БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 1 (108). – 69–82

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

УДК 004.056 DOI: 10.17212/2782-2230-2023-1-69-82

ВОПРОСЫ ОЦЕНКИ ДОВЕРИЯ К СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ*

В.В. СЕЛИФАНОВ[1], В.В. АНИКЕЕВА[2], И.А. ОГНЕВ[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: veronika.korotkova.95@mail.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, ассистент кафедры защиты информации. E-mail: i.ognev.2016@corp.nstu.ru*

Настоящая статья посвящена вопросам оценки доверия к системе управления рисками. Термин «доверие» в отношении информационных систем практически не применяется в настоящее время. Предложена процедура оценки доверия к системе управления рисками, состоящая из четырех этапов: 1) соответствие требованиям законодательства РФ; 2) соответствие национальным стандартам; 3) оценка оптимальности существующий системы управления рисками; 4) переоценка рисков. Приведено описание существующих методов оценки доверия к системе управления рисками. Сделан вывод о том, что сегодня нет существующих требований к системе оценки рисков даже в отдельных сегментах. В работе предлагается использовать предварительно согласованную заинтересованными сторонами выборку критериев для оценки рисков из системы стандартов, описывающих процесс определения рисков с точки зрения системной инженерии. Рассмотрены критерии и показатели, используемые в стандартах, определяющих системный анализ. За основу оценки рисков принята вероятностная оценка ряда показателей: риск нарушения надежности реализации процесса без учета требований по защите информации; риск нарушения требований по защите информации в процессе; интегральный риск нарушения реализации процесса с учетом требований по защите информации. Для расчета этих показателей рисков исследуемые сущности рассматриваются в виде моделируемой системы сложной структуры. Приведена математическая модель оценки рисков в соответствии с положениями стандартов по системной инженерии.

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

* Статья получена 17 февраля 2023 г.

ВВЕДЕНИЕ

Одной из основных особенностей функционирования информационных систем в настоящее время является обязательное взаимодействие между собой. Важным вопросом при этом является оценка доверия между ними.

С учетом последних изменений требований к функционированию и развитию систем данный вопрос необходимо рассматривать прежде всего сквозь призму нормативно-правового регулирования.

Термином «доверие» обозначаются меры, принятые для должной реализации потенциальных возможностей безопасности и состоящие из сформированного свидетельства и независимой оценки пригодности этих возможностей [1]. В настоящее время данный термин в законодательных, нормативных правовых актах Российской Федерации практически не используется применительно к информационным системам и предоставляемым сервисам. Начальным этапом оценки уровня доверия к субъекту информационного обмена в недоверенной среде является оценка доверия к системе оценки и управления рисками.

Оценку доверия к системе управления рисками можно разбить на следующие этапы:

1) соответствие требованиям законодательства РФ при оценке недопустимых рисков [2–5];

2) соответствие национальным стандартам [6–31];

3) оценка оптимальности существующей системы управления рисками;

4) проведение переоценки рисков.

1. ОПИСАНИЕ СУЩЕСТВУЮЩИХ ПОДХОДОВ

Первичный процесс оценки рисков осуществляется в соответствии законодательством в зависимости от типа объекта: государственные информационные системы – приказ ФСТЭК России № 17 [2]; информационные системы персональных данных – постановление Правительства РФ № 1119 [4]; автоматизированные системы управления производственными и технологическими процессами – приказ ФСТЭК России № 31 [3]; значимые объекты критической информационной инфраструктуры – постановление Правительства РФ № 127 [5].

В указанных нормативных правовых актах присутствуют критерии определения рисков, а также некоторые процедуры их переоценки. Проведение переоценки рисков в соответствии с данными нормативными правовыми актами проводится крайне редко.

