УДК 004.056, 004.838.2

КОМПЬЮТЕРНАЯ ПОДДЕРЖКА ФОРМИРОВАНИЯ ЦЕЛЕЙ ПРИ ПРОЕКТИРОВАНИИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

О.В. Лукинова

Рассмотрены компьютерные методы формирования списка целей обеспечения безопасности проектируемой системы защиты автоматизированных бизнес-процессов компании, реализованных в виде информационной системы, которая представляется моделью OSE/RM.

Ключевые слова: комплексная система защиты, объект защиты, модель OSE/RM, бизнес-процесс, оценочные критерии безопасности.

ВВЕДЕНИЕ

Формирование целей и стратегий их достижения — важнейшая составляющая процедуры принятий решений при осуществлении тех или иных мероприятий. В данной статье речь пойдет о проектировании системы безопасности, позволяющей защитить корпоративную информационную систему (КИС) от нежелательных информационных воздействий.

Процесс построения системы защиты характеризуется слабоструктурированностью, противоречивостью требований, неоднозначностью оценки ситуаций, ошибками в выборе приоритетов, поэтому выбрать «правильные» цели и стратегии их достижения без компьютерной поддержки становится все сложнее. Преодолеть сложности помогают системы поддержки принятия решений (СППР), которые определяются как человеко-машинные системы, позволяющие руководителям для принятия решений использовать свои знания, опыт и интересы, объективные и субъективные модели, оценки и данные, а также опыт принятия групповых решений [1]. С другой стороны, СППР, варьируя методы генерации целей, их оценки и ранжирования, может влиять на субъективные предпочтения лица, принимающего решения (ЛПР), и тем способствовать принятию лучших решений. Настоящая работа и посвящена описанию формализмов, которые позволят компьютерной системе в автоматизированном режиме определять цели обеспечения безопасности КИС.

1. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

Средством реализации автоматизированных бизнес-процессов компании является корпоративная информационная система (КИС). Поэтому вопрос о защите КИС правомерно ставить как вопрос о защите выполняемых в ней бизнес-процессов. В работе [2] подчеркивались преимущества, когда защищаемыми активами становятся бизнес-процессы, а именно: возможность оценить ущерб как материальные потери от неэффективной/некорректной работы, простоев бизнес-процессов; оправдать бюджет на защиту; сформировать реально обоснованную потребностями бизнеса политику информационной безопасности; обосновать достаточность планируемых средств защиты; проектировать систему защиты одновременно с разработкой КИС.

Функциональность ИТ-составляющей бизнес-процесса на референсном (логическом) уровне будем представлять моделью OSE/RM (Open System Environment/Reference Model) группы POSIX (Portable Operating System Interface for Unix) [3], представляющей КИС как сочетание платформенного и прикладного компонентов, а также проекций передней плоскости модели на плоскости защиты и администрирования (рис. 1).

Модель представляется в виде матрицы типов компонентов среды, состоящей из трех уровней и четырех функциональных групп в каждом:

— компоненты служб и сервисов промежуточного, системно-прикладного слоя (MW);

