УДК 338.24

С.Н. Гончаренко, Ю.Н. Рагозин

ВЫБОР ВАРИАНТОВ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛВС НА ОСНОВЕ КОМПЬЮТЕРНОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Главной целью системы информационной безопасности (СИБ) корпоративной ЛВС является обеспечение устойчивого функционирования предприятия, защита информационных ресурсов конфиденциального характера, обеспечение нормальной торговой и производственной деятельности всех структурных подразделений предприятия, а также повышение качества предоставляемых услуг и продуктов в интересах клиентов.

Решение, как обеспечить защиту и как ее реализовать в корпоративной ЛВС, какими должны быть типы и мощность мер и средств защиты, требует значительных размышлений. Защита ЛВС должна учитывать интересы и потребности организации в целом. Эта цель может быть достигнута только тогда, когда в решении задачи участвуют специалисты соответствующих подразделений предприятия: администраторы безопасности ЛВС, руководство предприятия, сотрудники службы защиты информации, владельцы данных и приложений, а также пользователи ЛВС.

Ранее в авторских работах [1, 2] был предложен метод выработки компромиссного решения, основанный на выборе определенных критериев (и шкал их измерения), которые принимаются для описания СИБ ЛВС. В качестве основных критериев рассматривались экономические критерии и критерии риска. Таким образом, каждый вариант СИБ представлялся в виде вектора определенной длины с конкретными значениями критериев. Множество векторов образует многомерное критериальное пространство, характеризующее совокупность всех рассматриваемых вариантов СИБ ЛВС.

В процессе разработки системы поддержки принятия решений (СППР) к вышеуказанным критериям добавился критерий оценки уровня доверия к безопасности объекта оценки. Доверие – основа для уверенности в том, что продукт или система ИТ (ЛВС) отвечает целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналитический опыт или специфический опыт. ГОСТ Р ИСО/МЭК 15408-3-2002 (требования доверия к безопасности) обеспечивает доверие с использованием активного исследования (причем, большее доверие является результатом приложения больших усилий при оценке). Предполагается, что проверку правильности документации и разработанного продукта или системы ИТ будут осуществлять опытные оценщики, уделяя осо-

Таблица 1

СИБ ЛВС	Обеспечение конфиденциальности, целостности и доступности к информации авторизованных пользователей					
Номер варианта СИБ ЛВС	Наименование критериев					
	Затраты на нейтрализацию угрозы 1 (т.р.)	Остаточный риск реализации угрозы 1 (балл)	----	Затраты на нейтрализацию угрозы n (т.р.)	Остаточный риск реализации угрозы n (балл)	Оценочный уровень доверия к СИБ (балл)
1 - m			---- ---- ----			

бое внимание области, глубине и строгости оценки. При этом не отрицаются и не комментируются относительные достоинства других способов получения доверия. Предлагаемые стандартом оценочные уровни доверия (ОУД1 – ОУД7), определяющие шкалу требований, позволяют с возрастающей степенью полноты и строгости провести оценку проектной, тестовой и эксплуатационной документации, правильности функционирования СИБ, стойкости механизмов защиты и сделать заключение об уровне безопасности объекта оценки.

Таким образом, критериальные оценки множества вариантов СИБ ЛВС можно представить в виде табл. 1.

Для организации защиты от угроз информационной безопасности и обеспечения экономически выгодного и безопасного использования информационных ресурсов ЛВС организации необходимо создать условия функционирования ЛВС с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба.

При практическом выполнении работ по реорганизации (проектированию) системы информационной безопасности корпоративной ЛВС в соответствии с существующими нормативно-методическими документами может быть использована следующая модель построения СИБ (рис. 1).

Данная модель представляет совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности ЛВС. Объективными факторами являются:

- ***угрозы информационной безопасности***, характеризующиеся вероятностью возникновения и вероятностью реализации;
- ***уязвимости*** СИБ ЛВС, влияющие на вероятность реализации угрозы;
- ***риск*** – фактор, определяющий возможный ущерб предприятия в результате реализации угрозы информационной безопасности (отражает вероятные финансовые потери – прямые или косвенные).