Определены следующие критерии проведения переоценки рисков для каждого типа объекта:

– для значимых объектов критической информационной инфраструктуры переоценка рисков (категории значимости) осуществляется не реже чем один раз в 5 лет, а также в случае изменения показателей критериев значимости объектов критической информационной инфраструктуры или их значений. Также результаты определения рисков (категорирования) в обязательном порядке согласуются с ФСТЭК России;

– для государственных информационных систем пересмотр класса защищенности осуществляется при изменении масштаба информационной системы или значимости обрабатываемой в ней информации;

– для информационных систем персональных данных контроль за выполнением требований [4] проводится не реже одного раза в 3 года;

– для автоматизированной системы управления производственными и технологическими процессами переоценка рисков (класса защищенности) проводится только в случае модернизации системы, в результате которой меняется уровень значимости (критичности) информации, обрабатываемой в автоматизированной системе управления или ее сегменте.

Стоит отметить две достаточно большие проблемы: во-первых, нормативно существует требование только к определению неприемлемых рисков [2–5], остальные вынесены за черту, и, во-вторых, отсутствие четких требований по управлению рисками. Они заданы только требованием по переоценке условий и максимальным промежутком времени, по истечении которого в любом случае необходимо повторно их оценить.

Таким образом, владелец системы должен сам создать систему управления рисками при отсутствии нормативных требований.

Результат ошибки здесь может стоить дорого и привести к неактуальности рисков и нанесению ущерба организации. Отсутствие цикличности рассмотрения актуальности конкретных рисков может привести к пересмотрению модели нарушителя, к неактуальности модели угроз, а также самой системы безопасности организации.

Таким образом, можно сделать вывод о том, что сейчас не существует системы требований к оценке рисков даже в отдельных сегментах, таких как значимые объекты критической информационной инфраструктуры Российской Федерации, государственные и муниципальные информационные системы. То есть при установлении взаимодействия между двумя системами у нас не существует системы и критериев оценки, исходя из которых можно будет определять базовый элемент доверия – доверие к тому, как определены риски. Причем отдельным вопросом будет стоять не только вопрос определения неприемлемых рисков, но и вопрос определения допустимых рисков.

Единственным универсальным инструментом в руках работников подразделений информационной безопасности остается ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [6], который определяет процесс управления рисками ИБ, состоящий из следующих этапов:

- установление контекста: определение области оценки рисков ИБ, установление внешних и внутренних факторов;
- оценка риска: определение ценности информационных активов, выявление потенциальных угроз и уязвимостей, определение существующих мер и средств контроля и управления и их воздействие на идентифицированные риски, определение возможных последствий и назначение приоритетов установленным рискам, а также их ранжирование по критериям оценки риска, зафиксированным при установлении контекста;
- обработка риска: определение мер и средств контроля и управления для снижения, сохранения, предотвращения или переноса рисков;
- принятие риска: документированное решение о принятии рисков с установленной за это ответственностью;
- коммуникация риска: обмен информацией о риске или ее совместное использование;
- мониторинг и переоценки риска: проведение непрерывного мониторинга происходящих изменений и регулярный пересмотр рисков ИБ, а также способов их обработки на предмет актуальности и адекватности потенциально изменившейся ситуации.

Использование данного документа носит рекомендательный характер.

Стоит отметить: в последнее время была принята система стандартов [7–31], описывающая процесс определения рисков с точки зрения системной инженерии.

В рамках развития государственной системы защиты информации на основе ГОСТ Р 57193–2016 «Системная и программная инженерия. Процессы жизненного цикла систем» [7] в 2021 году разработаны 23 национальных стандарта (ГОСТ Р 59329, ГОСТ Р 59357 [8–31]), описывающих оценку рисков в рамках процессов в жизненном цикле системы, объединенных в 4 группы процессов:

– процессы соглашения (приобретение и поставка продукции и услуг для системы);

– процессы организационного обеспечения проекта (управление моделью жизненного цикла, инфраструктурой, портфелем проекта, человеческими ресурсами, качеством, знаниями о системе);

– процессы технического управления (планирование, оценка и контроль проекта; управление решениями, рисками, конфигурацией, информацией; измерения; гарантии качества);

– технические процессы (анализ бизнеса или назначения; определение потребностей и требований заинтересованной стороны; определение системных требований; определение архитектуры проекта; системный анализ реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы).