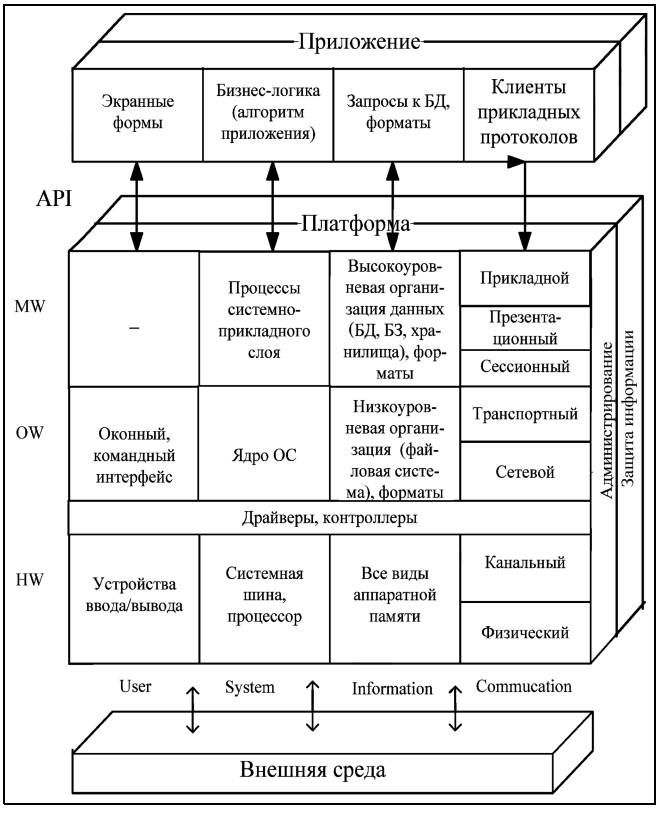

Рис. 1. Модель OSE/RM

— компоненты операционных систем или операционного слоя (OW);

— аппаратный слой (HW).

Функциональные группы компонентов в данной модели составляют:

— компоненты, обеспечивающие интерфейс с пользователем (User);

— компоненты, обеспечивающие все необходимые процессы в системе (System);

— компоненты, обеспечивающие организацию, представление, доступ и хранение данных (Information);

— компоненты телекоммуникационной среды, обеспечивающие взаимосвязь информационных систем (Communication); данный уровень представляет собой модель взаимосвязи открытых систем (OSI/RM — Open System Interconnection/Reference Model).

Приложение служит для реализации бизнес-задач, оно, собственно, и определяет содержимое бизнес-процесса. Платформа оказывает системные услуги приложению при его функционировании, которые вызываются посредством API (application program interface)-функций. Разумеется, приложений, необходимых для выполнения функций бизнес-процесса и «сидящих» на одной платформе, может быть несколько. Целью защитной компоненты должно стать обеспечение информационной безопасности компонент бизнес-процесса, реализуемых «клетками» передней плоскости.

2. ФОРМИРОВАНИЕ ОБЩЕЙ ЗАДАЧИ ПРИНЯТИЯ РЕШЕНИЙ

Первый шаг, осуществляемый СППР при проектировании комплексной системы защиты (КСЗ), под которой понимается комплекс программно-аппаратных средств защиты, заключается в формировании целей, которым она должна удовлетворять. Решение о необходимости защиты, как правило, принимается руководством организации, здесь важно понимание стратегических вопросов: какой уровень $\overline{KS}$ защиты необходим, чтобы обеспечить безопасное и непрерывное функционирование бизнеса; сколько будет стоить защита данного уровня St; какой ущерб U понесет компания в случае, если защита окажется недостаточно эффективной. Рис. 2 иллюстрирует эту взаимосвязь.

Набор целей достаточно стандартный, однако ЛПР может отдать предпочтение одному из следующих вариантов:

— если ЛПР ориентируется на минимальную стоимость системы защиты, то уровень безопасности $\overline{KS}$ будет, соответственно, невысок, а ущерб U — максимальным, т. е.

$$St^{\min} \Rightarrow \overline{KS}^{\min} \Rightarrow U^{\max}; \qquad \text{(А)}$$

— если ЛПР потребует обеспечить максимальную безопасность, то надо быть готовым к тому, что и стоимость такой системы окажется максимальной, но зато, можно уверенно предположить, что ущерб будет минимальным (если случится), т. е.

$$\overline{KS}^{\max} \Rightarrow St^{\max} \Rightarrow U^{\min}; \qquad \text{(Б)}$$

— если ЛПР придерживается стратегии приемлемого (а не минимального) ущерба $U < U^*$, то получит уровень защиты и стоимостные затраты в

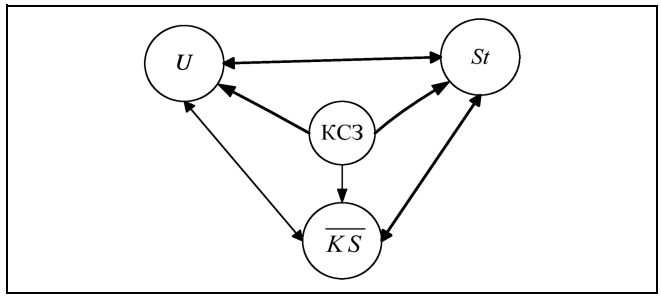

Рис. 2. Взаимосвязь стратегических целей

пределах от минимально до максимально возможных, т. е.

$$U < U^* \Rightarrow \overline{KS}^? \Rightarrow St^?. \qquad \text{(В)}$$

Выбор того или иного варианта развития событий — суть принятия решения на стратегическом уровне; СППР может осуществить его двумя способами.

