УДК 004.94

ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ: ИСПОЛЬЗУЕМ АВТОМАТИЗИРОВАННЫЙ ИНСТРУМЕНТАРИЙ

Морозова Е.В., Слепынина М.М., Тюрпеко Е.С., студенты гр. ИБс-211
Научный руководитель: Медведев А.В.
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

ASSESSMENT OF THE INFORMATION SYSTEM'S SECURITY: IT IS USED AUTOMATED TOOLS

Morozova E.V., Slepynina M.M., Tyurpeko E.S.
Scientific supervisor: Medvedev A.V.
Kuzbass State Technical University
named after T.F. Gorbachev, Kemerovo

Аннотация: на основе модельных данных апробирован комплексный автоматизированный инструментарий для оценки информационной безопасности информационной системы предприятия с использованием программного комплекса многопараметрического анализа задачи линейного программирования. Обосновано, что предложенная совокупность инструментов – математическая модель и пакет прикладных программ – может рассматриваться, как основа для разработки системы поддержки принятия решений в сфере оценки информационной безопасности.

Abstract: on the basis of model data, a complex automated toolkit was tested for assessing the information security of an enterprise information system using a software package for multi-parameter analysis of a linear optimal control problem. It is substantiated that the proposed set of tools - a mathematical model and a package of applied programs - can be considered as the basis for developing a decision support system in the field of information security assessment.

Ключевые слова: информационная безопасность, система поддержки принятия решений, оптимизационная модель, пакет прикладных программ.

Key words: information security, decision support system, optimization model, software package.

В настоящее время информационные технологии оказывают колоссальное – как положительное, так и отрицательное – воздействие и на

развитие техники, и на развитие человека, неся в себе не только удобство и скорость обработки данных, числовых массивов и т.п., но и угрозы выхода из строя технических объектов, информационных систем органов государственного управления [1], а также влияя на поведение и принятие решений самим человеком. Все это делает актуальной проблему защиты информации или информационной безопасности (ИБ), а также автоматизированной оценки ее уровня. В случае информационных систем достаточно крупных организаций такая оценка сильно затруднена без использования методов математического моделирования и средств автоматизированной обработки входных данных модели.

В статье, с помощью описанного в [2] автоматизированного программного комплекса, проводится анализ уровня ИБ некоторой модельной информационной системы, например, производственного предприятия, с использованием математической модели [3], представляющей собой линейную оптимизационную задачу математического программирования. Использование этой модели дает возможность предприятию, занимающемуся оценкой информационной безопасности своих информационных систем, оперативно получить полезное знание об уровне их информационной защищенности, а также об оптимальных затратах на снижение рисков реализации информационных угроз в заданных экспертами n направлениях (например, сбои в работе систем связи из-за низкой квалификации сотрудников, отсутствия или устаревания программного или аппаратного обеспечения, переполнения или недозагрузки каналов связи и др.) ИБ. При этом используемая модель и алгоритмы ее анализа обеспечивают возможности рассмотрения практикоориентированного количества угроз.

В работе проводится вычислительный эксперимент на основе модельно задаваемых числовых характеристиках угроз ИБ. Рассмотрим данные характеристики [3]. Пусть весовые коэффициенты b_i (i=1,…,n) отражают относительные значимости i-й угрозы, p_i денежных единиц (д.е.) – стоимость затрат для достижения экспертно задаваемого, достаточного для информационной безопасности i-го направления защищенности (д.е.); $ZMAX_i$, $ZMIN_i$ (д.е.) – максимальные и минимальные уровни финансовых затрат, задаваемые менеджментом предприятия, на исключение i-й угрозы, Z (д.е.) – максимальная сумма затрат на уменьшение всех угроз ИБ. Предположим, что предприятие рассматривает три (n=3) конкретные угрозы своей информационной безопасности, соответствующие модельные характеристики которых представлены в таблице 1.

