**БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 4 (107).** – 52–62

*ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ*

УДК 004.056 DOI: 10.17212/2782-2230-2022-4-52-62

# ОЦЕНКА РИСКОВ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ СИСТЕМЫ*

В.В. АНИКЕЕВА[1], В.В. СЕЛИФАНОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: veronika.korotkova.95@mail.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

Организации используют процесс определения архитектуры в рамках создания (модернизации, развития) и эксплуатации системы для обеспечения ее безопасности, качества и эффективности. Построение архитектуры отражает принципы, направляющие дизайн системы, учитывает риски, требования и ограничения для их реализации. В статье рассматривается процедура проведения оценки рисков в процессе определения архитектуры системы, а также предложены вероятностные методы решения задач по оценке возможных рисков, возникающих в процессе определения архитектуры системы, с учетом требований по защите информации.

**Ключевые слова**: архитектура системы, риск, оценка рисков, защита информации, пользователь, системная инженерия, информационная безопасность, государственная информационная система

## ВВЕДЕНИЕ

Цель процесса определения архитектуры – подготовка возможных вариантов архитектуры системы и выбор приемлемого варианта (одного или нескольких, если это необходимо). Последний должен отвечать интересам заинтересованных сторон, системным требованиям и выражать во множестве согласованных представлений различные точки зрения на систему [1].

* Статья получена 19 октября 2022 г.

Организации используют процесс определения архитектуры в рамках создания (модернизации, развития) и эксплуатации системы для обеспечения ее безопасности, качества и эффективности. В процессе определения архитектуры системы осуществляют защиту информации, направленную на обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию. Должна быть обеспечена надежная реализация процесса [1].

Для прогнозирования рисков и обоснования эффективных предупреждающих мер по их снижению или удержанию в допустимых пределах используют системный анализ с учетом требований по защите информации. Оценка рисков на этапе определения архитектуры системы позволяет эффективно применять целесообразные меры по их минимизации, а управление рисками позволит рационально выстраивать процессы информационной безопасности и распределять ресурсы для защиты активов компании. Кроме этого, выстроенный процесс управления рисками информационной безопасности позволит разработать и в случае необходимости применить четкие планы обеспечения непрерывности деятельности и восстановления работоспособности.

## 1. АНАЛИЗ ВОЗМОЖНЫХ РИСКОВ В ПРОЦЕССЕ ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ СИСТЕМЫ

Проблему возникновения рисков в процессе определения архитектуры целесообразно применять к большим системам. Анализ нынешнего состояния таких систем позволяет утверждать, что главной проблемой является территориальная распределенность и использование для решения функциональных задач разнообразных информационных технологий. В конечном итоге такая система представляет собой сложную структуру, состоящую из множества различных элементов. Для больших территориально распределенных систем актуальна такая проблема, как невозможность оперативного обнаружения неисправностей средств защиты информации. Некоторые части архитектуры могут временно выходить из строя, при этом пользователи и приложения не всегда уведомляются о том, что эти части заменены либо починены или что добавлены новые части для поддержки дополнительных пользователей либо приложений.

Функционирование таких систем обычно предполагается на базе информационно-телекоммуникационной инфраструктуры Центра обработки данных (далее – ЦОД). Прогнозированием рисков при построении архитектуры ЦОД занимается владелец данной инфраструктуры, поэтому подтверждением от-

сутствия неприемлемых рисков архитектуры ЦОД при размещении государственной информационной системы (далее – ГИС) в ЦОД в соответствии с требованиями законодательства [2] является аттестат соответствия.

При проведении аттестации в зависимости от класса защищенности и актуальных угроз безопасности системы предъявляется некий набор требований. Система мер защиты информации в ГИС включает следующие элементы: идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ), управление доступом субъектов доступа к объектам доступа (УПД), ограничение программной среды (ОПС), защита машинных носителей информации (ЗНИ), регистрация событий безопасности (РСБ), антивирусная защита (АВЗ), обнаружение вторжений (СОВ), контроль (анализ) защищенности информации (АНЗ), обеспечение целостности информационной системы и информации (ОЦЛ), обеспечение доступности информации (ОДТ), защита среды виртуализации (ЗСВ), защита информационной системы, ее средств, систем связи и передачи данных (ЗИС). Одной из мер [2] является обеспечение периодического резервного копирования информации на резервные машинные носители информации (ОДТ.4). Периодичность резервного копирования по требованиям [2] регламентируется в организационно-распорядительных документах оператора по защите информации. Владелец ЦОД может указать во внутренних документах, что резервное копирование должно проводиться раз в год, хотя этого недостаточно, а также периодичность выявления, анализа и устранения уязвимостей системы, угроз безопасности информации и оценки возможных последствий реализации угроз безопасности.

