только средства, включённые в Государственный реестр сертифицированных средств защиты информации, а полученные результаты анализа были использованы при реализации ряда IS-проектов компаниями-интеграторами [2–4].

Актуальность данного класса квалиметрических исследований обусловлена, как известно и представлено на рис. 1 из [5], проблемой большого числа СЗИ, представленных на современном рынке, и соответствующей сложностью выбора предпочтительных, а тем более *оптимальных* из них при создании систем обеспечения информационной безопасности объектов автоматизации. Ещё более остро стоит эта проблема для комплексных систем безопасности объектов автоматизации, в том числе морской инфраструктуры (от отдельных судов и кораблей до их соединений, до систем автоматизации тренажёрных центров, морских учебных заведений, проектных, конструкторских и технологических организаций, НИИ и заводов, корпораций и т.п., включая, например, подсистему обеспечения информационной безопасности единой АСЗИ Объединённой судостроительной корпорации).

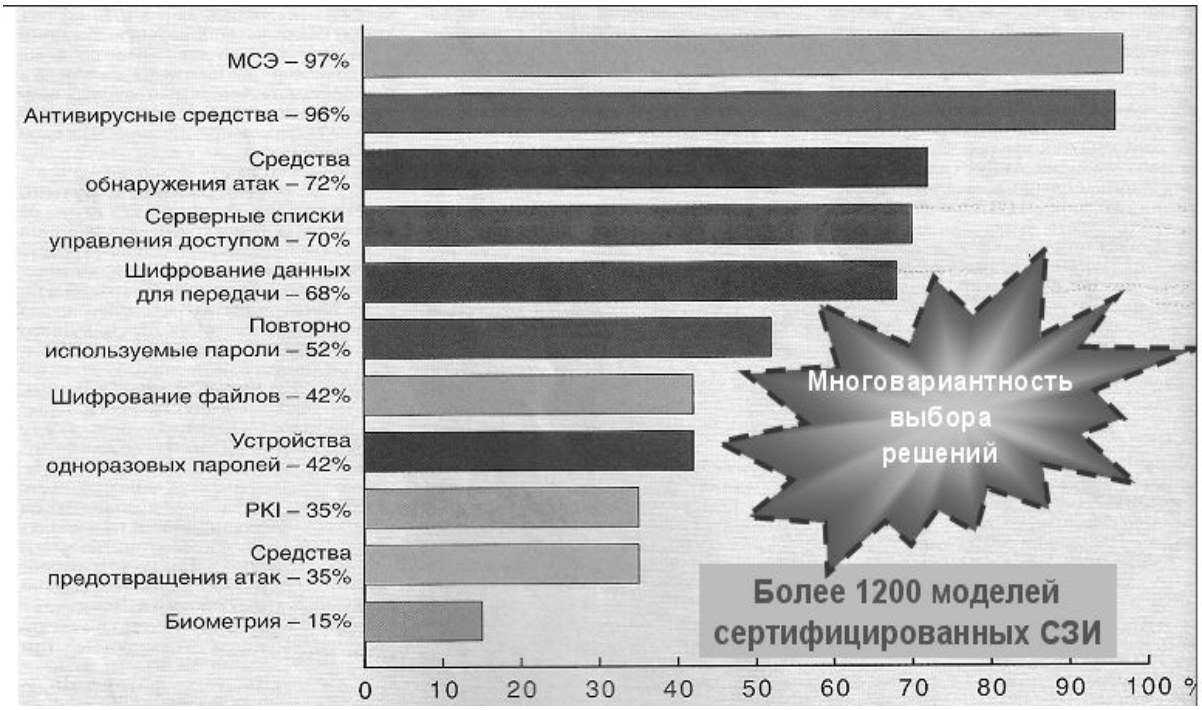

Рис. 1. Используемые технологии безопасности и проблема оптимизации их выбора

Только число межсетевых экранов (МСЭ) на рынке СЗИ согласно Госреестру сертифицированных СЗИ сегодня составляет более 150, выбор наиболее предпочтительных из них представляет собой весьма существенную проблему в связи с наличием в доступной литературе весьма ограниченных по объёму сведений и преимущественно рекламного характера.

