УДК 004.056

Головкова Елена Александровна,
к.т.н., доцент, Ангарский государственный технический университет,
e-mail: temnikova_ea@bk.ru

РАЗРАБОТКА ПРОГРАММЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КОНФИГУРАЦИИ 1С: ПРЕДПРИЯТИЕ 8.3

Golovkova E.A.

DEVELOPMENT OF AN INFORMATION MANAGEMENT PROGRAM SECURITY IN THE 1C: ENTERPRISE 8.3 CONFIGURATION

Аннотация. Представлен комплексный подход управления информационной безопасностью в виде процессов на диаграмме декомпозиции модели IDEF0. Анализ возможного ущерба информационным активам рекомендовано осуществлять по двум группам критериев с привлечением экспертов, опираясь на качественные шкалы. Экспертный анализ угроз информационной безопасности и уязвимостей, через которые они могут быть реализованы, предложено проводить в совокупности с применением качественных шкал, учитывая наличие в организации внедренных механизмов контроля. Результаты проведенного анализа выражены в виде суммарного уровня группы уязвимостей. Построена матрица определения величины риска информационной безопасности. Полученные качественные оценки сопоставлены с количественным показателем среднегодового ущерба и откалиброваны. В качестве маркера эффективности защитных механизмов, предлагается выбрать коэффициент возврата инвестиций. С целью повышения эффективности и удобства проведения экспертной оценки рисков информационной безопасности, автоматизации обработки результатов, полученных в ходе экспертизы, а также расчётов, на которые может опираться лицо, принимающее решение, была создана программа в конфигурации 1С: Предприятие 8.3.

Ключевые слова: риск-ориентированный подход, информационная безопасность, оценка возврата инвестиций.

Abstract. An integrated approach to information security management is presented in the form of processes on the decomposition diagram of the IDEF0 model. The analysis of possible damage to information assets is recommended to be carried out according to two groups of criteria with the involvement of experts, based on qualitative scales. Expert analysis of information security threats and vulnerabilities through which they can be implemented is proposed to be carried out in conjunction with the use of qualitative scales, taking into account the presence of implemented control mechanisms in the organization. The results of the analysis are expressed in the form of the total level of the vulnerability group. A matrix for determining the magnitude of information security risk is constructed. The obtained qualitative estimates are compared with the quantitative indicator of the average annual damage and calibrated. As a marker of the effectiveness of protective mechanisms, it is proposed to choose the return on investment ratio. In order to increase the efficiency and convenience of conducting an expert assessment of information security risks, automating the processing of the results obtained during the examination, as well as calculations on which the decision-maker can rely, a program was created in the configuration 1C: Enterprise 8.3.

Keywords: risk-based approach, information security, return on investment assessment.

В связи с глобализацией, возрастающей конкуренцией, стремительным развитием информационных технологий, увеличением объёма данных, которыми необходимо управлять, в значительной степени возросло внимание к проблемам информационной безопасности (ИБ).

Информация, являющаяся одним из ключевых ресурсов хозяйствующего субъекта, зачастую подвержена рискам ИБ [1]. Недобросовестные сотрудники, конкуренты, злоумышленники стараются завладеть ценными данными, стремясь нанести значительный репутационный, материальный ущерб или привести к полному банкротству организации. Поэтому управление рисками (УР) ИБ организации очень актуально.

Существует три ключевых свойства информации при управлении ИБ [2]: конфиденциальность (к), целостность (ц) и доступность (д).

Основные подходы управления ИБ представлены на рисунке 1.

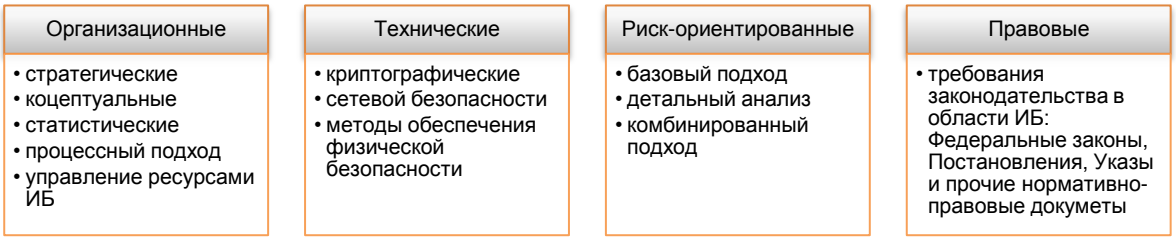

Рисунок 1 – Подходы управления ИБ

Процесс УРИБ можно представить в виде IDEF0-диаграммы, представленной на рисунке 2.