На базе информационно-телекоммуникационной инфраструктуры ЦОД обычно размещается достаточно большое количество систем различных организаций. Очевидно, что традиционная защита периметра, фокусирующаяся на атаках извне, не способна оградить от неприятностей, возникающих внутри информационно-телекоммуникационной инфраструктуры ЦОД. Соответственно возникает проблема разграничения трафика внутри ЦОД.

Помимо рисков, возникающих в информационно-телекоммуникационной инфраструктуре ЦОД, также существуют риски в процессе построения архитектуры на автоматизированных рабочих местах пользователей в организациях. Сегменты одной системы могут функционировать у разных юридических лиц. Из этого вытекает ряд других проблем (например, проблемы интеграции различных средств защиты информации, а также средств защиты информации разных производителей). Качество их взаимодействия внутри системы не всегда является оптимальным для выполнения как требуемых функций, так и набора составляющих данную систему средств защиты информации.

Анализ защищенности инфраструктуры больших систем, показал, что уровень защищенности большинства систем достаточно низок вследствие большого объема рисков. На этапе определения архитектуры для каждого элемента системы необходимо рассмотреть все группы рисков (технологические, инфраструтурные, системные и т. д.).

## 2. МАТЕМАТИЧЕСКИЕ МОДЕЛИ ДЛЯ ПРОГНОЗИРОВАНИЯ РИСКА

Для прогнозирования рисков в процессе определения архитектуры в системах применяются любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. Типовые модели и методы прогнозирования рисков обеспечивают вероятностную оценку следующих показателей:

– риск нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации;

– риск нарушения требований по защите информации в процессе определения архитектуры системы;

– интегральный риск нарушения реализации процесса определения архитектуры системы с учетом требований по защите информации.

В данной работе оценка осуществлена с использованием вероятностных показателей нахождения элементов моделируемой системы в определенном элементарном состоянии. Значения рисков предлагается рассчитывать с использованием метода, подробно изложенного в [2].

Для примера взята ГИС регионального масштаба со средней степенью возможного ущерба. Элементами системы являются:

1-й элемент – структурное подразделение, осуществляющее мониторинг работы систем защиты информации и реагирующее на инциденты информационной безопасности;

2-й элемент – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак;

3-й элемент – орган государственной власти, включающий АРМ пользователей, серверы;

4-й элемент – автоматизированные рабочие места пользователей ГИС в государственных бюджетных учреждениях;

5-й элемент – центр обработки данных, в котором развернута ГИС.

## 3. ПРОГНОЗИРОВАНИЕ РИСКА НАРУШЕНИЯ НАДЕЖНОСТИ РЕАЛИЗАЦИИ ПРОЦЕССА ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ СИСТЕМЫ

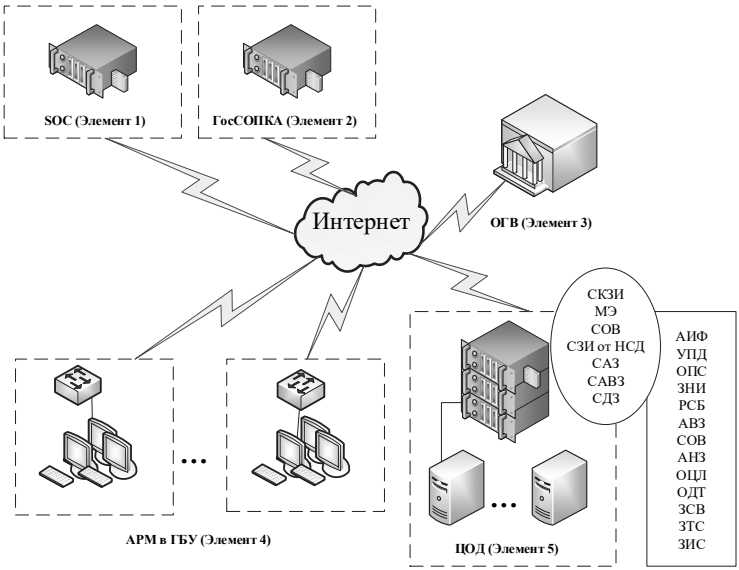
Надежность реализации процесса определения архитектуры моделируемой системы считается обеспеченной в течение заданного периода прогноза, если в течение этого периода надежно выполнены действия по определению архитектурных решений, ориентированные на применяемые процессы и технологии, причем эти архитектурные решения будут приемлемыми в течение такого же периода и в будущем (при эксплуатации моделируемой системы).