Допускается использование стадий жизненного цикла системы различным образом, чтобы удовлетворить стратегиям разнообразного бизнеса и снизить риски. Использование стадий одновременно и в различных последовательностях может привести к формам жизненного цикла с отчетливо различными характеристиками.

Основные усилия системной инженерии для обеспечения защиты информации сосредоточены:

– на определении выходных результатов и действий, предназначенных для достижения целей процесса и защиты активов, информация о которых необходима для достижения этих целей;

– выявлении потенциальных угроз и определении возможных сценариев возникновения и развития угроз для активов, подлежащих защите, выходных результатов и выполняемых действий процесса;

– определении и прогнозировании рисков, подлежащих системному анализу;

– проведении системного анализа для обоснования мер, направленных на противодействие угрозам и достижение целей процесса.

Система стандартов опирается на математические модели, отличающиеся от подходов, изложенных в ГОСТ Р 27005–2010.

С точки зрения оценки доверия к системе управления рисками, а именно корректного определения рисков в каждом процессе, необходимо рассмотреть критерии и показатели, используемые в стандартах, определяющих системный анализ.

За основу принята вероятностная оценка следующих показателей [8–31]:

– оценка риска нарушения надежности реализации процесса без учета требований по защите информации;

– оценка риска нарушения требований по защите информации в процессе;

– оценка интегрального риска нарушения реализации процесса с учетом требований по защите информации.

Для расчета этих показателей рисков исследуемые сущности рассматривают в виде моделируемой системы сложной структуры.

Моделируемая система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых необходимо рассматривать как «черный ящик», функционирующий в условиях неопределенности.

При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных состояний. Это пространство элементарных состояний формируют в результате статистического анализа произошедших событий с их привязкой к временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если...», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя процессов может быть дополнена гипотетичными событиями, характеризующими ожидаемые и(или) прогнозируемые условия функционирования системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

Для математической формализации используют следующие основные положения:

– к началу периода прогноза предполагается, что целостность моделируемой системы обеспечена, включая изначальное выполнение требований по защите информации в системе (в качестве моделируемой системы простой или сложной структуры могут быть рассмотрены выходные результаты с задействованными активами и действия процесса, к которым предъявлены определенные требования, включая требования по защите информации);

– в условиях неопределенностей возникновение и разрастание различных угроз описывается в терминах случайных событий;

– для различных вариантов развития угроз средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность мер и(или) защитных преград, предназначенных для воспрепятствования реализации угроз.

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение реализации рассматриваемого процесса.

В общем случае для системы, представленной в виде «черного ящика», применительно к выполняемым действиям, выходным результатам рассматриваемого процесса и защищаемым активам формально определяют следующие исходные данные:

– частота возникновения источников угроз в системе с точки зрения нарушения надежности реализации процесса;

– среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности системы (выполняемых действий процесса, выходных результатов и(или) защищаемых активов) с точки зрения нарушения надежности реализации процесса;

– среднее время между окончанием предыдущей и началом очередной диагностики целостности системы;

– среднее время системной диагностики целостности системы;

– среднее время восстановления нарушенной целостности;

– задаваемая длительность периода прогноза.

Оценки осуществляют с использованием вероятностных показателей нахождения элементов моделируемой системы в определенном элементарном состоянии. Прогнозирование интегрального риска предлагается оценивать в сопоставлении с возможным ущербом по формуле

$$R_{\text{инт}}(T_{\text{зд}}) = 1 - [1 - R_{\text{нд}}(T_{\text{зд}})] \cdot [1 - R_{\text{нр}}(T_{\text{зд}})], \quad (1)$$

где $R_{\text{нд}}(T_{\text{зд}})$ – риск нарушения надежности реализации процесса без учета требований по защите информации; $R_{\text{нр}}(T_{\text{зд}})$ – риск нарушения требований по защите информации в процессе; $R_{\text{инт}}(T_{\text{зд}})$ – интегральный риск нарушения реализации процесса с учетом требований по защите информации.

