«Применение математики в экономических исследованиях», М: Соцгиз, 1959).

3. Рациональный раскрой промышленных материалов / Л.В. Канторович, В.А. Залгаллер. – Новосибирск: Наука СО, 1971. – 320 с.

4. Dyckhoff, H. A typology of cutting and packing problems / H. Dyckhoff // European Journal of Operation Research. – 1990. – Vol. 44. – P. 145-159.

5. ESICUP – URL: https://www.euro-online.org/websites/esicup/.

6. Чеканин В.А. Развитие методов решения задач плотной упаковки объектов произвольной формы и различной размерности: дисс. на соискание ученой степени докт. техн. наук: 05.01.01 – Московский государственный технологический университет «СТАНКИН», 2021, – 435 с.

7. Роджерс Д., Адамс Дж. Математические основы машинной графики. – М.: Мир, 2001. – 604 с.

УДК 004.02

А.С. Ромыш, маг.; Н.Н. Пустовалова, доц.
(БГТУ, г. Минск)

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ И СТРУКТУРА СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

Высокая степень точности оценки рисков информационной системы (ИС) важна не только для внутренних целей организации, но и при взаимодействии с представителями внешних организаций, таких как аудиторы надзорных органов и сотрудники страховых компаний. Страховые компании могут быть заинтересованы в завышении оценочной стоимости рисков ИС с целью повышения доходности, а надзорные органы с целью снятия с себя ответственности в случае возможных инцидентов в подотчетных организациях.

Функциональная модель процесса управления информационными рисками, основана на применении SADT-методологии, которая представляет собой совокупность методов, правил и процедур, предназначенных для построения функциональной модели объекта какой-либо предметной области. Использование этой методологии позволяет обоснованно выбрать состав и функции основных этапов анализа и управления рисками добровольного страхования медицинских рисков.

Описание функциональных подсистем. Идентификация рисков − формирование перечня ресурсов, выделение групп ресурсов, выделение опасных состояний для ресурсов.

Предварительная оценка рисков − выделение опасных состояний

(ОС) для управления.

Разрабатываемая система управления информационными рисками состоит из девяти модулей, описание которых приведено ниже.

Модуль «Классификация рисков» представляет собой группировку рисков по частоте возникновения и размеру ущерба, выделение рисков для дальнейшего анализа и управления. Входные данные: предварительные экспертные оценки вероятностей реализации опасных состояний, предварительные оценки потенциальных ущербов; выходные данные: качественная оценка значимости опасных состояний.

Модуль «Алгоритм Мамдани» − предварительная оценка уровня рисков опасных состояний на основе алгоритма Мамдани [1]. Входные данные: оценка вероятности реализации ОС, правила вывода, оценки потенциальных ущербов, экспертные данные для построения функций принадлежности; выходные данные: значимость опасных состояний.

Модуль «Отказы ПО» − оценка вероятности отказов программного обеспечения (ПО) на разных этапах тестирования и эксплуатации на основе модели Коркорэна [3]. Входные данные: временные ряды различных типов отказов ПО; выходные данные: вероятности отказов разрабатываемого ПО.

Модуль «Предварительная оценка ущерба» − оценка ущерба для опасных состояний как связанных, так и не связанных с нарушением конфиденциальности. Входные данные: потеря или временная недоступность ресурса, сочетание потери ресурса и отсутствие резервной копии ресурса, аппаратный отказ ресурса, сбой или отказ ПО, прямые расходы, косвенные расходы, упущенная выгода; выходные данные: величина ущерба.

Модуль «Оценка морального ущерба» − оценка компенсации морального ущерба [2] в случае нарушения конфиденциальности данных. Входные данные: максимальная сумма выплат, критерии по которым возможна оценка ситуаций, шкалы, экспертные данные; выходные данные: реальная сумма выплат.

