УДК 004.056.5

А.И. Шлыков, А.С. Шабуров
Пермский национальный исследовательский
политехнический университет, Пермь

РАЗРАБОТКА МОДЕЛИ ОЦЕНКИ ОПЕРАТИВНОЙ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ

Современные информационные системы функционируют без учета рисков информационной безопасности, не обеспечивая эффективность систем защиты. Статья описывает модель оценки оперативной эффективности систем защиты информации коммерческих предприятий. В её основе лежит метод анализа рисков предприятия, а также метод анализа иерархий. С их помощью оценивается оперативная эффективность, а результатом являются данные о вероятностях угроз, степени ущерба и суммарного риска. В рамках разработки модель подвергается описанию принципов функционирования, в заключении даются рекомендации по использованию.

Ключевые слова: риск информационной безопасности, оперативная эффективность, метод анализа иерархий, модель оценки.

A.I. Shlykov, A.S. Shaburov
Perm National Research Polytechnic University, Perm

DEVELOPMENT OF A MODEL FOR ASSESSING THE OPERATIONAL EFFICIENCY OF THE INFORMATION SECURITY SYSTEM OF COMMERCIAL ENTERPRISES

Modern information systems operate without taking into account information security risks and ensuring effectiveness. The article describes a model for assessing the operational efficiency of information security systems. It is based on the method of risks analysis using the method of hierarchies analysis. With it, operational efficiency is assessed, and the result is data on the probabilities of threats, the degree of damage and total risk. As part of development, the model is subjected to a description of the operation principles, in the conclusion recommendations for use are given.

Keywords: information security risk, operational efficiency, hierarchy analysis method, assessment model.

Введение. Данные статистики по коммерческой отрасли в каждом отчёте приводят неутешительные факты - корпоративные системы предприятий привлекают большое число злоумышленников, а ущерб от реализации угрозы может быть сопоставим с рыночной ценностью предприятия. Компании, допускающие реализацию угроз для информационной системы (далее – ИС), не уделяют внимания оценке ресурсов и рисков. Согласно отчетам Eset и Anti-Malware [1], это происходит ввиду неграмотного моделирования бизнес-процессов на предприятии и отсутствию связи с обеспечением информационной безопасности (далее – ИБ). Бизнесу важна оценка бизнес-рисков компании, поскольку она используется для учёта потенциальных воздействий событий ИБ на приоритетные ресурсы ИС [2]. Бизнес-риски позволяют рассмотреть эффект,

который оказывает угроза на ИС, при помощи экономических и вероятностных метрик – именно языком финансов и потерь от бездействия в сфере ИБ можно объяснить руководству компании необходимость внедрения системы защиты информации. Поэтому риски необходимо моделировать на объекте (ИС предприятия). Угрозы и риски тесно связаны с оценкой оперативной эффективности системы защиты информации (далее – СЗИ) – моделировании такой СЗИ, которая позволяет получить минимальную степень риска. Для её моделирования нужно понимать, что риски направлены на бизнес-процессы. В области бизнес-аналитики организация моделируется как конгломерат бизнес-процессов [2, 3], а проектирование модели выполняется экспертом, обладающим опытом проведения анализа.

Описание модели. В основе моделирования оценки оперативной эффективности СЗИ лежит метод анализа рисков в сочетании с экспертной оценкой [4]. Привлечение экспертов необходимо, поскольку многие ИС не накапливают статистики по инцидентам ИБ - невозможно использовать статистические данные и моделировать вероятность как отношение числа событий к числу инцидентов. Иначе, модель предполагает, что компания на время аудита не накопила статистики – это наиболее вероятно, так как среднестатистические коммерческие системы не используют анализ типа SIEM.

Для проектирования модели, как в случае с экономической эффективностью СЗИ [5], применяется ситуационный анализ в предметной области рисков информационной безопасности. В моделировании используется семиотическая цепочка (Рисунок 1), состоящая из 3 единиц функционирования компании: бизнес-ресурс R_i – бизнес-функция (F_j) – бизнес-процесс (O_k).