Таблица 1 – Характеристики угроз ИБ

i	p_i	b_i	*ZMINi*	*ZMAXi*
1	2, var	0,333	10	100
2	3	0,333	5	10
3	4	0,333	7	50

С использованием автоматизированных средств [2] анализа модели [3] проведем следующий вычислительный эксперимент. Построим зависимости уровня $J_{ИБ}$ информационной безопасности системы от параметров Z и p_1, причем вторую зависимость будем строить, исходя из результатов первой, которая отражает минимальный пороговый уровень затрат на обеспечение ИБ. Из первой зависимости выберем два значения – недостаточный уровень бюджетной обеспеченности и достаточный уровень соответственно. При указанных значениях построим графики $J_{ИБ}(p_1)$. Полученный результаты изображены на рисунках 1 и 2.

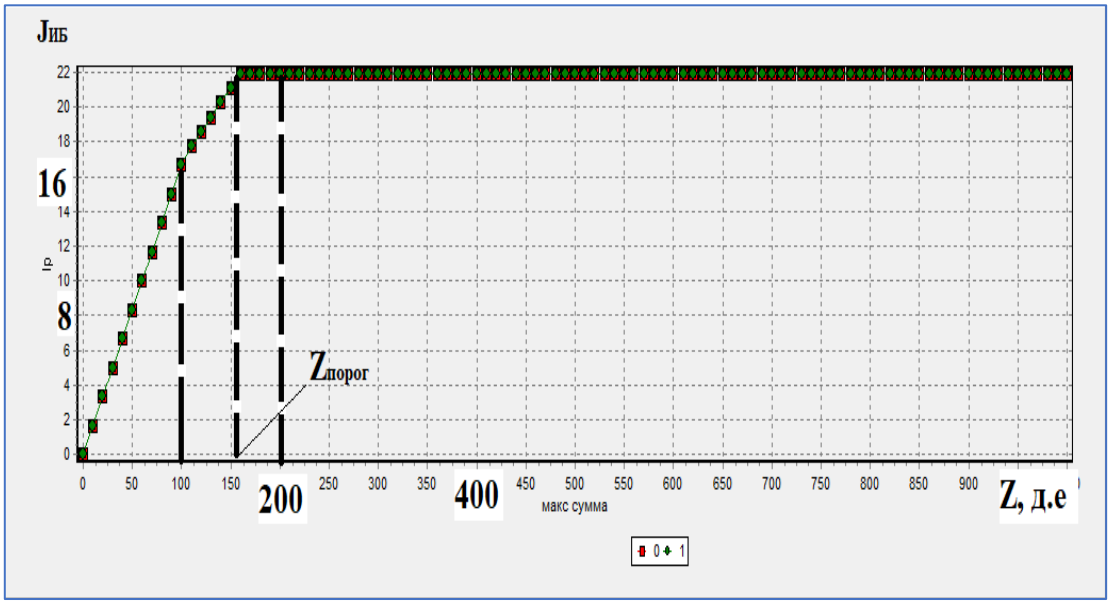

Рис.1 – Зависимость $J_{ИБ}(Z)$

Из рис.1 ИБ-аналитик может определить минимальный пороговый уровень затрат на обеспечение ИБ. Здесь он составляет Z≈160 д.е., при котором достигается максимальный уровень информационной защищенности $J_{ИБ}$≈22. Для построения зависимостей $J_{ИБ}(p_1)$ аналитик может выбрать значения недостаточного и достаточного уровней бюджетной обеспеченности Z, например, 100 и 200 д.е. соответственно.