Модуль оценки интегрального риска и построение рейтинга угроз − оценка риска опасных состояний на основе ЛВМ. Оценка значимости угроз в рамках одного опасного состояния, построение рейтинга угроз в рамках всей совокупности опасных состояний. Входные данные: вероятности элементарных угроз, величины ущерба реализации ОС, сценарий ОС; выходные данные: вероятность реализации ОС, уровень риска ОС, уровень риска ИС. На первом шаге для каждого опасного состояния «высокой» значимости строится сценарий.

Модуль выбора контрмер − разбиение контрмер на классы и упорядочивание контрмер в каждом классе, решение задачи формирования

перечня наиболее эффективного набора контрмер для заданного бюджетного ограничения. Входные данные: стоимость контрмер, эффективность контрмер для каждой из элементарных угроз, размер бюджета на ИБ; выходные данные: эффективный набор контрмер, уровень риска ИС с учетом контрмер.

Модуль оценки эффективности − подсчет уровня риска с учетом контрмер, подсчет показателя эффективности решения задачи управления рисками. Входные данные: уровень риска ИС до внедрения контрмер, уровень риска ИС с учетом контрмер; выходные данные: эффективность решения задачи управления ИР для ИС.

Модуль страхования − выбор рисков (опасных состояний) для страхования, расчет страховой премии и страховой. В случае индивидуального страхования входные данные: вероятность, ущерб, нагрузка; выходные данные: брутто-премия, страховая сумма, рекомендация на страхование. В случае массового страхования входные данные: вероятность наступления страховых случаев, ущерб, средние страховые суммы, средние выплаты, нагрузка; выходные данные: брутто-премия, рекомендации на страхование.

На рис. 1 представлен первый уровень функциональной модели системы с точки зрения разработчика.

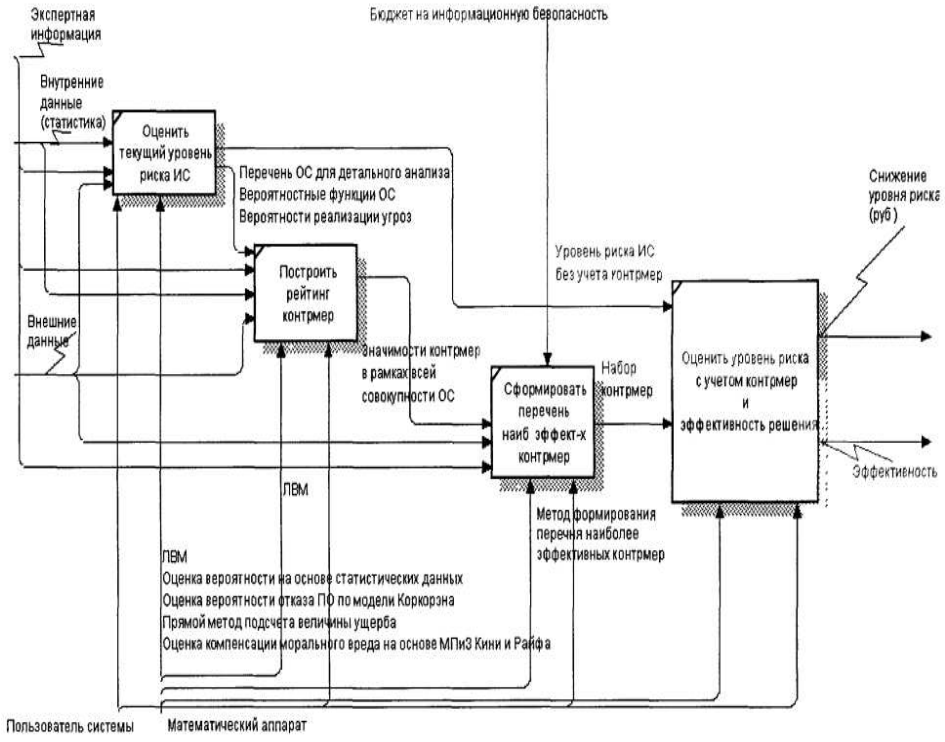

Рисунок 1 – Первый уровень функциональной модели системы

Таким образом, задачу оценки риска информационной системы в целом можно разбить на следующие этапы:

− описание структуры ресурсов информационной системы;

− описание множества опасных состояний ресурсов информационной системы;

− оценка вероятностей реализации опасных состояний, в том числе выявление меры влияния угроз на реализацию опасных состояний;

− оценка стоимости потерь от реализации опасных состояний.