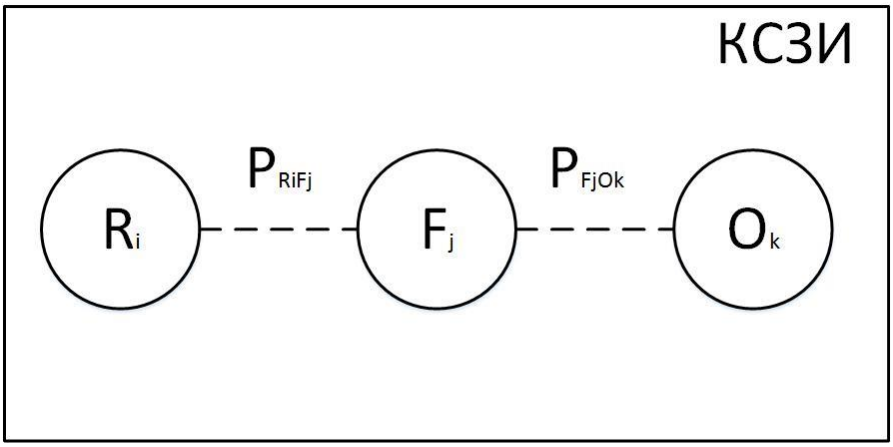

Рисунок 1 – Концептуальная модель оценки оперативной эффективности КСЗИ

Модель будет представлять собой оценку вероятности отказа всей системы, которая, моделируется в виде ресурсов, функций и бизнес-процессов. Результат будет риском информационной безопасности.

$$P(M_n)=\sum_{i=1}^{m}\sum_{j=1}^{l}\sum_{k=1}^{t} P_{R_{iF_j}} * P_{F_jO_k} \qquad (1)$$

Формула (1) означает, что суммарная вероятность отказа модели будет равна сумме всех возможных отказов ресурсов, функций и процессов.

Оптимальным вариантом оценки является метод анализа иерархий (метод Саати), который позволяет провести приоритезацию модели, выявлять критичные процессы, ресурсы и функции, оценить вероятность угрозы и величину рисков. Так как риск ИБ — это вероятность возникновения негативного события, наносящего ущерб бизнес-процессам организации или физическому лицу, то вероятность отказа модели $P(M_n)$ представляет собой риск ИБ. Для расчёта используется модель парных сравнений угроз и уязвимостей. Задача преобразования качественных описаний в количественные решается таблицами парных сравнений, отражающих относительную значимость уязвимостей и угроз. Общий вид таблицы лингвистических сравнений двух параметров показан в Таблице 1.

Таблица 1 – Показатели парных сравнений параметров эффективности

Лингвистическая оценка сравнения 1-го и 2-го параметра	Показатель
При наличии 1-го 2-й параметр эффективности не учитывается	9
Существенное превосходство 1-го над 2-м параметром	7
Использование 1-го параметра эффективности предпочтительнее, чем 2-го	5
Чуть более высокая значимость 1-го параметра против 2-го	3
Одинаковая значимость сравниваемых параметров	1

Описание множества сравниваемых параметров с использованием шкалы относительной значимости представлено в виде матрицы парных сравнений множества уязвимостей $B=\{b_1,b_1 \dots b_n\}$ [6]:

$$M_B=[b_{nm}], \quad (2)$$

Следующим шагом, ранговая шкала (таблица 1) определяет вектор доступности V уязвимостей для реализации злоумышленником:

$$V=(v_1,v_2 \dots v_s) \quad (3)$$

Взаимосвязь между угрозами и уязвимостями определяется матрицей их причинно-следственных связей:

$$M_{yy}=[c_{nS}], \quad (4)$$

Для расчёта вероятности возникновения угроз на основе матриц, нужно выявить зависимость между существующими уязвимостями и угрозами. В текущем состоянии расчёта перемножаются матрицы относительной значимости уязвимостей и причинно-следственных связей уязвимостей и угроз. Получится единственная матрица значимости уязвимостей для возникновения угроз:

$$M_{ПЗ}=M_{yy}\cdot M_B=[w_{ns}], \quad (5)$$

Далее, матрица (5) дополняется вектором влияния уязвимости на появление угрозы (6). Таким образом исследуется интегральный показатель влияния всех уязвимостей на возникновение *k*-й угрозы:

$$w_k = \sum_{r=1}^{S} w_{kr} \quad (6)$$

Дальнейшая нормализация вектора проводится так, чтобы максимальному значению соответствовало числу 9, а минимальному – 1. Матрица отношений элементов:

$$M_w = \begin{bmatrix} 1 & \cdots & 1/w_{ln} \\ \vdots & \ddots & \vdots \\ w_{ln} & \cdots & 1 \end{bmatrix} \quad (7)$$

Нахождение вероятностей возникновения угроз ИБ P_b проходит таким образом - находятся собственные числа в матрице M_w и из них вычисляется вектор, соответствующий максимальному значению вероятности по формуле (3).