Прогнозирование риска нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации проиллюстрировано для моделирования комплекса архитектурных решений (рисунок). Выявлены возможные угрозы, критично влияющие на безопасность каждого из структурных элементов моделируемой системы.

В соответствии со сформированными исходными данными по каждому из пяти составных элементов системы анализ результатов моделирования показал, что в вероятностном выражении риск нарушения надежности реализации процесса определения архитектуры системы без учета требований по защите информации в течение года составляет за весь комплекс архитектурных решений около 0,02 у. е. При увеличении периода прогноза от шести месяцев до двух лет риск возрастает от 0,01 до 0,04 у. е., что является допустимым риском.

## 4. ПРОГНОЗИРОВАНИЕ РИСКА НАРУШЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Для расчета прогнозирования риска нарушений требований по защите информации осуществлена привязка требований [2] к структуре комплекса архитектурных решений (рисунок). При этом учтены не только угрозы, связанные с причинами неадекватного учета требований по защите информации на уровнях принятия решений при определении архитектуры, но и гипотетичные угрозы, связанные с последствиями этого неадекватного учета на этапе функционирования системы.




Структурная схема ГИС

Structural diagram of the state information system

Анализ результатов моделирования показал, что в вероятностном выражении риск нарушения требований по защите информации в течение года составит за весь комплекс архитектурных решений около 0,0357 у. е. При увеличении периода прогноза от шести месяцев до двух лет риск возрастает от 0,018 до 0,071 у. е. Для допустимого риска на уровне 0,05 у. е. обоснован период до 17 месяцев, при котором сохраняются гарантии удержания риска в допустимых пределах в выбранных архитектурных решениях.

## 5. ПРОГНОЗИРОВАНИЕ ИНТЕГРАЛЬНОГО РИСКА НАРУШЕНИЯ РЕАЛИЗАЦИИ ПРОЦЕССА С УЧЕТОМ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Интегральный риск нарушения надежности реализации процесса определения архитектуры системы [1] для периода прогноза, равного одному году, по результатам расчетов составил 0,0548 у. е.

В соответствии с рекомендациями [2] можно констатировать превышение расчетных рисков по сравнению с допустимым уровнем риска, т. е. обоснова-

на потребность улучшения архитектурных решений в части уменьшения риска нарушения требований по защите информации.

Новые архитектурные решения также подлежат системному анализу с использованием прогнозирования рисков.

## ЗАКЛЮЧЕНИЕ

Предлагаемый метод позволяет оценивать на уровне вероятностных показателей различные риски для процесса определения архитектуры системы. Ожидается, что рациональное использование предложенного метода в жизненном цикле системы будет способствовать выявлению «узких мест» и снижению рисков в процессе определения архитектуры системы.

## СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 59347–2021. Системная инженерия. Защита информации в процессе определения архитектуры системы. – М.: Стандартинформ, 2021.

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

3. *Кидяева С.М., Шабурова А.В. Селифанов В.В.* Вопросы организации менеджмента рисков значимых объектов критической информационной инфраструктуры // Интерэкспо ГЕО-Сибирь. – 2022. – Т. 6. – С. 82–87.

4. *Костогрызов А.И.* Прогнозирование рисков по данным мониторинга для систем искусственного интеллекта // Безопасные информационные технологии: сборник трудов Десятой Международной научно-технической конференции. – М., 2019. – С. 220–229.

5. *Авдонин Р.Ю., Костогрызов А.И., Нистратов А.А.* Вероятностная оценка рисков для реализации процесса управления человеческими ресурсами системы // Безопасные информационные технологии: сборник трудов XI Международной научно-технической конференции. – М., 2021. – С. 2–11.