В соответствии с одним из них выбор делается автоматически, когда СППР на основании оценок рисков $Risk_i$ бизнес-процессов S_i, полученных подсистемой мониторинга [4], делает вывод о том, какой критерий должен быть главным. Алгоритм заключается в следующем:

а) на основании оценок ущерба $Pr(S_i)$ и угроз Y_i в работе [4] для рисков была получена следующая оценочная шкала «Риск»: «очень низкий», «низкий», «средний», «выше среднего», «высокий». Логично предположить (табл. 1), что если для S_i-го процесса:

— $Risk_i$ = «высокий», то СППР выбирает вариант целей (Б),

— $Risk_i$ = «средний» — вариант (В),

— $Risk_i$ = «очень низкий» — вариант (А).

б) если $Risk_i$ = «низкий» или $Risk_i$ = «выше среднего», то СППР проводит дополнительный анализ соотношения оценок ущерба $Pr(S_i)$ и угроз Y_i. Каждое лингвистическое значение шкалы «Риск» соответствует интервалу значений, полученных от произведения $Pr(S_i)$ на Y_i. Анализ заключается в том, что если значение произведения попадает в первую половину интервала шкалы, то СППР относит его в более низкую категорию; если оно попадает во вторую половину — то в категорию, лежащую правее (см. табл. 1).

В соответствии с другим способом СППР предлагает перечень возможных целей, которые хранятся в ее БД (разумеется, этот перечень может быть дополнен или модифицирован ЛПР):

— обеспечить безопасность бизнес-процессов в требуемом объеме;

— обеспечить безопасность бизнеса в рамках выделяемых средств;

— минимизировать ущерб, наносимый компании, если защита окажется недостаточной;

— строить защиту, исходя из установленных пороговых значений приемлемого ущерба;

— выделить ресурсы на организацию защиты информационных активов компании в достаточном объеме;

Таблица 1

Выбор целей в зависимости от риска

$St^{\min}$	?	$U < U^*$	?	$\overline{KS}^{\max}$
Очень низкий	Низкий	Средний	Выше среднего	Высокий

— минимизировать стоимость выделяемых на организацию защиты ресурсов.

Эксперты (имеется в виду, что работает группа экспертов) или ЛПР выбирают те или иные цели, а СППР отслеживает, чтобы этот выбор, в соответствии с вариантами (А), (Б) и (В), был непротиворечив и согласовывал их. Согласование можно проводить разными способами [1], в СППР может быть заложено несколько методов с тем, чтобы ЛПР мог выбрать процедуру согласования в зависимости от жесткости предъявляемых требований.

Тем самым СППР формирует постановку задачи (А), (Б) и (В) для рационального выбора защитных механизмов и в, конечном итоге, средств защиты.

3. ДЕТАЛИЗАЦИЯ ЦЕЛЕЙ, ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНОСТЬ БИЗНЕС-ПРОЦЕССОВ

Поскольку объектами защиты являются бизнес-процессы, реализация которых в КИС представляется в виде «куба» OSE/RM (см. рис. 1), перечень целей безопасности для проектируемой КСЗ целесообразно также структурировать в соответствии с этой моделью. В стандартах по информационной безопасности под безопасностью понимается обеспечение конфиденциальности данных, сохранности от подделки, доступности к данным и услугам, которые осуществляются как приложениями пользователям, так и платформой приложениям. При построении бизнес-процессов «клетки» OSE/RM реализуются конкретными данными, программным и аппаратным обеспечением. Эти реализации и подлежат защите. Тогда задача в том, чтобы по каждому S_i-му бизнес-процессу ($1 \leqslant i \leqslant N$, N — число бизнес-процессов, образующих функциональный состав данной КИС) необходимо обеспечить безопасность реализации каждой p-й «клетки» модели ($1 \leqslant p \leqslant P$, P — число реализованных «клеток» среды S_i-го бизнес-процесса) и цели безопасности формируются СППР на основании состава реализаций «клеток». Алгоритм детализации целей изображен на рис. 3. Дадим некоторые комментарии к блокам, требующим пояснения.