На рис. 2 представлена структура всей системы управления информационными рисками.

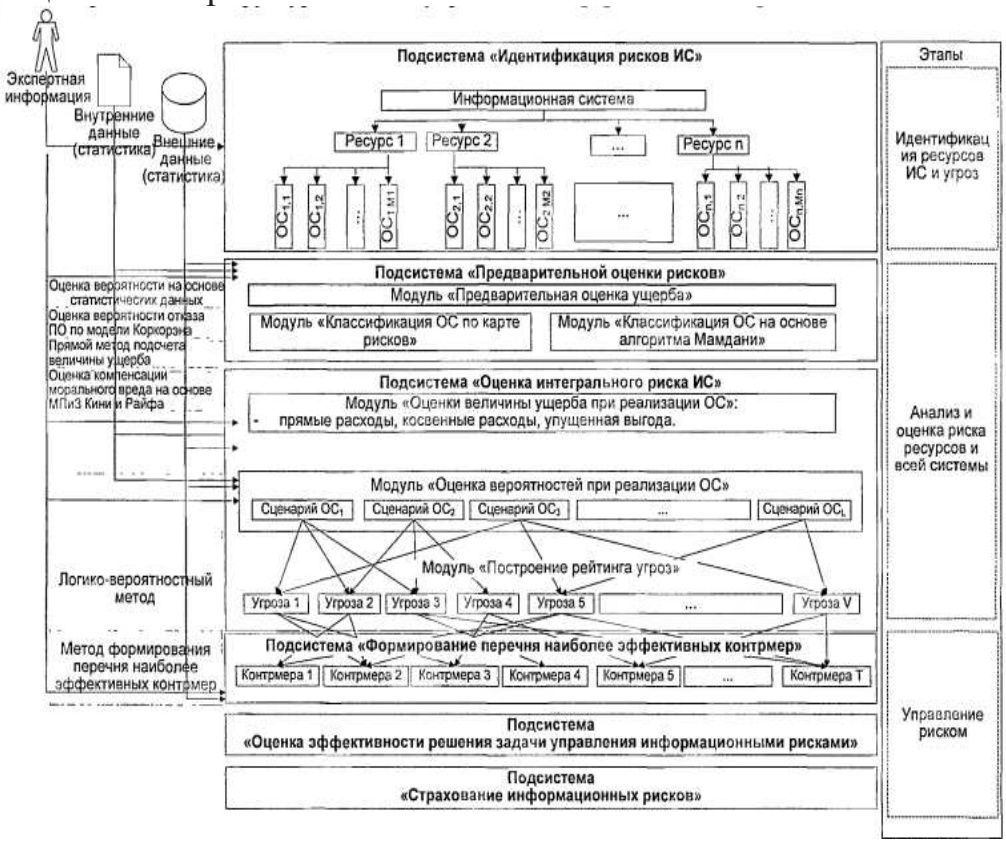

Рисунок 2 − Структура системы управления информационными рисками

В качестве дальнейшего развития системы управления информационными рисками предполагается разработка системы управления политикой безопасности, реализующей положения о стандартизации в области персональных данных.

ЛИТЕРАТУРА

1. Пегат А. Нечеткое моделирование и управление. − М.: Бином. Лаборатория знаний, 2009. – 798 с.

2. Север А.С., Пустовалова Н.Н. Методика подсчета размера компенсации морального ущерба // Модернизация и трансформация научной деятельности в условиях цифровизации: сборник статей междун. научно-практ. конф. 7 октября 2024 г. – Таганрог: МЦИИ ОМЕГА САЙНС. – 2024. – С. 16−18.

3. Семахин А.М. Методы верификации и оценки качества программного обеспечения: учебное пособие. – Курган: КГУ, 2018. – 150 с.