Оценка рисков может даваться с использованием различных как качественных, так и количественных шкал. Главное, чтобы существующие риски были правильно идентифицированы и проранжированы в соответствии со степенью их критичности для предприятия. На основе такого анализа может быть разработана система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

В настоящее время имеется большое разнообразие как методов анализа и управления рисками, так и реализующих их программных средств. Одним из популярных является метод CRAMM (the UK Government Risk

Analysis and Management Method), разработанный Службой Безопасности Великобритании в 1985 г. и используемый в качестве государственного стандарта как правительственными, так и коммерческими предприятиями. Разработкой и сопровождением одноименного программного продукта, реализующего этот метод, занимается фирма Insight Consulting Limited.

Другим мощным средством анализа и управления рисками является программное обеспечение Risk Watch, разрабатываемое американской компанией Risk Watch, Inc. В семейство Risk Watch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков:

- Risk Watch for Physical Security – для физических методов защиты ИС,
- Risk Watch for Information Systems – для информационных рисков,
- HIPAA-WATCH for Healthcare Industry- для оценки соответствия требованиям стандарта HIPAA,
- Risk Watch RW17799 for ISO17799 – для оценки требованиям стандарта ISO 17799.

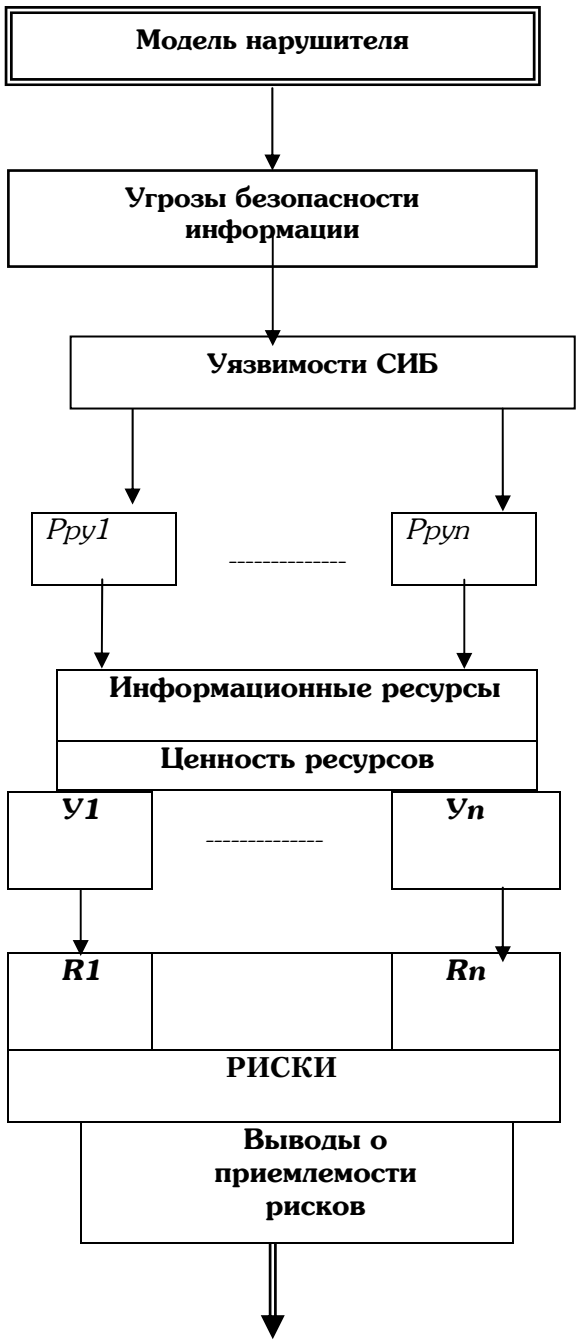
В методе Risk Watch в качестве критериев для оценки и управления рисками используются «предсказание годовых потерь» (Annual Loss Expectancy – ALE) и оценка «возврата от инвестиций» (Return on Investment – ROI).

Семейство программных продуктов Risk Watch по мнению специалистов имеет массу достоинств. К недостаткам данного продукта относят его относительно высокую стоимость.

Следует отметить и еще один программный продукт, разрабатываемый компанией Risk Associates, - систему COBRA (Consultative Objective and Bi-Functional Risk Analysis) как средство анализа рисков и оценки соответствия ИС стандарту ISO 17799. COBRA реализует методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. При разработке инструментария COBRA были использованы принципы построения экспертных систем, обширная база знаний по угрозам и уязвимостям, а также большое количество вопросников, с успехом применяющихся на практике. В семейство программных продуктов COBRA входят COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant.