В *блоке 2* определяются «клетки», подлежащие защите. Поэтому СППР предъявляет экспертам для выбора следующий список целей S_i-го бизнес-процесса:

1) обеспечить безопасность реализации «клетки» 1;

2) обеспечить безопасность реализации «клетки» 2;

...

P) обеспечить безопасность реализации «клетки» P.

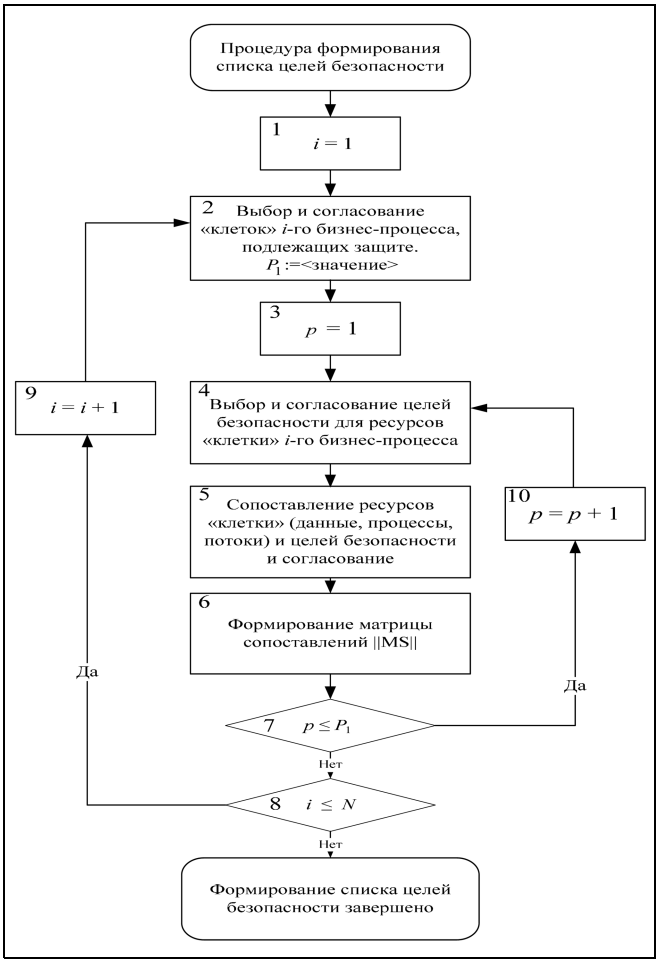

Рис. 3. Алгоритм процедуры детализированного формирования списка целей

Указанные цели могут выбираться экспертами и с помощью графического представления модели OSE/RM (см. рис. 1) рассматриваемой КИС. Затем СППР согласует списки. Пусть согласованный список состоит из целей для P_1 «клеток» ($P_1 \leqslant P$).

В *блоке 4* СППР определяет, какие, по мнению экспертов, из свойств безопасности должны быть обеспечены для p-й «клетки». Поэтому СППР проводит дальнейшую детализацию целей для выбранных «клеток». Эта процедура может осуществляться автоматически, на основании матрицы соответствия j-го оценочного критерия ценности информационных ресурсов и p-й «клетки», полученной подсистемой мониторинга [4] $Z = ||z_{pj}||$, где

$$z_{pj} = \begin{cases} 1 \text{ — соответствие есть,} \\ 0 \text{ — в противном случае.} \end{cases}$$