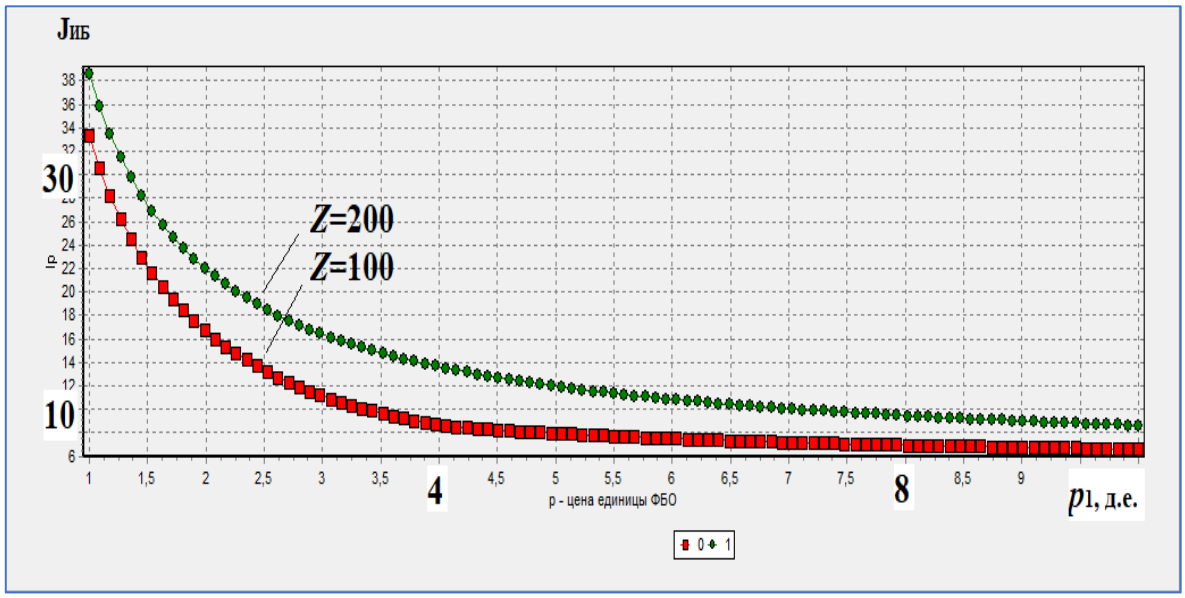

Рис.2 – Зависимости $J_{ИБ}(p_1)$ при недостаточном (Z=100) и достаточном (Z=200) уровнях бюджетной обеспеченности

Из рис.2 ИБ-аналитик может сделать следующие выводы:

1) уровень информационной безопасности информационной системы при достаточной бюджетной обеспеченности в среднем на 30% выше, чем в случае недостаточности бюджета;
2) увеличение параметра p_1 с 1 д.е. до 10 д.е. приводит к снижению уровня информационной безопасности системы приблизительно в диапазоне от 4.75 (при Z=200) до 5.7 (при Z=100) раз;

Очевидно, полученные результаты соответствует содержательной сути рассматриваемой задачи. При этом следует отметить, что приведенные данные ИБ-аналитик может получать оперативно, проводя многопараметрический анализ задачи, а совокупность оптимизационной модели ИБ, эффективных алгоритмов ее решения (симплекс-метод) и автоматизированный пакет прикладных программ позволяют рассматривать представленный инструментарий, как системно-аналитическую базу для поддержки принятия решений в сфере обеспечения ИБ не только предприятий, но и других технических и социально-экономических систем.

Список литературы

1. Медведев А.В. Об информационной безопасности автоматизированных комплексов социально-экономического анализа / А.В. Медведев, А.Г. Киренберг, Е.В. Прокопенко // Экономика и управление инновациями. – 2020. – №2(13). – С.37-44. – DOI 10.26730/2587-5574-2020-2-37-44.
2. Медведев А.В. Автоматизированная поддержка принятия оптимальных решений в инвестиционно-производственных проектах развития социально-экономических систем / А.В. Медведев. – Москва: Издательский Дом «Академия Естествознания», 2020. – 200 с. – DOI 10.17513/np.421.

3. Киренберг А.Г. К экономико-математическому моделированию и автоматизированному анализу защищенности информационных систем / А.Г. Киренберг, А.В. Медведев, Е.В. Прокопенко // Национальная безопасность России: актуальные аспекты: сборник избранных статей Всероссийской научно-практической конференции. – СПб: ГНИИ «Нацразвитие», 2022. – С.5-8.