Сами значения рисков $R_{\text{нд}}(T_{\text{зд}})$ и $R_{\text{нр}}(T_{\text{зд}})$ предлагается рассчитывать с использованием метода, подробно изложенного в [8–31].

В зависимости от процесса в системе стандартов приведены критерии оценки, позволяющие оценить полученные прогнозные данные.

Стоит отметить, что данные стандарты предназначены для прогнозирования рисков и прежде всего могут использоваться для построения цифровых двойников взаимодействующих систем.

В настоящей работе предлагается использовать их положения для взаимной предварительной оценки рисков в системах как перед установлением взаимодействия, так и в его процессе.

Принимая за основу показатели, приведенные для каждого из процессов, их конечную выборку следует согласовать с соответствующими подразделениями, ответственными за информационную безопасность.

Процессы управления рисками должны быть построены исходя из положений ГОСТ 27005–2010 и оцениваться также по указанным в нем требованиям.

ЗАКЛЮЧЕНИЕ

В настоящее время нормативно не определены методы и критерии оценки систем управления рисками взаимодействующих систем. В работе предлагается использовать предварительно согласованную заинтересованными сторонами выборку критериев для оценки рисков из системы стандартов [8–31], а также оценивать систему управления рисками, исходя из положений стандарта ГОСТ Р 27005–2010, что позволит создать универсальную систему, основанную не на «личном мировоззрении» отдельных работников, а на универсальной системе стандартов, исключающей субъективное мнение.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК ТО 19791–2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. – М.: Стандартинформ, 2010. – 127 с.

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. 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».

4. 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.

5. 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.

6. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 52 с.

7. ГОСТ Р 57193–2016. Системная и программная инженерия. Процессы жизненного цикла систем. – М.: Стандартинформ, 2016. – 99 с.

8. ГОСТ Р 59329–2021. Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы. – М.: Стандартинформ, 2021. – 27 с.

9. ГОСТ Р 59330–2021. Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы. – М.: Стандартинформ, 2021. – 29 с.

10. ГОСТ Р 59331–2021. Системная инженерия. Защита информации в процессе управления инфраструктурой системы. – М.: Стандартинформ, 2021. – 45 с.

11. ГОСТ Р 59332–2021. Системная инженерия. Защита информации в процессе управления портфелем проектов. – М.: Стандартинформ, 2021. – 33 с.

12. ГОСТ Р 59333–2021. Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы. – М.: Стандартинформ, 2021. – 41 с.

13. ГОСТ Р 59334–2021. Системная инженерия. Защита информации в процессе управления качеством системы. – М.: Стандартинформ, 2021. – 31 с.

14. ГОСТ Р 59335–2021. Системная инженерия. Защита информации в процессе управления знаниями о системе. – М.: Стандартинформ, 2021. – 29 с.

15. ГОСТ Р 59336–2021. Системная инженерия. Защита информации в процессе планирования проекта. – М.: Стандартинформ, 2021. – 29 с.

16. ГОСТ Р 59337–2021. Системная инженерия. Защита информации в процессе оценки и контроля проекта. – М.: Стандартинформ, 2021. – 33 с.

17. ГОСТ Р 59338–2021. Системная инженерия. Защита информации в процессе управления решениями. – М.: Стандартинформ, 2021. – 46 с.

18. ГОСТ Р 59339–2021. Системная инженерия. Защита информации в процессе управления рисками для системы. – М.: Стандартинформ, 2021. – 47 с.

19. ГОСТ Р 59340–2021. Системная инженерия. Защита информации в процессе управления конфигурацией системы. – М.: Стандартинформ, 2021. – 29 с.

20. ГОСТ Р 59342–2021. Системная инженерия. Защита информации в процессе измерений системы. – М.: Стандартинформ, 2021. – 31 с.

