ISSN 2305-994X

МАТЕРИАЛЫ
23-Й НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ
МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

30 июня – 03 июля 2014 г.

При участии

Федеральной службы безопасности РФ

Федеральной службы охраны РФ

Федеральной службы по финансовому мониторингу

Федеральной службы по техническому и экспортному контролю

Учредители и организаторы

Комитет по информатизации и связи Санкт-Петербурга

Комитет по науке и высшей школе Санкт-Петербурга

МОО «Ассоциация защиты информации»

ФГБОУ ВПО «СПбГПУ»

ЗАО «НПП «СТЗИ»

Генеральный спонсор

НЕОБИТ
НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Главный спонсор

Информ Инвест Групп

Партнеры

СПб Филиал ОАО «НПК «ТРИСТАН»

РЦЗИ ФОРТ

Санкт-Петербург, 2014

лимита времени на обработку информации в условиях неполной и нечеткой информации о состоянии сетевых элементов и ЗМС в целом. Он позволяет снизить размерность оптимизационных задач и, как следствие, улучшить оперативность и адекватность выработки управленческих решений по управлению ЗМС.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и государственного контракта №14.BBB.21.0097.

Баранов П.А.

НАПРАВЛЕНИЯ ТЕОРИИ РИСКОВ В ПРИЛОЖЕНИИ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

НИУ Высшая школа экономики, г.Москва

Опыт изучения области знаний управления рисками демонстрирует высокую вариативность применяемых методик. Результаты, достигаемые путем использования риск-ориентированного подхода при управлении деятельностью организации в целом или отдельных направлений деятельности, включают улучшение контроля за процессами деятельности, увеличение горизонта прогнозирования, повышение качества планирования. В то время, как основополагающая структура знания определена, предлагаемые методики реализации подхода многообразны и могут применяться в различных областях деятельности организации. Наиболее распространены в применении данного подхода страхование, финансовый анализ, управление проектами, направленными на повышение эффективности производства, поддержание безаварийной работы комплексов оборудования. Набирает популярность управление рисками в сфере информационных технологий (далее - ИТ). Это относится как к организации ежедневной деятельности ИТ подразделений, так и к продвижению новых проектов. Соответственно и в области информационной безопасности (далее - ИБ) также определено понятие риска и управления рисками ИБ.

В настоящее время принят ряд международных стандартов в области управления рисками, таких как ISO 31000:2009, инструкция ISO Guide 73:2009, BS 31100:2008, стандарты FERMA, COSO и другие. В отношении ИБ основные стандарты - это ISO серии 27000 и BS серии 7799, являющиеся их историческим прародителем. Российские стандарты представляют собой переложения (перевод с изменениями) международных стандартов. Однако, в нашей стране применение стандартов не является обязательным. Указанные стандарты по большей части и формируют упомянутую выше базовую структуру знания.

Вместе с тем, основные принятые принципы управления рисками, допускают применение широкого спектра алгоритмических механизмов, применяемых для управления риском как для целостного процесса, так и для реализации отдельных его шагов. В литературе и опубликованных исследованиях в этой области можно выделить несколько направлений применения указанных алгоритмов. Эти направления характеризуются приоритетными целями и инструментами, используемыми для их достижения, а также способами применения указанных инструментов, часто обусловленными изначальной областью применения конкретной методики. Три наиболее ярко выраженных направления - это: работа с риском с помощью

математических и статистических моделей (здесь следует заметить, что математическое моделирование в применении к проблемам ИТ вообще, пока еще слабо развито), принятие решения на основании оценки финансовых показателей и обращение с риском, как с продуктом принятия решений в ходе работы с цепочкой проблем.

Каждое из сформировавшихся направлений освещено в технической и финансово-экономической литературе, при этом источники адресуют свои методики как способы управления рисками. Имеется ряд опубликованных работ, специализирующихся на управлении рисками ИТ и ИБ. С целью определения применимости методик к решению задач ИБ и повышения эффективности управления ИБ в конечном итоге, видится полезным осветить преимущества и недостатки каждого из направлений, спроецировать их на область ИБ, и предложить круг вопросов защиты информации, в решении которых могут оказаться наиболее эффективными методики одного из направлений.

По предварительным результатам проводимых исследований можно сделать вывод о том, что методики с применением математического моделирования могут применяться в сфере аудита ИБ и оценки защищенности информационных ресурсов. Рекомендации по применению методик оценки финансово-экономических показателей относятся к задачам расширения функциональности систем обеспечения ИБ организации и ее модернизации. Работа с риском в аспекте решения ряда связанных проблем может быть рекомендована при решении текущих вопросов обеспечения ИБ.

Применение методик разных направлений дает возможность их взаимно интегрировать при решении смежных (в смысле решаемых в рамках одного процесса обеспечения безопасности информационных ресурсов) задач ИБ за счет применения единых метрик, шкал критичности, методик оценки риска. Наиболее выигрышные комбинации методик и соответствующие им механизмы сопряжения представляют собой предмет для дальнейшего исследования.

Волкова А.С., Калинин М.О.

СИСТЕМА ПРОГРАММНО-КОНФИГУРИРУЕМОЙ БЕЗОПАСНОСТИ ДЛЯ КРУПНОМАСШТАБНЫХ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННЫХ КОМПЛЕКСОВ

ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет», г.Санкт-Петербург

Современные системы обеспечения информационной безопасности с ростом сложности и гетерогенности информационных комплексов становятся чрезмерно громоздкими и менее эффективными. Эти системы не всегда способны развиваться одновременно с информационными технологиями и адаптироваться к изменяющейся картине угроз. Динамически растущие информационные системы, включающие облачные платформы и сервисы хранения и обработки больших объемов данных, мобильные сети изменяющейся топологии (mesh-сети, сети типа MANET, Интернет вещей), решения на базе BYOD и прочие технологии, значительно изменили среду применения традиционных моделей безопасности и определили необходимость создания новой адаптивной и гибко управляемой системы, способной противостоять как текущим, так и новым угрозам. Такая система может быть построена на базе концепции программно-конфигурируемой безопасности (ПКБ), являясь надстройкой