Технические данные, выявленные в ходе сертификационных испытаний СЗИ, как правило, не публикуются [3, 4], а проведение сравнительных тестовых испытаний доступно далеко не каждой даже крупной компании. Это ставит компании-интеграторы по существу в неразрешимый либо крайне рискованный «тупик» технического и системного обоснования проектных решений.

Пример сложности современных проектных решений в области обеспечения комплексной безопасности и актуальности обоснования оптимальных проектных решений приведён в работах [2, 4] применительно к задаче концептуального проектирования.

Методика выполнения указанных исследований и испытаний в развитие [1] включала систематизацию известных данных, формирование групп сравнения альтернативных вариантов СЗИ, их специальный анализ и ранжирование. Исходные данные были заимствованы, прежде всего, из Государственного реестра сертифицированных СЗИ, а также с сайтов фирм-производителей (вендеров), из аналитических статей и материалов тестирования СЗИ. Кроме того, использовались консультации специалистов-разработчиков и специалистов-интеграторов.

При проведении исследований основное внимание было уделено систематизации критериев и показателей эффективности использования каждой из групп СЗИ (для соответствующих классов), моделированию для различных вариантов использования СЗИ наиболее характерных (типовых) вариантов отношений предпочтений заказчиков с соответствующим определением матрицы индексов важности соответствующих критериев. Полимодельность задания исходных данных по отношениям предпочтений подтвердила возможность получения при рейтинг-анализе альтернативных решений наиболее «объективной картины» формирования отношений предпочтений лицом, принимающим проектное и управленческое решение (ЛПР).

При определении рондомизированных сводных показателей использовался математический аппарат и средства информационной поддержки анализа и синтеза сводных показателей при информационном дефиците профессора Н. В. Хованова, как было ранее отражено в [1].

При этом формирование матрицы индексов интегральных критериев качества для соответствующих классов СЗИ позволило по существу создать равные условия и добиться сопоставимости всего ряда сравниваемых проектных решений. С другой стороны, согласование получаемых результатов с разработчиками СЗИ обеспечило минимизацию информационного дефицита при выполнении комплексного квалиметрического рейтинг-анализа.

Тем самым многокритериальное и полимодельное сравнение альтернативных вариантов СЗИ выполнялось для синтезированной по технологии КРОПУР системы моделей предпочтений Заказчика, согласовываемой с Разработчиком. Соответствующее ранжирование вариантов СЗИ обеспечивало реализацию заданных отношений модельных предпочтений Заказчика и Разработчика с последующей реализацией соответствующей согласованной типизации СЗИ, что также весьма важно для таких сравнительно новых областей знаний, как информационная безопасность.

Обсуждение полученных результатов рейтинг-анализа основных классов СЗИ, уточнение и корректировка отдельных исходных данных, выполненные с участием разработчиков СЗИ и при их, как правило, взаимном согласии с полученными выводами и рекомендациями, оформлено соответствующими протоколами и актами компаний-разработчиков (вендеров) и компаний-интеграторов. Широкое обсуждение полученных результатов среди специалистов и их одобрение, в том числе на указанных специализированных конференциях, позволяет рекомендовать к широкому использованию данные результаты при создании комплексов и систем обеспечения информационной безопас-

ности информационно-коммуникационных систем практически любой сложности и структуры.

Следует особо отметить масштаб сформированной базы данных, практически отражающей все основные классы СЗИ. Так, база сравниваемых вариантов межсетевых экранов составила более 140 моделей, для средств антивирусной защиты – более 10 моделей, для IDS/IPS – более 8 моделей. По каждой из моделей (вариантов) СЗИ в базе накопленных данных представлены в систематизированном и «рафинированном» виде практически все функционально значимые характеристики и параметры, естественно, с указанием их источника. Тем не менее сведения по точности отдельных данных и характеристик по известным причинам требуют их дальнейшей актуализации и систематизации.

