УДК 004.056

К. К. Мартыненко[1], А. В. Ценина[1], В. В. Селифанов[1]*

Оценка эффективности модели обработки рисков

[1] Новосибирский государственный технический университет, г. Новосибирск, Российская Федерация
* e-mail: k.martynenko.2019@stud.nstu.ru

Аннотация. В статье рассмотрена оценка эффективности модели управления рисками. Были проанализированы нормативные правовые акты, определяющие неприемлемые риски для информационных систем различных типов, а также национальные стандарты, рассматривающие вопрос обработки рисков. На основе изученной информации была составлена блок-схема процесса управления рисками на всех этапах жизненного цикла информационной системы. Был выполнен анализ методов моделирования, исходя из которого для реализации модели процесса было выбрано имитационное моделирование. В среде моделирования AnyLogic была реализована модель процесса обработки рисков, выполнен обзор логических блоков модели. Выделены критерии, на основе которых была проведена оценка эффективности. Получены статистические данные, позволяющие оценить эффективность разработанной модели. Сделаны выводы об эффективности разработанной модели процесса обработки рисков.

Ключевые слова: система защиты, управление рисками, анализ рисков, оценка рисков, имитационное моделирование, модель, итерация, контекст среды, нейтрализация рисков, принятие рисков, оценка эффективности

K. K. Martynenko[1], A. V. Tsenina[1], V.V. Selifanov[1]*

Evaluating the effectiveness of the risk processing model

[1] Novosibirsk State Technical University, Novosibirsk, Russian Federation
* e-mail: k.martynenko.2019@stud.nstu.ru

Abstract. The article considers the assessment of the effectiveness of the risk management model. Regulatory legal acts defining unacceptable risks for information systems of various types, as well as national standards considering the issue of risk processing were analyzed. On the basis of the studied information a block diagram of the risk management process at all stages of the information system life cycle was drawn up. The analysis of modelling methods was performed, on the basis of which simulation modelling was chosen to implement the process model. In AnyLogic modelling environment the model of the process of risk processing was implemented, the review of logical blocks of the model was performed. Criteria were identified, on the basis of which the efficiency assessment was carried out. Statistical data allowing to estimate the efficiency of the developed model were obtained. Conclusions about the effectiveness of the developed model of the risk processing process are made.

Keywords: protection system, risk management, risk analysis, risk assessment, simulation modelling, model, iteration, environmental context, risk neutralization, risk acceptance, performance evaluation

Введение

Построение системы защиты, включая систему оценки рисков и управления ими для их нейтрализации – необходимый этап для создания функционирующей

информационной системы. Однако в устоявшемся подходе к построению системы защиты процесс оценки рисков и управления ими практически не учитывается, так как описан в основном в национальных стандартах, требования которых не обязательны к исполнению. При этом риски тесно связаны с угрозами и уязвимостями, на нейтрализацию которых направлены меры защиты, а значит не могут не быть учтены при обеспечении безопасности информации.

В ходе исследования были изучены публикации, рассматривающие различные подходы к управлению рисками: «Вопросы оценки доверия к системе управления рисками» [1], «Вопросы управления рисками управления решениями защиты информации» [2], «Метод оценивания рисков в системах принятия решений с учетом защиты информации» [3]. В приведенных исследованиях не рассмотрен в полной мере комплексный подход к управлению рисками в информационных системах различных типов.

Цель исследования – разработать систему обработки рисков, учитывающую требования к информационным системам на протяжении всего жизненного цикла и оценить ее эффективность. Для достижения цели требовалось выполнить следующие задачи:

– провести анализ нормативной правовой базы, устанавливающей требования к определению рисков безопасности информации;

– определить требования, которым должна отвечать система обработки рисков;

– разработать прототип (блок-схему) процесса обработки рисков;

– изучить методы моделирования процессов;

– построить модель процесса обработки рисков на основе разработанной блок-схемы;

– выделить критерии оценки эффективности процесса управления рисками;

– провести оценку эффективности разработанной модели и сделать выводы на основе полученных результатов.