Если, например, БД некоторой «клетки» оценивалась по критерию «Нормативные акты, регламентируемые актив», то это может быть база персональных данных сотрудников, доступ к которой на основании закона [5] конфиденциален. А если речь идет об электронном магазине, то все «клетки», отвечающие за связь и организацию удаленного взаимодействия, должны обеспечивать высокую доступность, так как именно эти «клетки» оценивались по критерию «Приносимый доход» или «Объем недополученного дохода». Анализ, указывающий на связь оценочного критерия и свойства безопасности, производится в подсистеме предпроектного проектирования при формировании списка критериев. Таким образом, СППР делает выводы о том, какие свойства безопасности (конфиденциальность (K), целостность (C), доступность (D)) надо обеспечить тем или иным «клеткам» и предъявляет их экспертам для утверждения или модификации, если экспертов выводы СППР не устраивают; после чего списки согласовываются.

В результате каждой p-й «клетке» ставится в соответствие вектор целей $\overline{KS}_p$ (C, D, K), содержащий одно, два или все три свойства (цели) безопасности, которые надо обеспечить.

В *блоке 5* СППР уточняет и согласовывает с какими конкретно информационными объектами, ассоциированными с «клеткой», соотносятся цели вектора $\overline{KS}_p$. Такими объектами могут быть хранимые, обрабатываемые или передаваемые данные пользовательских массивов, служебные данные операционной системы или самой системы безопасности; коды и процессы платформенного, прикладного и защитного компонентов, а также объекты аппаратного слоя (см. рис. 1). Обозначим список детализированных согласованных целей $Sp_p(sp_1^K, ..., sp_k^K, sp_1^C, ..., sp_c^C, sp_1^D, ..., sp_d^D)$, где $(sp_1^K, ..., sp_k^K)$ — подмножество целей, которые обеспечивают свойство конфиденциальности (K), $(sp_1^C, ..., sp_c^C)$ — свойство целостности (C) и $(sp_1^D, ..., sp_d^D)$ — доступности (D) к объектам p-й «клетки».

В *блоке 6* СППР по каждой «клетке» формирует матрицу сопоставления $\|MS_p\|$ размера $3 \times \max(k, c, d)$, где

$$ms_{ij}^p = \begin{cases} 1 \text{ — } i\text{-я цель присвоена } j\text{-му объекту} \\ p\text{-й "клетки",} \\ 0 \text{ — в противном случае.} \end{cases}$$

Описанную процедуру формирования и согласования целей СППР проводит циклически по каждой «клетке» каждого бизнес-процесса.

В результате СППР сформирует распределение по «клеткам» детализированных и согласован-

ных списков Sp_p, векторов $\overline{KS}_p$ и матриц таких сопоставлений $\|MS_p\|$. Объединяя списки Sp_p, СППР получит согласованные списки возможных целей $Sp_i = \bigcup_{p=1}^{P_1} Sp_p$, обеспечивающих безопасность S_i-х бизнес-процессов, $i = 1, ..., N$.

4. ФОРМИРОВАНИЕ КРИТЕРИЕВ БЕЗОПАСНОСТИ

Цели Sp_i должны описывать проектное решение системы защиты в соответствии с требуемым уровнем безопасности. Задача компьютерной системы заключается в том, чтобы на основании определенных критериев уметь оценивать варианты проектируемой системы. В качестве таких критериев логично использовать параметры «уровень конфиденциальности» (K), «уровень целостности» (C), «уровень доступности» (D), которые и составят критериальные векторы безопасности $\overline{KS}_i$ (C, D, K), хотя, если рассуждать на детальном уровне, то речь следует вести не о векторах, а о критериальных матрицах безопасности $\|KS_i\|$ (для обозначения целей безопасности и их оценочных критериев используются одни и те же обозначения, так как семантически их смысл одинаков). Значения $\overline{KS}_i$ задаются как термы T лингвистических переменных или как балльные оценки (табл. 2), важно, чтобы они были однородными.

Указанные шкалы сформированы на основании нормативных и законодательных документов [6] и хранятся в базе данных СППР. Однако в подсистеме предпроектного проектирования они могут быть модифицированы и согласованы.

4.1. Процедура определения значений критериев

Эксперты должны выразить свои требования к безопасности бизнес-процессов в форме тех или иных значений критериев $\overline{KS}_i$, а стало быть, необходимо реализовывать процедуру определения целевых значений векторов безопасности $\overline{KS_i^{\text{цель}}}$ (K, C, D).

