БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2024. – № 1 (112). – 23–41

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2024-1-23-41

НЕКОТОРЫЕ ВОПРОСЫ УПРАВЛЕНИЯ РИСКАМИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ*

К.К. МАРТЫНЕНКО[1], А.В. ЦЕНИНА[2], В.В. СЕЛИФАНОВ[3]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: k.martynenko.2019@stud.nstu.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: cenina.2020@stud.nstu.ru*
[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

В статье предложен подход к оценке рисков информационной безопасности автоматизированных систем управления технологическими процессами, государственных информационных систем, муниципальных информационных систем, информационных систем персональных данных и объектов критической информационной инфраструктуры на основе требований законодательства Российской Федерации в области защиты типов информационных систем, проекта национального стандарта ГОСТ Р ИСО/МЭК 27005, планируемого к принятию в ближайшее время, и стандартов оценки рисков в рамках процессов в жизненном цикле системы от ГОСТ Р 59329–2021 до ГОСТ 59357–2021, опубликованных в 2021 году. Эти стандарты построены на основе ГОСТ Р 57193–2016, который описывает процессы жизненного цикла систем, созданных человеком. Рассмотрена проблема обработки остаточного риска в отношении неприемлемых рисков, после анализа которой предложен другой принцип управления безопасностью. Получена методика оценки доверия к системе управления рисками, с помощью которой необходимо строить систему управления рисками на объектах критической информационной инфраструктуры.

Ключевые слова: критическая информационная инфраструктура, государственные информационные системы, автоматизированные системы, автоматизированные системы управления технологическим процессом, муниципальные информационные системы, информационные системы персональных данных, риск, неприемлемый риск, остаточный риск, система защиты, защита информации, стандарт, информационная система

* Статья получена 11 февраля 2024 г.

ВВЕДЕНИЕ

Построение системы защиты – необходимый этап для создания функционирующей информационной системы. Процесс создания системы защиты включает в себя несколько этапов: классификацию информационной системы, определение актуальных угроз безопасности информации, уязвимостей системы и мер, достаточных для недопущения реализации угроз.

Первый этап построения системы защиты – классификация информационной системы – непосредственно связан с ее типом. Существуют следующие типы информационных систем: информационные автоматизированные системы, автоматизированные системы управления технологическими процессами (далее – АС, АСУ ТП) [1], государственные информационные системы, муниципальные информационные системы (далее – ГИС, МИС) [2], информационные системы персональных данных (далее – ИСПДн) [3] и объекты критической информационной инфраструктуры (далее – ОКИИ) [4]. Исходя из типа информационной системы производится ее классификация, или категорирование в случае ОКИИ, а на основе их классификации определяются актуальные для информационной системы угрозы, уязвимости и меры защиты информации, достаточные для нейтрализации актуальных угроз. Таким образом происходит построение системы защиты информации в Российской Федерации.

Оценка рисков осуществляется в ряде стандартов: с ГОСТ Р 59329–2021 по ГОСТ Р 59357–2021. Они определяют риски на разных этапах либо как мгновенное значение, либо как процесс, протекающий столько, сколько живет информационная система. Однако в указанных стандартах описываются и оцениваются риски, но отсутствует описание процесса их обработки [35].

Несмотря на то что главная цель защиты информации – недопущение реализации рисков, система защиты направлена в первую очередь на нейтрализацию угроз. При этом угрозы с рисками либо связаны опосредованно, как в случае ГИС через потенциал нарушителя, либо не связаны совсем. Также для эффективного менеджмента информационной безопасности требуется учитывать связь рисков, угроз и уязвимостей. В нормативных правовых актах (далее – НПА), регламентирующих защиту информации и использующихся при построении системы защиты, практически не прослеживается непрерывная связь между рисками, угрозами и уязвимостями. На практике при изменении хотя бы одного из этих факторов должны быть пересмотрены и остальные. Для своевременного отслеживания таких изменений разрабатываются системы управления рисками.

В Российской Федерации существуют стандарты, направленные на управление рисками. Для менеджмента рисков информационной безопасности был подготовлен ГОСТ Р ИСО/МЭК 27005 «Информационная безопасность, кибербезопасность и защита частной жизни. Руководство по управлению рисками информационной безопасности. Требования и руководства», 5 октября 2023 года вышел проект обновления этого стандарта. Согласно новой редакции ГОСТ Р ИСО/МЭК 27005–2022, риском является влияние неопределенности на достижение поставленных целей. Также в новом издании было увеличено число факторов, влияющих на определение критериев последствий, оценки и принятия рисков, а также дополнительно были рассмотрены критерии вероятности и определения уровня риска. Этот государственный стандарт предназначен для обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска [5].