Исследование направлено на выявление эффективного подхода к управлению рисками в различных информационных системах и его результаты могут применяться при обеспечении защиты информации в различных организациях.

Методы и материалы

В ходе исследования использовались требования нормативных правовых актов [4–7], определяющих неприемлемые риски для различных типов информационных систем [8–10]. Для определения рисков безопасности информации на этапе эксплуатации информационной системы использовались стандарты по системной инженерии на основе ГОСТ Р 57193-2016 (рис. 1) [11, 12].

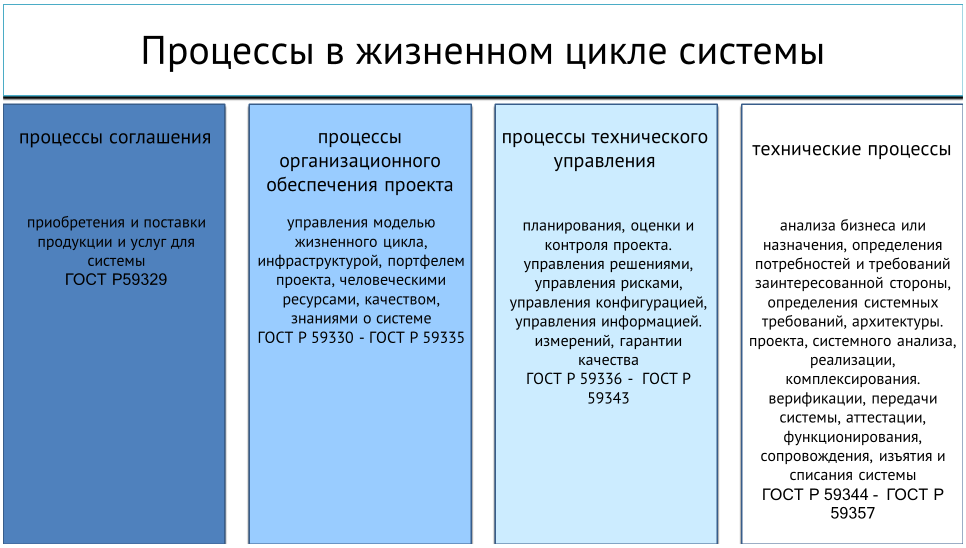

Рис. 1. Перечень государственных стандартов по системной инженерии, распределённых по процессам в жизненном цикле системы

Для построения системы управления рисками использовались материалы проекта национального стандарта ГОСТ Р ИСО/МЭК 27005-2022 [13], в частности схема процесса управления рисками. Были задействованы четыре варианта обработки рисков:

– избегание риска (принятие решения о прекращении деятельности, провоцирующей риск);

– изменение риска (изменение вероятности возникновения нежелательных событий и последствий или серьёзности ущерба при реализации данных событий);

– сохранение рисков (временное принятие выгод и издержек от риска);

– разделение риска (распределение ответственности через привлечение других сторон как внутри организации, так и вне неё).

В качестве способа моделирования было выбрано имитационное, в рамках которого создаётся модель системы (фактически её «цифровой двойник»), в которой с достаточной точностью был описан данный процесс [14].

В качестве инструмента моделирования и оценки эффективности было выбрано AnyLogic – российское программное обеспечение для моделирования (в том числе имитационного) [15], которое позволяет рассматривать различные бизнес-процессы и оценивать возможности по их оптимизации [16].

Были выделены параметры модели, полезные для изучения процесса:

– время задержки;

– вероятность распределения агентов между возможными вариантами дальнейшей обработки.