Автоматическая процедура формирования целевых векторов состоит из следующих шагов.

Шаг 1. Определение *базового* уровня критериев в соответствии с приоритетом бизнес-процесса.

Шаг 2. Определение *предпочитаемого* уровня на основе субъективной значимости критериев для эксперта.

Шаг 3. Определение *ожидаемого* уровня критериев с учетом степени риска среды.

Заметим, что в этой процедуре СППР применяет исключительно эвристические алгоритмы, которые могут быть модифицированы, дополнены или заменены прямым вводом экспертных оценок.

В подсистеме мониторинга [4] были получены оценки ценности информационных ресурсов, сопоставленных «клеткам» $Pr(K_p)$ и средние по бизнес-процессу $Pr(S_i)$ по шкале «высокий-4», «средний-3», «низкий-2», «очень низкий-1», «отсутствует-0» (через дефис здесь и далее в лингвистических шкалах приведены балльные оценки). Поэтому СППР может определять значения в двух режимах: обобщенном, на уровне бизнес-процессов (определяются значения векторов $\overline{KS}_i$) и детальном — для «клеток», и тогда речь следует вести о матрицах $\|KS_i\|$. Для простоты изложения опишем алгоритм обобщенного режима, уровень «клеток» работает аналогично.

Рассмотрим бизнес-модель, состоящую из трех бизнес-процессов банковского сектора:

бизнес-процесс S_1: расчетно-кассовое обслуживание юридических лиц;

бизнес-процесс S_2: стратегическое планирование;

бизнес-процесс S_3: депозитарное обслуживание.

Шаг 1. Определение базового уровня. Средние оценки $Pr(S_i)$ определяют вектор приоритетов $Pr^{b/p}(Pr(S_1), Pr(S_2), ..., Pr(S_N))$, где N — число бизнес-процессов. Пусть для нашей бизнес-модели

Таблица 2

Критерии безопасности и их лингвистические значения

K — конфиденциальность	Терм	Коммерческая тайна	Строго конфиденциально	Конфиденциально	Внутренний документ	Несекретно
	Балл	4	3	2	1	0
C — целостность	Терм	Очень высокая	Высокая	Средняя	Низкая	Отсутствует
	Балл	4	3	2	1	0
D — доступность	Терм	Очень высокая (24×7)	Высокая (24×5)	Средняя (8×7)	Низкая (8×5)	Не поддерживается
	Балл	4	3	2	1	0

подсистема мониторинга сформировала вектор $Pr^{b/p}(4, 3, 1)$.

Для каждого бизнес-процесса на основании вектора $Pr^{b/p}$ СППР назначает базовые значения критериев безопасности, т. е. получим векторы базовых значений критериев безопасности по всем процессам $K^B(T_1^*, T_2^*, ..., T_N^*)$, $C^B(T_1^*, T_2^*, ..., T_N^*)$, $D^B(T_1^*, T_2^*, ..., T_N^*)$, где $T_i^* = Pr(S_i)$ — базовые значения критериев S_i-го бизнес-процесса.

Таким образом, получим базовые вектора безопасности $K^B(4, 3, 1)$, $C^B(4, 3, 1)$, $D^B(4, 3, 1)$ (табл. 3). Эти же значения получают и все «клетки» реализаций данных бизнес-процессов в соответствии с моделью OSE/RM.

Шаг 2. Определение предпочитаемого уровня. Специфика бизнеса влечет и разные требования к защите, т. е. значимость тех или иных критериев безопасности для разных типов бизнеса разная, например, банковский сектор зачастую отдает предпочтения целостности БД экономической информации, нежели ее конфиденциальности. Поэтому СППР должна выяснить точку зрения ЛПР относительно важности для него критериев $\overline{KS}_i$. Важность оценивается по шкале «очень высокая-4», «высокая-3», «средняя-2», «низкая-1» (см. пример в табл. 4). Таблицы типа табл. 4 заполняются для каждого бизнес-процесса и согласовываются экспертами заранее в подсистеме предпроектного проектирования.