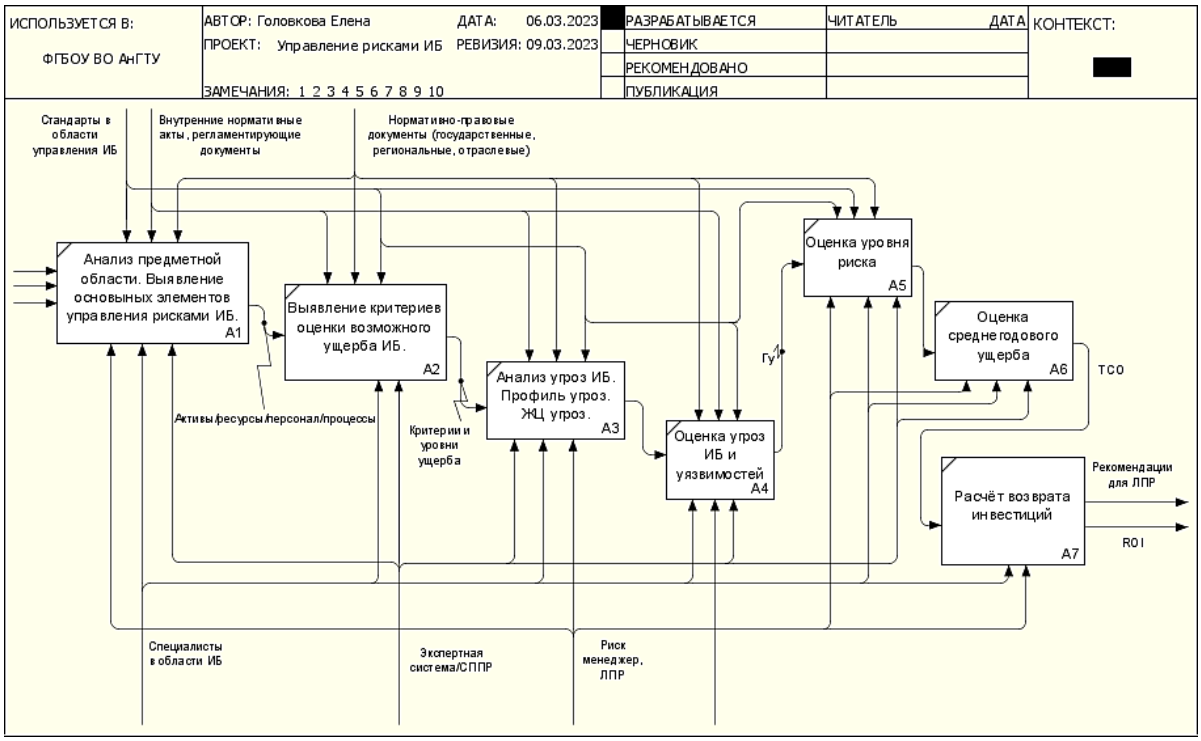

Рисунок 2 – Диаграмма декомпозиции процесса управления рисками ИБ

Этапы комплексного риск-ориентированного подхода. 1 этап: анализ факторов риска является ключевым при принятии оптимальных решений по их обработке. К ним относятся активы организации (см. рисунок 3), возможный ущерб от реализации угроз, уязвимости, механизмы контроля, размер среднегодовых потерь (ALE) и возврат инвестиций (ROI).