Для оценки эффективности модели использовались следующие формулы [17]:

1. Показатель эффективности управления защитой информации $W_э$, определяемый как вероятность своевременного принятия и применения правильного решения, которое обеспечивает оптимальное использование возможностей контролируемых технических средств, определяется по формуле (1):

$$W_э = P_{св.сб} \cdot P_{пр} \cdot P_{св.пр} \cdot P_{пр.р}, \quad (1)$$

где $P_{св.сб}$ – вероятность своевременного сбора всего объёма требуемой информации для принятия решений, $P_{пр}$ – вероятность правильного принятия решений, $P_{св.пр}$ – вероятность своевременного и правильного принятия решений, $P_{св.р}$ – вероятность своевременной реализации принятых решений.

2. Вероятность правильного принятия решений $P_{пр}$ вычисляется по формуле (2):

$$P_{пр} = \frac{1}{M}\sum_{j=1}^{M}\frac{S_{пр.j}}{L_j}, \quad (2)$$

где M – число рассматриваемых ситуаций, L_j – количество принимающих решения лиц в работе для j-й ситуации, $S_{пр.j}$ – число правильно принятых решений для j-й ситуации [18].

3. Вероятность своевременного и правильного принятия решений $P_{св.пр}$ рассчитывается по формуле (3):

$$P_{св.пр} = \frac{1}{M}\sum_{j=1}^{M}\frac{R_j}{S_{пр.j}}, \quad (3)$$

где R_j – число своевременно и правильно принятых для j-й ситуации решений, определяемое по формулам (4) и (5):

$$R_j = \sum_{i=1}^{L} R_{ij}, \quad (4)$$

$$\begin{cases} R_{ij} = 1, \text{если } t_{ij} \le t_{доп} \\ R_{ij} = 0, \text{если } t_{ij} > t_{доп} \end{cases}, \quad (5)$$

где t_{ij} – текущее значение времени, которое было потрачено на принятие решения i-м лицом, принимающим решение, в j-й ситуации, $t_{доп}$ – допустимое время принятия решения.

5. Вероятность своевременной реализации принятых решений $P_р$ рассчитывается по формуле (6):

$$P_{пр.р} = \frac{1}{Q \cdot M}\sum_{j=1}^{M}\frac{C_j}{R_j}, \quad (6)$$

где C_j – число своевременно реализованных правильных принятых решений для j-й ситуации, определяемое по формулам (7) и (8), Q – число направлений связи, соответствующее числу исполнителей.

$$C_j = \sum_{q=1}^{Q} C_{qj}, \quad (7)$$

$$\begin{cases} C_{qj} = 1, \text{если } t_{qj} \le t_{\text{доп.р.}} \\ C_{qj} = 0, \text{если } t_{qj} > t_{\text{доп.р.}} \end{cases}, \quad (8)$$

где t_{qj} – текущее значение времени, которое было потрачено на реализацию правильно и своевременно принятых решений в j-й ситуации, $t_{\text{доп.р.}}$ – допустимое время реализации принятого решения [19].

5. При проведении N оптов математическое ожидание правильности принимаемого решения $\widetilde{P_{\text{пр}}}$ вычисляется по формуле (9), а дисперсия случайной величины для оценки точности полученных результатов – по формуле (10)

$$\widetilde{P_{\text{пр}}} = \frac{1}{N} \sum_{n=1}^{N} P_{\text{пр}.n}, \quad (9)$$

$$\sigma^2(P_{\text{пр}}) = \sum_{n=1}^{N} \left(P_{\text{пр}.n} - P_{\text{пр}}\right)^2 / N - 1, \quad (10)$$

где $P_{\text{пр.n}}$ – выборка значений правильности принимаемых решений в N опытах [20].

Результаты

Была разработана блок-схема процесса управления рисками (рис. 2).

На основе блок-схемы в AnyLogic была разработана модель процесса обработки рисков (рис. 3).

Пример расчёта оценки эффективности представлен в таблице 1

Обсуждение.