Наряду с рассмотренными достаточно сложными подходами к оценке уровня риска существуют и простые одномерные подходы, которые рассматривают только ограниченные компоненты. Например, риск, связанный с угрозой, может рассматриваться как функция относительной вероятности, что угроза может произойти и ожидаемых потерь, которые могут быть понесены при реализации угрозы. В этом случае риск рассчитывается как произведение нормализованных вероятности появления угрозы (через определенное уязвимое место) и возможных потерь.

Человек принимает решение на основе собственной целостной совокупности представлений о ситуации (ментальной модели). Однако ментальные модели содержат представления, не укладывающиеся в логическое мышление, поэтому решения и действия человека не всегда имеют под собой логическую основу. Проведенные психологические исследования показывают, что при отсутствии аналитической поддержки ЛПР



- разрабатывается при участии подразделения по защите информации или службы безопасности предприятия
- полный перечень угроз безопасности информации для конкретной ЛВС

- полный перечень уязвимостей СИБ, через которые потенциально возможна реализация угроз БИ

- вероятности реализации угроз через существующие уязвимости

- непосредственно влияет на уровень возможного ущерба

- уровни ущерба (материальных потерь) при реализации угроз

- оценка рисков в информационной системе

- итоговая оценка риска в информационной системе

Рис. 1. Модель построения СИБ

часто пользуются упрощенными, а порой и противоречивыми решающими правилами [7].

Только автоматизированные системы поддержки принятия решения в настоящее время способны обеспечить сравнение и анализ большого количества вариантов проектов, каждый из которых оценивается по многим критериям. Роль СППР при этом состоит в представлении информации в наглядном графическом виде, представлении ЛПР аналитических возможностей для исследования множества предложенных вариантов и поддержке ведения переговоров по сближению позиций в процессе выбора компромиссного варианта решения.

Компьютерная поддержка процесса принятия решений так или иначе основана на формализации методов получения исходных и промежуточных оценок, даваемых ЛПР, и алгоритмизации самого процесса выработки решения.

Термин «система поддержки принятия решений» появился в начале семидесятых годов. За это время дано много определений СППР. Так в [4] СППР определяется как «комплекс математических и эвристических методов и моделей, объединенных общей методикой формирования альтернатив управленческих решений в организационных системах, определения последствий реализации каждой альтернативы и обоснования выбора наиболее приемлемого решения». Каждая СППР носит сугубо индивидуальный характер, поскольку определяется конкретным содержанием решаемой управленческой проблемы и особенностями процедуры принятия решений в той или иной организации. Если процедуры принятия решений регулярны, устойчивы, например, периодическое планирование производственной деятельности, то состав и последовательность функционирования системы поддержки принятия решений закрепляются в качестве нормативных методик, использующих преимущественно формальные модели и методы при незначительном использовании диалоговых процедур. При решении периодически возникающих проблемных ситуаций с высокой степенью неопределенности и, как правило, не имеющих полных аналогов в прошлом, системы поддержки принятия решений разрабатываются индивидуально под каждую проблему, в их состав включают преимущественно логико-эвристические и экспертные методы и модели. При этом главную роль начинают играть диалоговые процедуры.

Хотя конкретные реализации СППР очень сильно зависят от области применения, методы генерации решений, их оценка и согласование основываются на одних и тех же базовых теоретических принципах и предпосылках. Схема функционирования компьютерной СППР приведена на рис. 2 [5, 6].

Номера блоков на рис. 2 показывают последовательность принятия решений, стрелки обратной связи – цикличность процесса.

В основе разработанного подхода для поиска компромиссного решения (рис. 3) лежит реализация двух способов визуализации критериального пространства – двумерный, когда число отображенных на графике критериев равно двум, и многомерный, когда число критериев больше двух. В многомерном способе координатные оси представлены в виде радиусов окружности, отстоящих друг от друга на равные углы.

ЛПР имеет возможность задавать количество, название и веса (значимость) критериев, а также значения

Рис. 2. Схема функционирования компьютерной СППР

критериев для каждой точки отображения, назначать на критериальном пространстве целевые точки, которые отражают позицию ЛПР по рассматриваемой проблеме, задавать для целевых точек кластеры, которые выражают возможный компромисс со стороны ЛПР и выглядят как прямоугольная область вокруг целевой точки в двумерном изображении, либо как внутренность фигуры, ограниченной многоугольниками, в многомерном отображении. ЛПР может назначать до 26 целевых точек и до 10 кластеров в каждой из них. Целевые точки и кластеры можно перемещать, удалять, добавлять, а у кластеров, кроме того можно изменять радиусы.