В итоге по бизнес-процессам СППР получит матрицу предпочтений $TS^{b/p} = ||ts_{ij}||$, где ts_{ij} — оценки значимости j-го критерия для i-го бизнес-процесса.

Оценки значимости критериев корректируют базовый уровень безопасности, т. е. векторы $D^B(T_1^*, T_2^*, ..., T_N^*)$, $C^B(T_1^*, T_2^*, ..., T_N^*)$, $K^B(T_1^*, T_2^*, ..., T_N^*)$ подправляются величинами ts_{ij}, например, если:

— $ts_{ij} = 3$, то соответствующее базовое значение остается без изменений,

— $ts_{ij} = 2$, то базовое значение уменьшается на 1,

— $ts_{ij} = 1$, то базовое значение уменьшается на 2.

Тогда получим табл. 5 предпочитаемых уровней критериев безопасности

или в векторном виде $K^W(3, 3, 1)$, $C^W(3, 1, 0)$, $D^W(4, 1, 0)$.

Вообще говоря, на этом этапе можно завершить алгоритм, если эксперты решат не учитывать оценки риска среды, и тогда при выборе средств защиты можно либо ориентироваться на матрицу предпочитаемых уровней, либо вначале производить выбор средств по базовой матрице, а в случае, если таких средств не найдется, ослаблять условия выбора до матрицы предпочитаемых уровней.

Шаг 3. Определение ожидаемого уровня. В подсистеме мониторинга на основе рейтинга уязвимостей бизнес-процесса и потенциала возможного нарушителя были получены оценки угроз Y_p, которые могут быть реализованы в «клетках» среды, а также оценки всего бизнес-процесса Y_i [4]. В работе [7] приведена классификация уязвимостей по критериям безопасности, к нарушению которых ведет использование уязвимости злоумышленником. На основании этой классификации СППР получает матрицу оценок угроз $Y^{b/p} = ||y_{ij}||$, где y_{ij} — оценка опасности уязвимостей i-го бизнес-процесса по j-му критерию. Пусть для нашего примера эти оценки представлены матрицей $Y^{b/p} = \begin{pmatrix} 4 & 3 & 2 \\ 1 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix}$.

Ненулевые значения говорят о том, что ресурсы данного бизнес-процесса содержат уязвимости, которыми может воспользоваться нарушитель.

Таблица 3

Базовые уровни критериев безопасности бизнес-процессов

Наименование бизнес-процесса	*K*	*C*	*D*
Расчетно-кассовое обслуживание юридических лиц	4	4	4
Стратегическое планирование	3	3	3
Депозитарное обслуживание	1	1	1

Таблица 4

Значения важности критериев безопасности

Наименование бизнес-процесса	Важность критерия		
	K	*C*	*D*
Расчетно-кассовое обслуживание юридических лиц	2	2	3
Стратегическое планирование	3	2	1
Депозитарное обслуживание	3	2	1

Таблица 5

Предпочитаемые уровни критериев безопасности бизнес-процессов

Наименование бизнес-процесса	Предпочитаемый уровень		
	K	*C*	*D*
Расчетно-кассовое обслуживание юридических лиц	3	3	4
Стратегическое планирование	3	1	1
Депозитарное обслуживание	1	0	0

Они должны учитываться при планировании защиты, т. е. ожидаемые уровни критериев безопасности K^{O}, C^{O} и D^{O} должны быть построены на основе предпочитаемых, но с учетом поправок на значения оценок угроз. В частности, возможны варианты:

— если оценка опасности нулевая, то уровень защиты для этого бизнес-процесса по данному критерию может быть снижен также до нуля;

— поднимать предпочитаемые уровни на значение оценки угрозы, но максимум до базовых значений (тогда сознательно допускаем некоторую «дырку» в защите, если полученная сумма окажется меньше максимально возможного значения критерия), табл. 6;

— если оценки угроз ненулевые, поднимаем оценки K, C и D до максимального уровня.