Среди приведённых моделей требований Заказчика в практике рейтинг-анализа СЗИ наиболее востребованными оказались и могут быть рекомендованы модели «Бюджетная» и «Системная» в силу современного состояния рынка СЗИ, специфики требований «современных» Заказчиков.

Материалы исследований СЗИ для класса сканеров информационной безопасности в порядке иллюстрации приведены на рис. 2 для 7 моделей сканеров и 7 вариантов их комплексного использования (одновременного (вариант «I+P+X+R+T»), парного (варианты «I+X», «T+X», «T+I») и т.п.).

Результаты рейтинг-анализа СЗИ: Сканеры ИБ

Объекты	Название сканера безопасности, производитель
IS (I)	Internet Scanner 7.0 (Internet Security Systems, сертификат № 862-2004
PC (P)	Сетевой сканер "Ревизор сети" 1.2.1.0 ("ЦБИ-сервис", сертификат № 845/1-2004
MBSA_	Microsoft Baaseline Securite Analyzer v.2.0 (Microsoft)
XP (X)	XSpider 7.0 (Positive Technologies)
Retina (R)	Retina 4.9.221 (eEye Digital Security)
TNeWT (T)	Tenable NeWT 2.0 (Tenable Network Security)
AppDet_	AppDetective (Application Security)
I+P+X+R+T	Комплекс 5 сканеров: IS+PC+XP+Retina+TNeWT
I+P+X+R	Комплекс 4 сканеров: IS+PC+XP+Retina
I+P+X	Комплекс 3 сканеров: IS+PC+XP
I+X	Комплекс 2 сканеров: IS+XP
T+X	Комплекс 2 сканеров: TNeWT+XP
T+X+R	Комплекс 3 сканеров: TNeWT+XP+Retina
T+I	Комплекс 2 сканеров: TNeWT+IS

Оптимальный вариант

Рис. 2. Результаты рейтинг-анализа СЗИ для класса сканеров информационной безопасности

В частности, рейтинг-анализ вариантов комплексного использования сканеров ИБ показал, что практически из всех возможных комбинаций комплексирования сканеров наиболее результативным является вариант «T+X» (на рис. 2 указан выноской «Оптимальный вариант»). Он представляет собой комплексное использование сканера ИБ «Tenable NeWT (версии 2.0) компании Tenable Network Security и сканера «XSpider» (версии 7.0) компании Positive Technologies. Оптимальность данной варианта комплексного использования СЗИ обуславливается наилучшим соотношением достигаемого качества сканирования и суммарной стоимости используемых средств.

Среди других результатов рейтинг-анализа следует отметить: существенное влияние на результаты рейтинг-анализа модели отношений предпочтений Заказчика, низкой точности задания исходных данных отдельных производителей и их несопоставимости в ряде случаев для отдельных средств защиты информации.

Результаты испытаний и исследований показали, прежде всего, реальную возможность и актуальность оптимизации структуры и системных параметров комплексного использования СЗИ в составе подсистем (систем) комплексной защиты информации (СКЗИ) в составе АСЗИ.

Так, приведённые примеры наглядно иллюстрируют возможность оптимизации информационно-технической избыточности синтезируемых систем СЗИ, а также необходимость и возможность получения квалиметрически состоятельных оценок за счёт повышения точности задания исходных данных путём проведения сравнительных тестовых испытаний, в том числе на базе универсальных информационно-моделирующих стендов и комплексов (УИМК), что позволяет:

- при закупке средств оценивать их параметры и свойства, проводить функциональный входной контроль и активно осваивать тем самым новые программно-аппаратные средства (ПАС) как по отдельным их видам, так и в комплексе;
- при интеграции средств оценивать проектные архитектурные варианты, проверять ПАС в различных условиях функционирования ИКС на совместимость, устойчивость, эксплуатационные особенности и т.п., оптимизировать параметры их настройки, а также анализировать и синтезировать оптимальные проектные комплексные программно-аппаратные решения;
- выполнять предварительные аттестационные и сертификационные испытания СЗИ с целью качественной и экономичной подготовки к их сертификации;
- отрабатывать технологические методы и рекомендации по эффективному использованию ПАС применительно к условиям Заказчиков, в том числе с учётом аудита их ИКС (тест-аудита, экспресс-аудита, систем-аудита, контрольного аудита) и формирования SWOT-результатов;
- выполнять оперативные проработки новых технологических и проектных решений в обеспечение разработки аванпроектов и пилотных проектов создания ИКС;
- актуализировать данные и систематизировать базы данных рейтинг-анализа по тематике информационной безопасности ИКС, систем хранения информации, оптимальных проектных решений построения, создания и эксплуатации ИКС и другим, а также формировать перечни рекомендаций по эффективному проектному выбору СЗИ как внутри компаний, так и в отрасли, например, в масштабах Объединённой судостроительной корпорации;
- обучать персонал и демонстрировать перспективные системные и технические решения по вопросам IT-возможностей ИКС, IS-проблемам, рискам и путям их снижения, вариантам возможных атак на ИКС и оценке эффективности существующих на рынке и лучших СЗИ.

Практика выполнения рейтинг-анализа СЗИ и СКЗИ основных классов, полученные результаты и предложения рекомендуются исследователям сложных организационно-технических процессов и систем (включая специалистов по моделированию и квалиметрическому оцениванию сложных колмплексов и систем), разработчикам, проектировщикам и системными интеграторами объектов автоматизации морской инфраструктуры для поиска квалиметрически обоснованных предпочтительных и оптималь-

ных проектных решений, для обоснования перспективных направлений исследований, для формирования бизнес-стратегий развития компаний, а также целого ряда других приложений поиска оптимальных проектных и управленческих решений на основе количественной оценки ожидаемой эффективности и качества.

Особое значение полученные результаты и формирование баз данных рейтинг-анализа СЗИ по конкурентным предпочтениям соответствующих моделей приобретают в связи с учётом в технологии КРОПУР, используемой при формировании баз данных и их систематической актуализации, ряда альтернативных моделей предпочтений Заказчиков.

Пожалуй, наибольшую полезность для разработчиков-проектировщиков и управленцев различных уровней изложенный подход к квалиметрическому сравнению вариантов проектного выбора (как это рассмотрено на конкретном примере реализации технологии КРОПУР для вариантного проектирования СЗИ по всем их классам) имеет при использовании и актуализации (по результатам испытаний) подобных баз данных и их публикации испытательными лабораториями и органами сертификации СЗИ и ИКС в целом для различных ведомств и корпораций, включая Объединённую судостроительную корпорацию.

Литература

1. **Алексеев А. В.** Технология и программный комплекс квалиметрической ранговой оценки качества сложных информационно-аналитических систем // Материалы IX Всероссийской научно-практической конференции МОРИНТЕХ-ПРАКТИК «Информационные технологии в судостроении – 2008». СПб., 2008. С. 110–118.
2. **Антимонов С. Г., Сердюк В. А., Алексеев А. В., Калинин И. В.** Новые подходы к выбору средств антивирусной защиты при поддержке принятия комплексных проектных решений по обеспечению информационной безопасности // Сб. докл. V Юбилейной Всероссийской конференции «Обеспечение информационной безопасности. Региональные аспекты. 2006», 12–16.09.2006, Сочи. М.: Академия информационных систем, 2006. С. 90–95.
3. **Алексеев А. В.** Технология квалиметрической ранговой оптимизации проектных и управленческих решений» // Труды Международной научной школы «Моделирование и анализ безопасности и риска в сложных системах (МА БР-2007)». СПб.: ГОУ ВПО «СПбГУАП», 2007. С. 285–290.
4. **Алексеев А. В.** Оптимизация проектных и управленческих решений при комплексном обеспечении безопасности большого города // Безопасность большого города / Сб. ст.под ред. Э.И.Слепяна. СПб.: Изд-во Сергея Ходова, 2007. С. 400–418.
5. **Грибунин В. Г.** Тенденции развития средств защиты информации / IT-Security. 2006. С. 18.