21. ГОСТ Р 59344–2021. Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы. – М.: Стандартинформ, 2021. – 31 с.

22. ГОСТ Р 59345–2021. Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы. – М.: Стандартинформ, 2021. – 27 с.

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

24. ГОСТ Р 59348–2021. Системная инженерия. Защита информации в процессе определения проекта. – М.: Стандартинформ, 2021. – 41 с.

25. ГОСТ Р 59350–2021. Системная инженерия. Защита информации в процессе реализации системы. – М.: Стандартинформ, 2021. – 28 с.

26. ГОСТ Р 59351–2021. Системная инженерия. Защита информации в процессе комплексирования системы. – М.: Стандартинформ, 2021. – 29 с.

27. ГОСТ Р 59353–2021. Системная инженерия. Защита информации в процессе передачи системы. – М.: Стандартинформ, 2021. – 45 с.

28. ГОСТ Р 59354–2021. Системная инженерия. Защита информации в процессе аттестации системы. – М.: Стандартинформ, 2021. – 33 с.

29. ГОСТ Р 59355–2021. Системная инженерия. Защита информации в процессе функционирования системы. – М.: Стандартинформ, 2021. – 29 с.

30. ГОСТ Р 59356–2021. Системная инженерия. Защита информации в процессе сопровождения системы. – М.: Стандартинформ, 2021. – 27 с.

31. ГОСТ Р 59357–2021. Системная инженерия. Защита информации в процессе изъятия и списания системы – М.: Стандартинформ, 2021. – 46 с.

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: sfo1@mail.ru

Аникеева Вероника Валерьевна, ассистент кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: veronika.korotkova.95@mail.ru

Огнев Игорь Александрович, ассистент кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: i.ognev.2016@corp.nstu.ru

DOI: 10.17212/2782-2230-2023-1-69-82

Issues of assessing the credibility of the risk management system*

V.V. Selifanov[1], V.V. Anikeeva[2], I.A. Ognev[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer, Department of Information Security. E-mail: sfo1@mail.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, assistant of Data Protection Department. E-mail: veronika.korotkova.95@mail.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Assistant of Data Protection Department. E-mail: i.ognev.2016@corp.nstu.ru*

This article is devoted to the assessment of confidence in the risk management system. The term trust in relation to information systems is practically not used nowadays. The author proposes a procedure for assessing confidence in the risk management system, which consists of four stages: compliance with the requirements of Russian legislation and national standards, assessing the optimality of the existing risk management system and reassessing risks. A description of existing methods for assessing confidence in risk management systems has been given. It is concluded that at present there are no existing requirements to the system of risk assessment even in some segments. The paper proposes to use a pre-agreed by stakeholders' selection of criteria for assessing risks from a system of standards that describe the process of risk assessment in terms of systems engineering. The criteria and indicators used in the standards that define systems analysis are considered. Probabilistic assessment of a few indicators is taken as the basis of risk assessment: risk of violation of reliability of process implementation without regard to information protection requirements; risk of violation of information protection requirements in the process; integral risk of violation of process implementation with regard to information protection requirements. To calculate these risk indicators the investigated entities are examined in the form of a modeled system of a complex structure. A mathematical model for assessing risks in accordance with the provisions of systems engineering standards is presented.

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

REFERENCES

1. State Standard R ISO/MEK TO 19791–2008. Information technology. Methods and means of ensuring safety. Safety assessment of automated systems. Moscow, Standartinform Publ., 2010. 127 p. (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).

* *Received 17 February 2023.*

3. Order of the FSTEC of Russia dated March 14, 2014 No. 31 "On approval of the requirements for ensuring the protection of information in automated control systems for production and technological processes at critically important facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to life and human health and for the environment". (In Russian).

4. Decree of the Government of the Russian Federation dated November 1, 2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems". S Sobranie zakonodatel'stva Ros-siiskoi Federatsii = Collection of the legislation of the Russian Federation, 2012, no. 45, pt. 4, art. 6257. (In Russian).

