М. М. Тараскин, Ю. И. Коваленко

МЕТОДИКА ИССЛЕДОВАНИЯ УГРОЗ, УЯЗВИМОСТЕЙ И РИСКОВ В ОРГАНИЗАЦИИ

Одним из важнейших этапов построения оптимальной системы комплексной защиты информации в организации являются этапы всестороннего исследования угроз, уязвимостей и, как следствие, рисков.

Методика исследования угроз, уязвимостей и рисков в организации включает в себя: модель системы защиты информации, методику формализованного описания угроз, уязвимостей и рисков системы комплексной защиты информации и синтеза соотношений между ними (описательная и математическая составляющие).

При разработке модели системы защиты информации в организации необходимо: установить границы исследования; учитывать взаимосвязи между ресурсами; выполнять этапы (для выделенных ресурсов определяется их ценность как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т. п., описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации).

На основе разработанной модели представляется возможным обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы комплексной защиты информации в организации.

Описательная составляющая методики формализованного описания угроз, уязвимостей и рисков системы комплексной защиты информации включает: цель защиты информации; идентификацию и оценку информационных активов организации; исследование источников проблем для безопасности информации в организации (угрозы и уязвимости); исследование рисков для безопасности информации в организации; принятие решения по обеспечению безопасности информации в организации. Описательная составляющая методики формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними позволяет систематизировать порядок этапов ее проведения, определить их содержание, выработать те или иные рекомендации по обеспечению безопасности информации в организации для конкретной ситуации.

Математическая составляющая методики формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними на основе математического аппарата алгебры логики позволяет: в формализованном виде описать потенциальные угрозы безопасности информации в организации; оценить потенциальные уязвимости информационной безопасности в организации; обоснованно сделать выводы о потенциальных рисках для информационной безопасности организации и оценить их степень важности.

Применение в реальной обстановке методики формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними позволит получать обоснованные выводы о наличии рисков и тем самым обусловит выработку эффективных решений по их демпфированию или минимизации ущерба от них.

СПИСОК ЛИТЕРАТУРЫ:

1. *Мирошниченко В. М.* Национальная безопасность Российской Федерации. Обеспечение и организация управления: книга. М: Экзамен, 2002.
2. *Боридько С. И., Забелинский А. А., Коваленко Ю. И., Тараскин М. М.* Защита информации в организациях: методика исследования угроз, уязвимостей и рисков: монография. М.: МИНИТ, 2011.
3. *Лихтарников Л. М., Сукачев Т. Г.* Курс лекций по математической логике (учебное пособие). Новгород: Новгородский государственный педагогический институт, 1993.
4. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст).

А. А. Тихомиров, А. И. Труфанов, А. Россодивита

МОДЕЛЬ ВЗАИМОДЕЙСТВУЮЩИХ СТВОЛОВЫХ СЕТЕЙ В РЕШЕНИИ ЗАДАЧ ТОПОЛОГИЧЕСКОЙ УСТОЙЧИВОСТИ СЛОЖНЫХ СИСТЕМ

Введение. В теории комплексных сетей, которая ярко заявила о себе в [1], окончательно сформировалась, интенсивно и глубоко прорабатывалась в течение последнего десятилетия, сети принято разделять на социальные, биологические и технологические. При этом основной исследовательский интерес базируется на платформе топологически изощренных, но однородных обособленных невзаимодействующих сетей, представляемых плоскими конструкциями классической теории графов. В то же время признано, что существует необходимость в изучении взаимосвязанных сетей [2], с помощью которых можно было бы адекватно описать сложные системы и учесть основные особенности взаимодействия и взаимовлияния их элементов. Практика информационной безопасности с традиционной стратификацией мер на этическую, правовую организационную, техническую, физическую и математическую компоненты и новой сетевой интерпретацией предполагает обязательность их комплексного применения, тем самым подтверждая эту необходимость.

Метод. Для построения сетевой модели, отражающей связи, характерные для реальных систем, во-первых, использовался заявленный ранее подход «кружева единых сетей», или CNL, в представлении стволовых сетей [3], т. е. тройками (S, T, C), где S является непустым множеством стволов, T — непустым множеством тематических слоев, а $C = (C_1, C_2, .. ., C_l)$ представляет собой набор бинарных отношений на множестве S, где C_i соответствует тематический слой i. В отличие от традиционной «плоской» комплексной сети, стволовая сеть изображается в виде объемной структуры. Во-вторых, принималась во внимание различная природа сетей и представляющих их акторов. Следуя [4], комбинации разнородных сетей предлагается называть композитными сетями.

Основные результаты. В настоящей работе определена новая — композитная — стволовая сеть как множество S-сетей, описанных на клумбах $B = \{B_1, B_2, .. B_m\}$, которые представляют собой непересекающиеся множества стволов. Тогда ассоциации — мультиплеты (пары, тройки…), включающие в себя неповторяющиеся стволы различных клумб (S_i, S_k, S_i, …), так называемые букеты, объясняют функционирование реального объекта. Другими словами, букеты составлены из стволов, последние крепят узлы многослойной сети одного и того же характера, например узлы транспортной сети — авиалиний, железных дорог, линий речного транспорта, автобусных маршрутов… Нами сознательно введена новая простая терминология для преодоления междисциплинарных