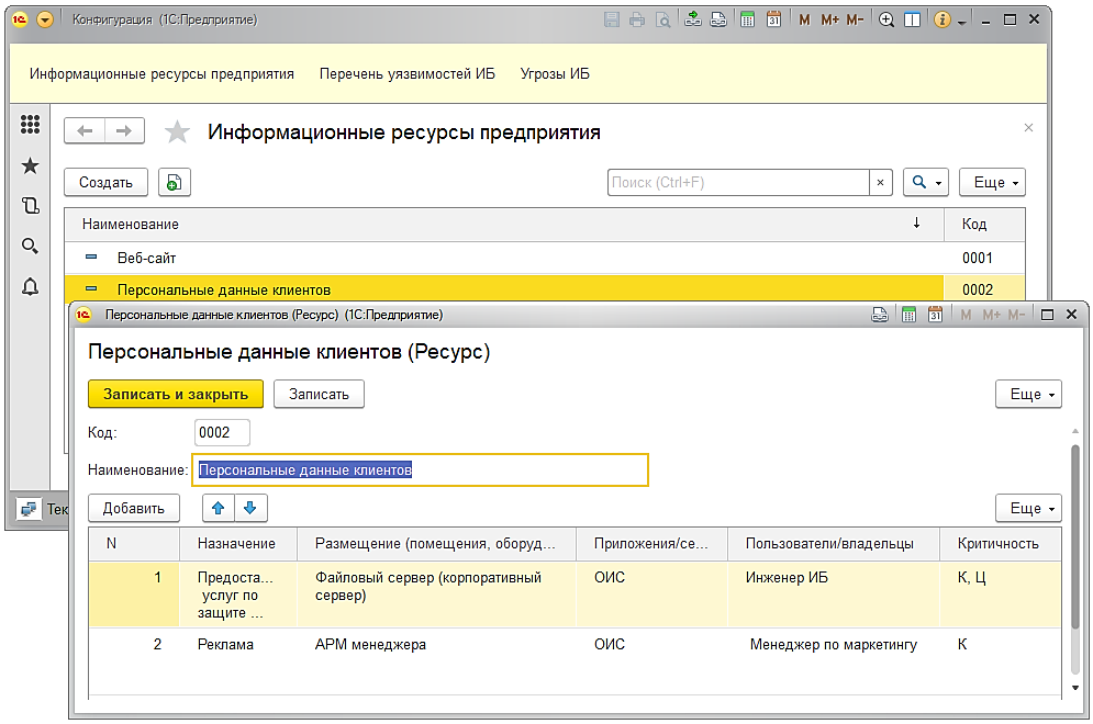

Рисунок 3 – Классификация информационных ресурсов

2 этап: анализ возможного ущерба. Выделим две основные группы критериев: ущерб коммерческим (У1) и репутационным (У2) интересам организации. Шкалы с уровнями ущерба представлены на рисунках 4, 5.

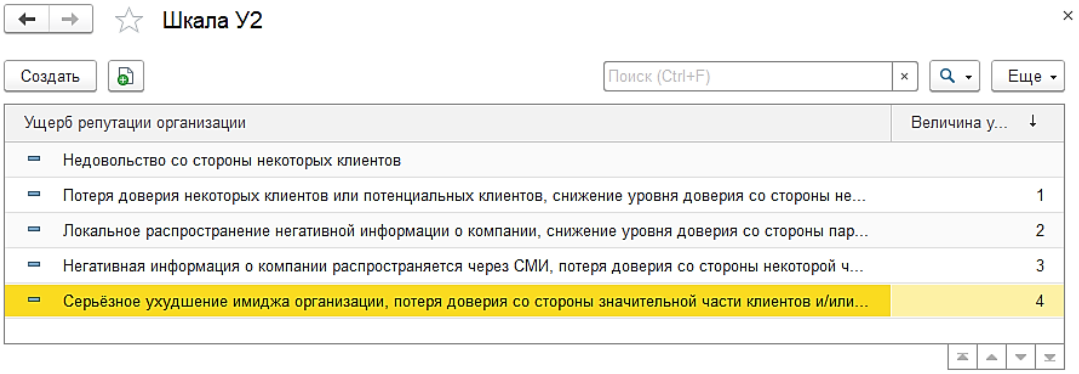

Рисунок 4 – Пятибалльная качественная шкала У2

3 этап: анализ возможных угроз ИБ в отношении активов организации и нежелательных инцидентов, приводящих к ущербу; описание профиля и жиз-

ненного цикла угроз. На рисунке 6 представлен фрагмент иерархического справочника с перечнем угроз, которым руководствуется эксперт при анализе.