5. Decree of the Government of the Russian Federation of 08.02.2018 No. 127 "On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values". Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2018, no. 8, pt. 4, art. 1204. (In Russian).

6. State Standard R ISO/MEK 27005–2010. Information technology. Methods and means of ensuring safety. Information security risk management. Moscow, Standartinform Publ., 2011. 52 p. (In Russian).

7. State Standard R ISO/MEK 27005–2010. System and software engineering. Systems Life Cycle Processes. Moscow, Standartinform Publ., 2016. 99 p. (In Russian).

8. State Standard R 59329–2021. System engineering. Protection of information in the processes of acquisition and supply of products and services for the system. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

9. State Standard R 59330–2021. System engineering. Protection of information in the process of managing the system life cycle model. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

10. State Standard R 59331–2021. System engineering. Information protection in the process of system infrastructure management. Moscow, Standartinform Publ., 2021. 45 p. (In Russian).

11. State Standard R 59332–2021. System engineering. Protection of information in the process of managing a portfolio of projects. Moscow, Standartinform Publ., 2021. 33 p. (In Russian).

12. State Standard R 59333–2021. System engineering. Protection of information in the process of managing human resources of the system. Moscow, Standartinform Publ., 2021. 41 p. (In Russian).

13. State Standard R 59334–2021. System engineering. Protection of information in the process of system quality management. Moscow, Standartinform Publ., 2021. 31 p. (In Russian).

14. State Standard R 59335–2021. System engineering. Protection of information in the process of knowledge management about the system. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

15. State Standard R 59336–2021. System engineering. Protection of information in the process of project planning. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

16. State Standard R 59337–2021. System engineering. Protection of information in the process of evaluation and control of the project. Moscow, Standartinform Publ., 2021. 33 p. (In Russian).

17. State Standard R 59338–2021. System engineering. Protection of information in the process of decision management. Moscow, Standartinform Publ., 2021. 46 p. (In Russian).

18. State Standard R 59339–2021. System engineering. Protection of information in the process of risk management for the system. Moscow, Standartinform Publ., 2021. 47 p. (In Russian).

19. State Standard R 59340–2021. System engineering. Protection of information in the process of system configuration management. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

20. State Standard R 59342–2021. System engineering. Protection of information in the process of measuring the system. Moscow, Standartinform Publ., 2021. 31 p. (In Russian).

21. State Standard R 59344–2021. System engineering. Protecting information during business analysis or system assignment. Moscow, Standartinform Publ., 2021. 31 p. (In Russian).

22. State Standard R 59345–2021. System engineering. Protection of information in the process of determining the needs and requirements of the interested party for the system. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

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

24. State Standard R 59348–2021. System engineering. Protection of information in the process of defining a project. Moscow, Standartinform Publ., 2021. 41 p. (In Russian).

25. State Standard R 59350–2021. System engineering. Protection of information in the process of system implementation. Moscow, Standartinform Publ., 2021. 28 p. (In Russian).

26. State Standard R 59351–2021. System engineering. Protection of information in the process of complexing the system. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

27. State Standard R 59353–2021. System engineering. Protection of information during the transfer of the system. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

28. State Standard R 59354–2021. System engineering. Protection of information in the process of system certification. Moscow, Standartinform Publ., 2021. 33 p. (In Russian).

29. State Standard R 59355–2021. System engineering. Protection of information in the process of system operation. Moscow, Standartinform Publ., 2021. 29 p. (In Russian).

30. State Standard R 59356–2021. System engineering. Protection of information in the process of system maintenance. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

31. State Standard R 59357–2021. System engineering. Protection of information in the process of withdrawal and decommissioning of the system. Moscow, Standartinform Publ., 2021. 46 p. (In Russian).

Для цитирования:

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.

For citation:

Selifanov V.V., Anikeeva V.V., Ognev I.A. Voprosy otsenki doveriya k sisteme upravleniya riskami [Issues of assessing the credibility of the risk management system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 69–82. DOI: 10.17212/2782-2230-2023-1-69-82.