Создание модели процесса обработки рисков позволяет проанализировать работу во времени и проводить оптимизационные мероприятия, в том числе на основе данных по оценке эффективности. При расчёте оценки эффективности стоит отметить, что показатель уменьшается при увеличении количества рассматриваемых ситуаций.

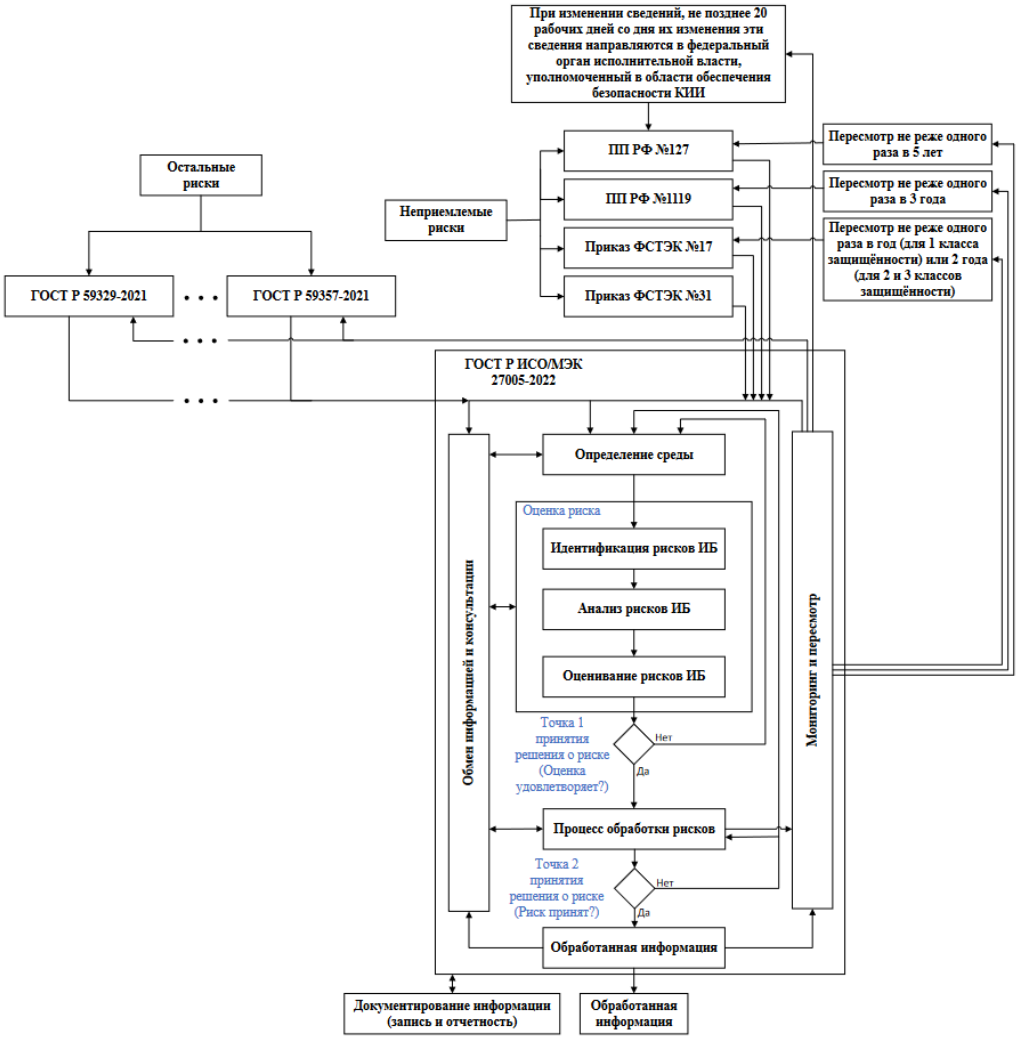

Рис. 2. Схема обработки рисков

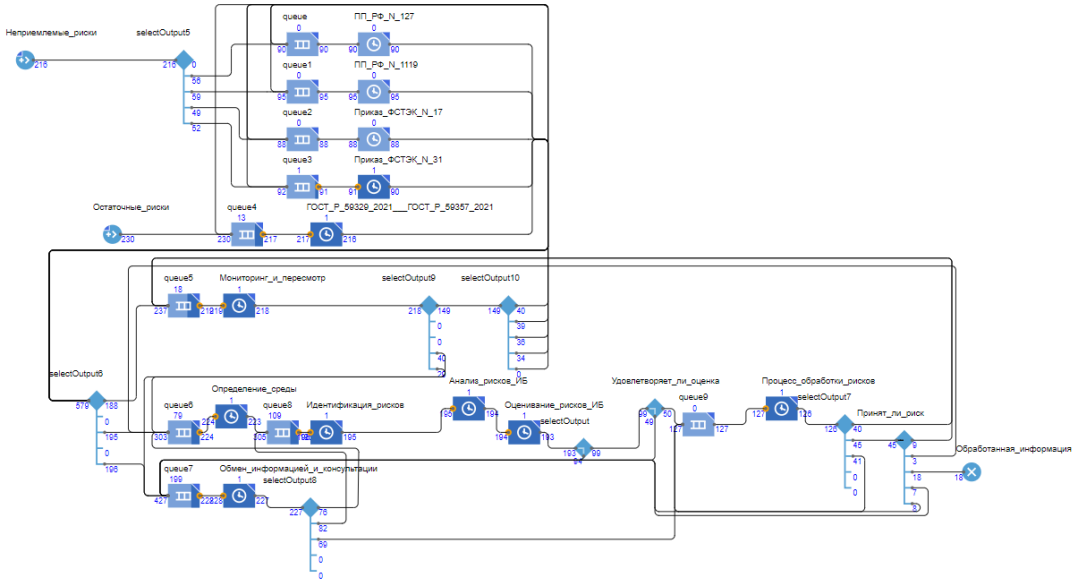

Рис. 3. Имитационная модель процесса обработки рисков информационной безопасности

Таблица 1

Наименование величины	Расчёт 1					Расчёт 2		
Wэ	0,019720508					0,019466105		
$P_{св.сб}$	0,5					0,5		
$P_{пр}$	0,70452381					0,602777778		
$P_{св.пр}$	0,804761905					0,841269841		
$P_{пр.р}$	0,068666667					0,077777778		
M	5					3		
Q	10					10		
$S_{пр.j}$	3	5	1	4	7	3	1	7
L_j	5	7	3	4	8	5	3	8
R_j	2	5	1	2	6	2	1	6
C_j	1	3	1	1	5	1	1	5

Заключение

В результате выполнения работы была рассмотрена проблема отсутствия комплексной системы управления рисками, которая включала бы в себя учёт как неприемлемых рисков, так и всех рисков, возникающих на различных этапах жизненного цикла. В качестве документа, определяющего процесс управления рисками, был выбран проект стандарта ГОСТ Р ИСО/МЭК 27005-2022 года, который предусматривает итеративный подход к управлению рисками и регулярный их пересмотр. На основе стандарта была создана имитационная модель процесса управления рисками и была выполнена оценка его эффективности, которая зависела от числа рассматриваемых ситуаций. В дальнейших исследованиях можно рассмотреть применимость других стандартов семейства 270xx в данном комплексном процессе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Селифанов В. В., Аникеева В. В., Огнев И. А. Вопросы оценки доверия к системе управления рисками // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 69–82. – DOI: 10.17212/2782-2230-2023-1-69-82.

2. Селифанов В. В., Солдатов А. Ю., Солдатов Е. Ю., Подлегаев А. И., Скориков В. С. Вопросы управления рисками управления решениями защиты информации / В. В. Селифанов, А. Ю. Солдатов, Е. Ю. Солдатов, А. И. Подлегаев, В. С. Скориков // Вопросы обеспечения безопасности в киберпространстве: материалы Всероссийской научно-технической конференции (16 декабря 2022 года). – Махачкала: Дагестанский государственный технический университет, 2022 г. – С. 80-87.