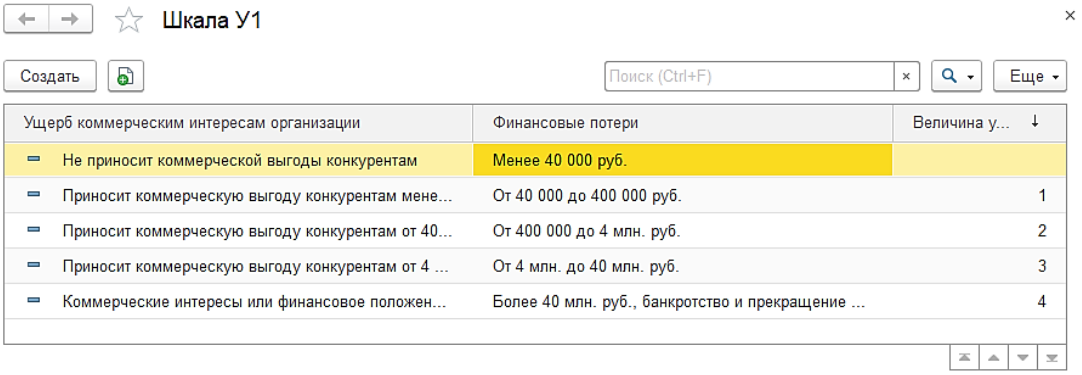

Рисунок 5 – Пятибалльная количественная шкала У1

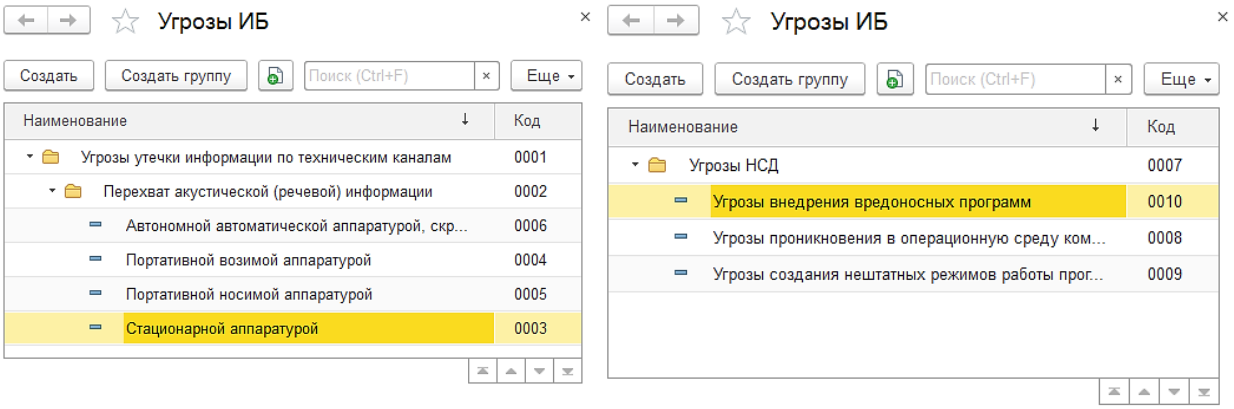

Рисунок 6 – Фрагмент справочника Угрозы ИБ

Анализ уязвимостей (фрагмент перечня которых представлен на рисунке 7), ассоциированных с активами организации. Уязвимость является условием, позволяющим угрозе реализоваться, поэтому оценку угроз и уязвимостей предлагается осуществлять в совокупности.