Перейдем к расчёту ущерба, который наносит угроза незащищенной ИС. Ущерб U_i рассчитывают, как относительную величину стоимости ИС к ущербу, который нанесет *i*-я угроза незащищенной ИС:

$$U_i = h_i * (S_u + S_{ou} + S_{czu}) \quad (8)$$

Далее необходимо оценить вероятности устранения угроз ИБ. Они определяются тем, насколько полно учтены качественные и количественные требования к КСЗИ при ее проектировании. Вероятность устранения *j*-й угрозы по выходит из выражения:

$$P^i_{yj} = \sum_{q=1}^{l} k^i_{jq} * x^i_{jq}, \quad (9)$$

где k^i_{jq}– весовой коэффициент значимости требования для устранения угрозы; x^i_{jq}– степень выполнения требований к СЗИ для устранения угрозы.

Риск для ИС – это произведение вероятности возникновения угроз и ущерба в случае их реализации. Величина показывает, какой вероятный ущерб может понести предприятие в связи с реализацией угрозы ИБ:

$$R = \sum_{i=1}^{n} P_{bi} * U_i * (1 - P_{yi}) \quad (11)$$

Чем выше вероятность устранения угрозы СЗИ, тем меньший риск понесет компания при их реализации. Модель не предполагает изменение ИС во времени, модельное время для неё не задаётся. Модель может быть реализована в математической системе Mathcad, а графы визуализироваться в системе Gephi.

Заключение. Таким образом, предложенная модель позволяет оценить эффективность ликвидации рисков информационной безопасности системой защиты, иначе рассчитать оперативную эффективность СЗИ. Модель позволяет рассчитать вероятности реализации угроз ИБ, равно как степень ущерба, в произведении определяя риски информационной безопасности. В дальнейшем модель необходимо апробировать на реальном объекте защиты, тем самым доказав актуальность и применимость результатов научного исследования.

Библиографический список

1. Анализ рынка ИБ в России. Часть 1. // [Электронный ресурс] - Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1 (Дата обращения: 17.05.19);

2. Баранова Е.К. Методики анализа и оценки рисков ИБ // Образовательные ресурсы и технологии. – 2015. – № 1 (9). – С. 73-79.;

3. Информационная безопасность и бизнес-процессы компании. // [Электронный ресурс]: https://cyberleninka.ru/article/v/informatsionnaya-bezopasnost-i-biznes-protsessy-kompanii (Дата обращения: 15.01.19);

4. Motzek A., Möller R. Context- and bias-free probabilistic mission impact assessment // Computers & Security. – 2017. – №65. – P. 166-186.;

5. Шлыков А.И., Шабуров А.С. О формализации подходов к разработке моделей многокритериальной оценки эффективности систем защиты информации // Автоматизированные системы управления и информационные технологии – 2020;

6. Wheeler E. Security Risk Management: Building Information Security Risk Management Program from the Ground Up // Syngress Publishing, 2011.

Сведения об авторах

Шлыков Алексей Игоревич - магистрант кафедры «Автоматики и телемеханики», Пермский национальный исследовательский политехнический университет, гр. КЗИ-19-1м, г. Пермь. E-mail: thekingofthedas@gmail.com

Шабуров Андрей Сергеевич - кандидат технических наук, доцент кафедры «Автоматики и телемеханики», Пермский национальный исследовательский политехнический университет, г. Пермь. E-mail: shans@at.pstu.ru

About the authors

Shlykov Alexey Igorevich - student of the Department of Automation and Telemechanics. Perm National Research Polytechnic University, Perm. E-mail: thekingofthedas@gmail.com

Shaburov Andrey Sergeevich - Candidate of Technical Sciences, Associate Professor of the Department of Automation and Telemechanics. Perm National Research Polytechnic University, Perm. E-mail: shans@at.pstu.ru