3. Селифанов В. В., Солдатов А. Ю., Солдатов Е. Ю., Подлегаев А. П., Скориков В. С. Метод оценивания рисков в системах принятия решений с учетом защиты информации // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 84–92. https://doi.org/10.55648/1998-6920-2023-17-2-84-92.

4. Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

5. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации. – 2012. – № 45, ч. 4. – Ст. 6257.

7. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателе критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации. – 2018. – № 8, ч. 4. – Ст. 1204.

8. Кириллова А. Д. Экспертная система аудита информационной безопасности АСУ ТП / А. Д. Кириллова // Информационные технологии интеллектуальной поддержки принятия решений: материалы V Всероссийской конференции (16–19 мая 2017 года). - Уфа: ГОУ ВПО "Уфимский государственный авиационный технический университет", 2017. – Том 2. – С. 172-174.

9. Евстратенко Е. С., Селифанов В. В., Старикова А. А. Построение системы защиты информации государственной информационной системы с учетом управления рисками информационной безопасности // Научные исследования: от теории к практике. – Чебоксары: ООО «Центр научного сотрудничества "Интерактив плюс"», 2016. – № 1(7). – С. 154-157.

10. Попов И. Ю. Разработка метода оценки соответствия обеспечения безопасности персональных данных в информационных системах согласно требованиям регулятора / И. Ю. Попов // Сборник трудов V Всероссийского конгресса молодых ученых: материалы конгресса (12–15 апреля 2016 года). – Санкт-Петербург: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2016. – Том 2. – С. 94-98.

11. ГОСТ Р 57193-2016. Системная и программная инженерия. Процессы жизненного цикла систем – М: Стандинформ, 2016. – 95 с.

12. Костогрызов А. И., Степанов П. В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд. «Вооружение, политика, конверсия», 2008. 404 с.

13. ГОСТ Р ИСО/МЭК 27005–2022. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2023. – 100 с.

14. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217−244. http://www.scirp.org/journal/ajor/.

15. Малыгина С. Н., Неупокоева Е. О. Обзор современных средств имитационного моделирования // Труды Кольского научного центра РАН. Серия: Технические науки. – 2022. – Т. 13, № 2. – С. 134–143. – DOI 10.37614/2949-1215.2022.13.2.013.

16. Хроль Е.В., Уварова А.Г., Кужильный А.В. Разработка имитационных моделей с помощью AnyLogic // Современные инновации, системы и технологии. – 2023. – 3(4). – С. 119-131. – DOI 10.47813/2782-2818-2023-3-4-0119-01310.

17. Моделирование процессов и систем защиты информации. AnyLogic : учебное пособие / А. В. Шабурова, В. А. Селифанов, В. В. Селифанов, П. А. Звягинцева, Ю. А. Исаева, А. С. Голдобина, А. В. Селифанов. – Новосибирск : СГУГиТ, 2020. – 70 с.

18. Построение сзигис с использованием моделирования трехуровневой системы УПРАВЛЕНИЯ Голдобина А.С. В книге: МНСК-2018: Информационные технологии. Материалы 56-й Международной научной студенческой конференции. 2018. С. 103.

19. Создание трехуровневой модели управления системой защиты информации в государственных информационных системах Селифанов В.В., Голдобина А.С., Звягинцева П.А. Интерэкспо Гео-Сибирь. 2018. № 7. С. 237-243.

20. Имитационная модель для управления защитой информации при оценке эффективности государственных и муниципальных систем Селифанов В.В., Исаева Ю.А., Голдобина А.С., Звягинцева П.А. Интерэкспо Гео-Сибирь. 2018. № 7. С. 296-299.