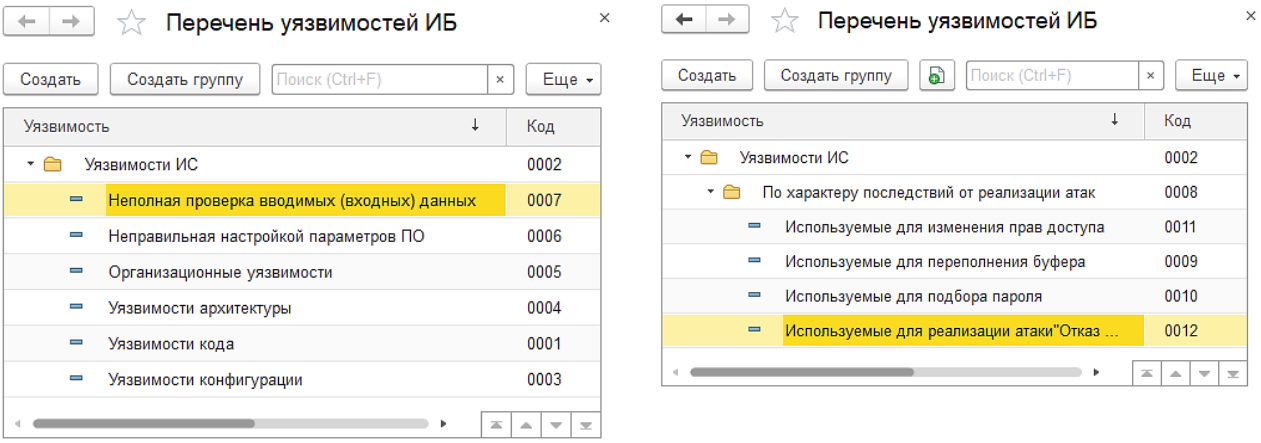

Рисунок 7 – Фрагмент справочника с перечнем уязвимостей

Рассмотрим организацию, стоимость бизнеса которой равна 40 млн. руб.

Информационными активами, для которых будет проводиться анализ угроз и уязвимостей, являются веб-сайт (Р1) и техническая документация заказчика (Р2).

В соответствии с критериями У1 и У2, определяется ценность актива:

Р1: (К) – х (Ц) – 3 (Д) – 2;

Р2: (К) – 4 (Ц) – 4 (Д) – х.

Для расчета суммарного уровня группы уязвимостей ГУ необходимо ориентироваться на уровни РРУ, РУУ и РМК, представленные на рисунке 8. Найдем ГУ по формуле:

$$\Gamma_{\text{У}} = \sum_{i=1}^{n} \text{Р}_{\text{уу}} - \sum_{i=1}^{n} \text{Р}_{\text{МК}}.$$

Вероятность реализации угроз ($Р_{РУ}$)

- Н – низкая вероятность (раз в 5-10 лет);
- НС – вероятность ниже среднего (раз в 2-3 года);
- С – средняя вероятность (раз в год);
- ВС – вероятность выше среднего (раз в квартал);
- В – высокая вероятность (каждый день).

Уровни уязвимости ($Р_{УУ}$)

- Н – вероятность успешной реализации угрозы 0 – 0,1;
- НС – вероятность успешной реализации угрозы 0,3;
- С – вероятность успешной реализации угрозы 0,5;
- ВС – вероятность успешной реализации угрозы 0,7;
- В – вероятность успешной реализации угрозы 0,9 – 1.

Уровени механизмов контроля ($Р_{МК}$)

- Н – вероятность обхода м.к. 0,9 – 1;
- НС – вероятность обхода м.к. 0,7;
- С – вероятность обхода м.к. 0,5;
- ВС – вероятность обхода м.к. 0,3;
- В – вероятность обхода м.к. 0 – 0,1.

Рисунок 8 – Качественные шкалы для расчета суммарного уровня группы уязвимостей

4 этап: определение величины риска (ВР) по матрице [3], представленной на рисунке 9. ВР от 0-4 соответствует низкому уровню риска; 5-8 – среднему; 9-12 – высокому.