В табл. 7 приведен пример целевых векторов, числовые значения которых получены в результате выполнения шагов 1—3. Функции, в соответствии с которыми осуществлялись поправки, представляют собой эвристики, их список может изменяться и дополняться экспертами, именно поэтому в таблице приведено k ожидаемых уровней.

Если S_i-й бизнес-процесс обменивается данными с бизнес-процессом S_j, то целевые значения должны быть выровнены: если входящий в S_j-й бизнес-процесс информационный поток имеет больший уровень по некоторому критерию, то значение S_j-го бизнес-процесса по этому критерию надо увеличить.

Таблица 6

Ожидаемые уровни критериев безопасности бизнес-процессов

Наименование бизнес-процесса	Ожидаемый уровень		
	K	*C*	*D*
Расчетно-кассовое обслуживание юридических лиц	4	4	4
Стратегическое планирование	4	2	2
Депозитарное обслуживание	1	0	3

Таблица 7

Наборы целевых векторов защиты бизнес-процессов

Уровни защиты бизнес-процесса S_i	*K*			*C*			*D*		
	S_1	S_2	S_3	S_1	S_2	S_3	S_1	S_2	S_3
Базовый	4	3	1	4	3	1	4	3	1
Предпочитаемый	3	3	1	3	1	0	4	1	0
Ожидаемый 1	4	4	1	4	2	0	4	2	3
— " — 2	4	4	0	4	4	0	4	4	4
...	...	...	...	...	...	...	...	...	...
— " — k	3	3	1	4	1	2	2	0	0

Таким образом, СППР получает набор целевых векторов для i-х бизнес-процессов $\overline{KS_i^{\text{цель}}}(K(T^*), C(T^*), D(T^*))$, где $K(T^*)$, $C(T^*)$, $D(T^*)$ — уровни конфиденциальности, целостности и доступности соответственно, которые должна обеспечивать КСЗ для S_i-х бизнес-процессов, а T^* — означает выбранные значения (термы) лингвистических переменных. Если описанный алгоритм отработает в детализированном режиме, то СППР получит наборы векторов безопасности по «клеткам» $\overline{KS_p^{\text{цель}}}(K(T^*), C(T^*), D(T^*))$. Это означает, что цели, обеспечивающие безопасность на уровне бизнес-процессов или на уровне «клеток», сформированы.

ЗАКЛЮЧЕНИЕ

Рассмотренные компьютерные методы и алгоритмы группового принятия решений позволяют в автоматизированном режиме формировать цели при проектировании комплексной системы защиты для корпоративной информационной системы. В дальнейшем СППР должна будет сформировать возможные стратегии, позволяющие достичь целевых векторов $\overline{KS_i^{\text{цель}}}$. В качестве стратегий рассматриваются различные варианты состава защитных средств, выбор которых осуществляется с учетом критериев стоимости St и ущерба U, т. е. должна решаться одна из задач (А), (Б) или (В).

ЛИТЕРАТУРА

1. *Трахтенгерц Э.А.* Компьютерная поддержка формирования целей и стратегий. — М.: СИНТЕГ, 2005. — 224 с.
2. *Лукинова О.В.* Формализация задачи планирования защиты распределенной компьютерной сети на основе бизнес-процессного подхода // Надежность. — 2009. — № 1. — С. 72—80.
3. *ISO/IEC TR 14252 — 1996.* Guide to the POSIX Open System Environment.
4. *Лукинова О.В.* Компьютерные методы мониторинга и анализа защищенности при функционировании автоматизированных бизнес-процессов компании // Открытое образование. — 2011. — № 4. — С. 37—47.
5. *Закон* Российской Федерации № 152 «О персональных данных» от 27.07.2006.
6. *Закон* Российской Федерации «О государственной тайне» от 27.07.1993.
7. *Сердюк В.А.* Новое в защите от взлома корпоративных систем. — М.: Техносфера, 2007. — 360 с.

Статья представлена к публикации членом редколлегии А.Д. Цвиркуном.

Лукинова Ольга Васильевна — канд. техн. наук,
ст. науч. сотрудник,
Институт проблем управления им. В.А. Трапезникова РАН,
г. Москва, ☎ (495) 334-89-70, ✉ Lobars@mail.ru.