6. *Исаева В.Э., Шабуров А.С.* Анализ рисков объекта критической информационной инфраструктуры, агрегированных по угрозам или последствиям // Инновационные технологии: теория, инструменты, практика. – 2020. – Т. 1. – С. 426–432.

7. *Керимов К.Ф.* Методика оценки рисков информационной безопасности электронных ресурсов при физических угрозах // Проблемы вычислительной и прикладной математики. – 2020. – № 4 (28). – С. 97–106.

8. *Кругликов С.В., Касанин С.Н., Кулешов Ю.В.* Методический подход к комплексному описанию объекта информационной защиты // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 39–51.

9. *Прокин А.А., Бояркин Е.А., Радаев К.Д.* Управление рисками информационной безопасности // Студенческий меридиан среднего профессионального образования в вузе. – Саранск, 2021. – С. 126–129.

10. *Васильев В.И., Вульфин А.М., Кириллова А.Д.* Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования // Моделирование, оптимизация и информационные технологии. – 2022. – № 10 (2). – DOI: 10.26102/2310-6018/2022.37.2.022.

11. *Куркин А.В. Шевченко Я.С.* Оценка рисков информационной безопасности с применением нечеткого моделирования // Неделя науки Санкт-Петербургского государственного морского технического университета. – 2020. – № 4. – Ст. 45.

12. *Цветкова И.С., Сенцова А.Ю.* Использование метода, основанного на марковских моделях, для оценки рисков информационной безопасности // Информационные технологии. Проблемы и решения. – 2021. – № 4 (17). – С. 107–113.

13. *Кучеренко Д.В.* Архитектура системы управления развитием региональной инфраструктуры государственных информационных систем // Вестник Санкт-Петербургского университета государственной противопожарной службы МЧС России. – 2021. – № 4. – С. 215–222.

14. *Ильина О.П.* Архитектура системы информационной безопасности // Инновационные технологии и вопросы обеспечения безопасности реальной экономики. – СПб., 2020. – С. 74–87.

***Аникеева Вероника Валерьевна***, ассистент кафедры защиты информации Новосибирского государственного технического университета. E-mail: veronika.korotkova.95@mail.ru

***Селифанов Валентин Валерьевич***, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: sfo1@mail.ru

DOI: 10.17212/2782-2230-2022-4-52-62

## Risk assessment in the process of determining the system architecture*

**V.V. Anikeeva[1], V.V. Selifanov[2]**

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Assistant of the Department of Information Security. E-mail: veronika.korotkova.95@mail.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer of the Department of Information Security. E-mail: sfo1@mail.ru*

Organizations use the process of defining the architecture as part of the creation (modernization, development) and operation of the system to ensure its safety, quality and efficiency. The architecture reflects the principles guiding the design of the system, takes into account the risks, requirements and limitations for their implementation. The article discusses the procedure for conducting a risk assessment in the process of determining the system architecture, and also suggests probabilistic methods for solving problems of assessing possible risks arising in the process of determining the system architecture, taking into account information security requirements.

**Keywords**: system architecture, risk, risk assessment, information protection, user, system engineering, information security, state information system

## REFERENCE

1. State Standard R 59347–2021. System engineering. Protection of information in system architecture definition process. Moscow, Standartinform Publ., 2021. (In Russian).

2. Order of the FSTEC of Russia dated 11.02.2013 N 17 "On approval of requirements for the protection of information not constituting a state secret contained in state information systems". (In Russian).

3. Kidyaeva S.M., Shaburova A.V., Selifanov V.V. Voprosy organizatsii menedzhmenta riskov znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury [Issues of formation of risk management of significant objects of critical information infrastructure]. Interekspo GEO-Sibir'= Interexpo GEO-Siberia, 2022, vol. 6, pp. 82–87.

4. Kostogryzov A.I. [Risks prediction for artificial intelligence systems using monitoring data]. Bezopasnye informatsionnye tekhnologii [Secure information technologies]. Proceedings of the Tenth International Scientific and Technical Conference. Moscow, 2019, pp. 220–229. (In Russian).