Информационные ресурсы предприятия | Перечень уязвимостей ИБ | Угрозы ИБ | Шкала У1 | Шкала У2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	Стоимость ресурса	Уровень угрозы																								
2		Н					НС					С					СВ					В				
3		Уровень уязвимости																								
4		Н	НС	С	ВС	В	Н	НС	С	ВС	В	Н	НС	С	ВС	В	Н	НС	С	ВС	В	Н	НС	С	ВС	В
5	0	0	1	2	3	4	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8
6	1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
7	2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
8	3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
9	4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12

Рисунок 9 – Матрица величин риска

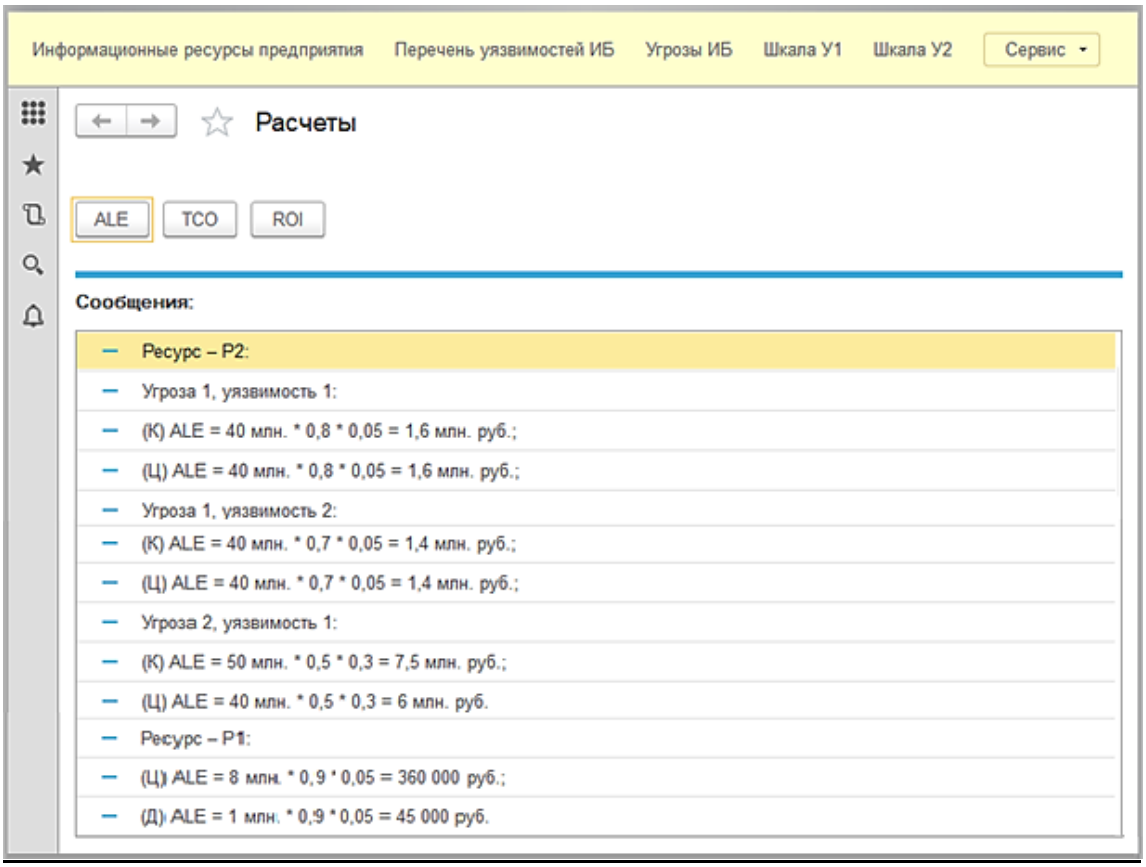

Рисунок 10 – Результаты расчетов ALE для Р1 и Р2

Определение величины риска активов Р1 и Р2:

для Р2 (техническая документация заказчика):

- угроза 1, уязвимость 1: (К) ВР = 5 (Ц) ВР = 5 (Д) = х.
- угроза 1, уязвимость 2: (К) ВР = 4 (Ц) ВР = 4 (Д) = х.
- угроза 2, уязвимость 1:(К) ВР = 8 (Ц) ВР = 8 (Д) = х.

для Р1 (веб-сайт):

- угроза 3, уязвимость 1: (К) ВР = х (Ц) ВР = 3 (Д) = 2.

5 этап: определение среднегодового ущерба по формуле:

$$\mathrm{ALE} = \mathrm{P_У} \cdot \mathrm{k} \cdot \mathrm{P_{РУ}},$$

где РУ – размер ущерба; k – количество инцидентов в год; РРУ – вероятность успешной реализации угрозы.