СППР сама автоматически определяет три точки, ближайшие к целевой (в смысле евклидова расстояния), которые могут быть предложены в качестве компромиссного решения, а также автоматически фиксирует точки, попавшие в кластер. Многокритериальное отображение может быть спроецировано на отображение меньшей размерности для детального анализа.

Рис. 3. Структурная схема автоматизированной системы выбора компромиссного решения

Дополнительным инструментом является построение Парето-оптимального множества альтернатив, чтобы заранее отсеять заведомо неудачные варианты. Но его не следует применять при нахождении компромиссного решения ЛПР с антагонистическими взглядами.

В системе постоянно отображается информация о точках, ближайших к целевым точкам и точкам, попавшим в кластеры. Все действия ЛПР протоколируются, и есть возможность вернуться к предыдущему варианту.

Для практического использования СППР разработаны три методики, которые подробно описаны в статье автора [3].

Разработанный компьютерный продукт поддержки выбора компромиссного решения прошел успешное апробирование на одном из крупнейших предприятий связи Российской Федерации при выборе компромиссного варианта из ранее разработанных и предлагаемых на рынке типовых СИБ корпоративных ЛВС и получил название «Выбор компромиссного решения - СИБ ЛВС» (ВКР – СИБ ЛВС).

Необходимо отметить, что разработанная система лишь обеспечивает поддержку процедуры переговоров

по выбору компромиссного решения: представляет удобный интерфейс и средства для исследования предложенных вариантов решений, отражения позиции каждого из ЛПР и нахождения компромисса. Процедура переговоров с использованием «ВКР – СИБ ЛВС» принципиально является человеко-машинной. Выбор решения и ответственность за его принятие всегда остается прерогативой управленца, и в этом процессе, кроме компьютерного анализа, большую роль играют опыт и искусство менеджера.

Данный подход имеет еще то преимущество, что отдельные ЛПР могут при назначении своей области предпочтений принимать во внимание не весь набор критериев, а только некоторые из них. Это означает, что в качестве ЛПР можно приглашать экспертов – специалистов в узких областях (например, специалиста по криптографии, по аппаратным средствам, по экономике информатизации и т.д.), которые, с одной стороны обладают высокой компетенцией в своей области знания, а с другой стороны, чаще, чем специалисты широкого профиля, имеются в наличии и которых поэтому легче найти.

СПИСОК ЛИТЕРАТУРЫ

1. *Еремин В.М., Рагозин Ю.Н.* Выбор вариантов обеспечения безопасности в информационных системах муниципальных организаций./Проблемы регионального и муниципального управления. Материалы Международной научной конференции. Москва, 2005 г.
2. *Рагозин Ю.Н.* Информационная безопасность корпоративных ЛВС – проблема выбора оптимального решения. / Вестник академии промышленности и менеджмента. Выпуск 5. Москва 2006 г.
3. *Рагозин Ю.Н.* Принципы выбора и вербальной оценки компромиссных решений в системах комплексной защиты информации. / Безопасность информационных технологий. №1, Москва, МИФИ, ВНИИПВТИ, 2007 г.
4. Экономико-математический энциклопедический словарь / *Гл. ред. В.И. Данилов-Данильян.*- М., 2003 г.
5. *Трахтенгерц Э.А.* Компьютерная поддержка принятия решений: Научно-практическое издание. Серия «Информатизация России на пороге XXI века». – М.; СИНТЕГ, 1998 г.
6. *Трахтенгерц Э.А.* Принятие решений на основе компьютерного анализа. – М.; Институт проблем управления, 1996 г.
7. *Slovic P., Fishhoff B., Lichtenstein S.* Behavioral decision theory // Annu. Phychol. Rev. Vol. 28. 1997.

Коротко об авторах

Гончаренко С.Н. – доцент кафедры «Автоматизированные системы управления»,
Рагозин Ю.Н. – доцент кафедры «Информационная безопасность»,
Московский государственный горный университет.

Рецензент д-р техн. наук, проф. *Н.И. Федунец.*