* *Received 10 October 2022.*

5. Avdonin R.Yu., Kostogryzov A.I., Nistratov A.A. [Risk estimation for the implementation of the system's human resource management process]. Bezopasnye informatsionnye tekhnologii [Secure information technologies]. Proceedings of the XI International Scientific and Technical Conference. Moscow, 2021, pp. 2–11. (In Russian).

6. Isaeva V.E., Shaburov A.S. Analiz riskov ob"ekta kriticheskoi informatsionnoi infrastruktury, agregirovannykh po ugrozam ili posledstviyam [Risk analysis of a critical information infrastructure object, aggregated threats or by effects]. Innovatsionnye tekhnologii: teoriya, instrumenty, praktika = Innovative technologies: theory, tools, practice, 2020, vol. 1, pp. 426–432.

7. Kerimov K.F. Metodika otsenki riskov informatsionnoi bezopasnosti electronnykh resursov pri fizicheskikh ugrozakh [Electronic resources information security risk assessment method at physical threats]. Problemy vychislitel'noi i prikladnoi matematiki = Problems of Computational and Applied Mathematics, 2020, no. 4 (28), pp. 97–106.

8. Kruglikov S.V., Kasanin S.N., Kuleshov Yu.V. Metodicheskii podkhod k kompleksnomu opisaniyu ob"ekta informatsionnoi zashchity [Methodical approach to the complex description of information protection object]. Voprosy kiberbezopasnosti = Cybersecurity Issues, 2022, no. 4 (50), pp. 39–51.

9. Prokin A.A., Boyarkin E.A., Radaev K.D. Upravlenie riskami informatsionnoi bezopasnosti [Information security risk management]. Studencheskii meridian srednego professional'nogo obrazovaniya v vuze [Student meridian of secondary vocational education at the university. University collection of scientific papers]. Saransk, 2021, pp. 126–129.

10. Vasilyev V.I., Vulfin A.M., Kirillova A.D. Analiz i upravlenie riskami informatsionnoi bezopasnosti ASU TP na osnove kognitivnogo modelirovaniya [Analysis and management of ICS cybersecurity risks based on cognitive modeling]. Modelirovanie, optimizatsiya i informatsionnye tekhnologii = Modeling, Optimization and Information Technology, 2022, no. 10 (2). DOI: 10.26102/2310-6018/2022.37.2.022.

11. Kurkin A.V. Shevchenko Ya.S. Otsenka riskov informatsionnoi bezopasnosti s primeneniem nechetkogo modelirovaniya [Risk assessment of information security with fuzzy modeling]. Nedelya nauki Sankt-Peterburgskogo gosudarstvennogo morskogo tekhnicheskogo universiteta, 2020, no. 4, art. 45. (In Russian).

12. Tsvetkova I.S., Sentsova A.Yu. Ispol'zovanie metoda, osnovannogo na markovskikh modelyakh, dlya otsenki riskov informatsionnoi bezopasnosti [Using the method based on Markov models to assess information security risks]. Informatsionnye tekhnologii. Problemy i resheniya = Information Technologies. Problems and solutions, 2021, no. 4 (17), pp. 107–113.

13. Kucherenko D.V. Arkhitektura sistemy upravleniya razvitiem regional'noi in-frastruktury gosudarstvennykh informatsionnykh sistem [The architecture of the development management system of the regional infrastructure of state information systems]. Vestnik Sankt-Peterburgskogo universiteta gosudarstvennoi protivopozharnoi sluzhby MChS Rossii = Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia, 2021, no. 4, pp. 215–222.

14. Ilyina O.P. Arkhitektura sistemy informatsionnoi bezopasnosti [Architecture security information system]. Innovatsionnye tekhnologii i voprosy obespecheniya bezopasnosti real'noi ekonomiki [Innovative technologies and issues of ensuring the security of the real economy]. St. Petersburg, 2020, pp. 74–87.

Для цитирования:

Аникеева В.В., Селифанов В.В. Оценка рисков в процессе определения архитектуры системы // Безопасность цифровых технологий. – 2022. – № 4 (107). – С. 52–62. – DOI: 10.17212/2782-2230-2022-4-52-62.

For citation:

Anikeeva V.V., Selifanov V.V. Otsenka riskov v protsesse opredeleniya arkhitektury sistemy [Risk assessment in the process of determining the system architecture]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 4 (107), pp. 52–62. DOI: 10.17212/2782-2230-2022-4-52-62.