Полученные значения, представленные на рисунке 10, можно сравнить со значениями откалиброванной шкалы.

Цель обработки риска – выбор эффективных механизмов, сокращающих среднегодовые потери организации от инцидентов ИБ при максимальном возврате инвестиций.

6 этап: рассчитаем ROI по формуле:

$$\mathrm{ROI} = \frac{\mathrm{ALE} - \mathrm{TCO}}{\mathrm{TCO}} \cdot 100\ \%,$$

где TCO – стоимость защитных механизмов, которая рассчитывается по

формуле: TCO = ПР + К1 + К2, где К1, К2– косвенные затраты первой и второй групп, ПР – сумма капитальных затрат и расходов на управление.

Посчитано, что затраты организации в год на охранные мероприятия составили 3 млн. руб., на сотрудников внутренней ИБ – 4,5 млн. руб., на обновление программных средств защиты – 1,5 млн. руб., дополнительные расходы – 300 000 руб. Приняв ALE = 19,9 млн. руб., рассчитаем ROI. Результаты автоматизированных расчетов представлены на рисунке 11.

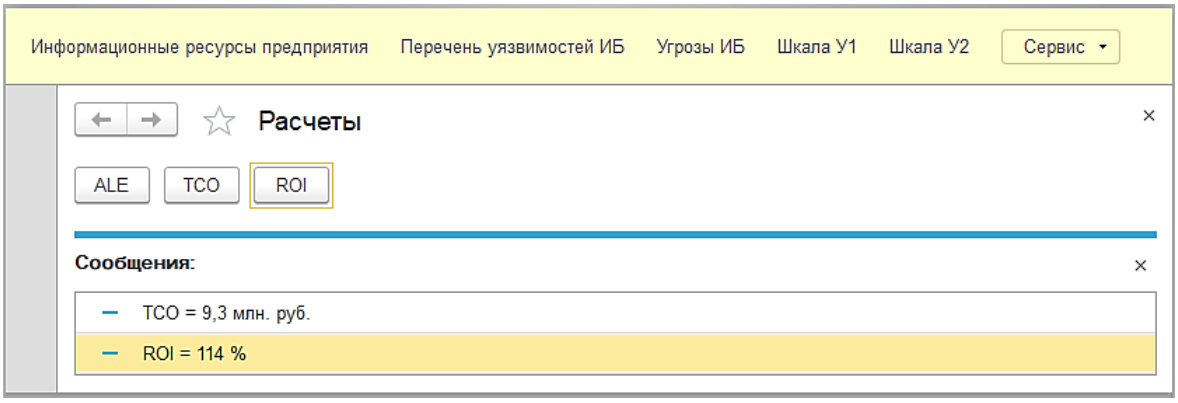

Рисунок 11 – Результаты расчета TCO и ROI

ROI > 100 % свидетельствует о том, что затраты на ИБ окупились, есть прибыль от вложений (ROI = 100 % – это точка безубыточности, 0 < ROI < 100 % – возвращается часть затрат).

В дальнейших исследованиях планируется провести регрессионный анализ эффективности мер защиты информации, проанализировать частоту попыток реализации угроз и уязвимостей, наиболее подверженных им, и оптимизировать экспертную систему управления рисками ИБ.

ЛИТЕРАТУРА

1. **Темникова, Е. А.** Обзор систем оценки и управления рисками информационной безопасности / Е. А Темникова, Е. А Павлова. – Текст : непосредственный // Информационные технологии и проблемы математического моделирования сложных систем. – 2017. – Вып. 18. – С. 33-39.

2. **Дорофеев, А. В.** Менеджмент информационной безопасности: основные концепции / А. В. Дорофеев. – Текст : непосредственный //Вопросы кибербезопасности. – 2014. – № 1(2). – С. 67-73.

3. **Краковский, Ю. М.** Выбор и ранжирование компетенций персонала, обслуживающего информационную систему с конфиденциальной информацией / Ю. М. Краковский, К. В. Затрутина. – Текст : непосредственный // Молодая наука Сибири: электрон. науч. журн. 2021. – №1(11). – URL: http://mnv.irgups.ru/toma/111-2021