После осуществления классификации объекта, определения неприемлемых рисков и рисков на разных этапах жизненного цикла необходимо применить подходы по управлению рисками. Учитывая ГОСТ Р ИСО/МЭК 27005 и ряд стандартов с ГОСТ Р 59329–2021 по ГОСТ Р 59357–2021, а также построение связи между рисками, угрозами и уязвимостями, можно построить эффективную систему управления рисками, при этом эффективность такой системы требуется оценивать по определенным критериям (рис. 1) [35].

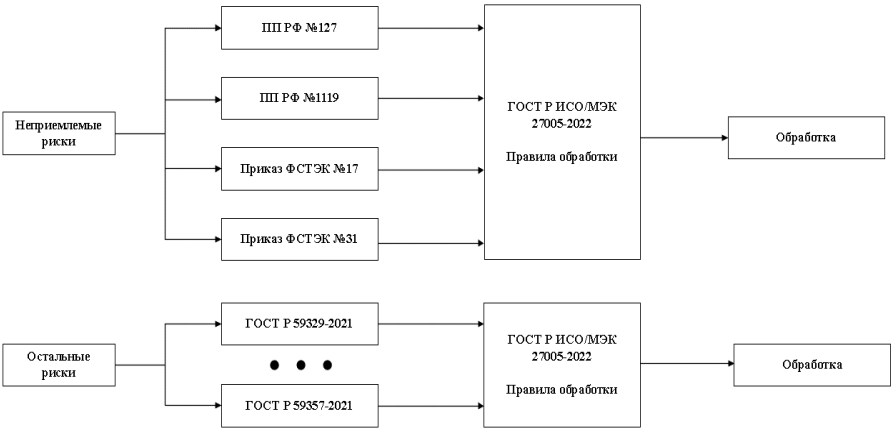

Рис. 1. Схема обработки рисков

Fig. 1. Risk processing scheme

1. ОБРАБОТКА ОСТАТОЧНОГО РИСКА

Объекты критической информационной инфраструктуры имеют особенность: из их определения вытекает отсутствие конструктивного механизма исчисления ущерба как инструмента управления безопасностью критической информационной инфраструктуры (далее – КИИ). Также в определениях не только КИИ, но и АСУ ТП, ГИС, МИС, ИСПДн присутствуют термины «недопустимый», «неприемлемый» в отношении ущерба, порождаемого инцидентом. При проекции данного подхода на управление безопасностью это приводит к тому, что неприемлемость возможного ущерба означает недопустимость остаточного риска, в том числе невозможность использования этого понятия для описания целевого состояния безопасности объекта. Субъективная вероятность инцидента (мера экспертной уверенности в том, что данное событие состоится в действительности) явно отлична от нуля, но при этом не может быть снижена до нуля в силу отсутствия методов доказательства полноты применяемой модели угроз. Всё это в совокупности приводит к двум проблемам:

- к неограниченности использования защитных мер в условиях ограниченности ресурсов, выделяемых организацией для обеспечения безопасности;
- принципиальной недостижимости целевого состояния объекта управления в рамках традиционного рискориентированного подхода к управлению безопасностью.

Из сочетания условий ненулевой субъективной вероятности и недопустимости остаточного риска следует принципиальная недостижимость целевого состояния объекта управления в рамках традиционного рискориентированного подхода к управлению безопасностью [36].

Учитывая эти особенности управления безопасностью, предполагается использование методологии, основанной не на идентификации угроз возникновения рисков и самих рисков, а на идентификации активностей по их компенсации. Такой подход позволяет дополнить идентификацию рисков через непосредственную связь рисков и видов применяемых защитных мер. В данном случае целью обеспечения безопасности является исчерпание потенциала защиты независимо от содержания и направленности агрессивных проявлений. Целевое состояние безопасности определяется в терминах видов и характеристик защитной деятельности, а не в терминах угроз и гармонизированных с ними сущностей, таких как нарушитель, актив, уязвимость и прочие. Это позволяет прекратить использование оценки компенсации некоторого набора актуальных угроз, претендующего на исчерпывающую полноту.

Однако в рамках этой методологии также существует проблема оценки исчерпывающей полноты при анализе комплекса защитных мер, поэтому предлагается использование асимптотического управления безопасностью, подразумевающего процесс приближения к цели. В данном случае используются все возможные защитные активности, внедрение каждой из которых повышает уровень защищенности, но с учетом ограниченности выделяемых на безопасность объекта ресурсов [37].

При реализации этого принципа управления безопасностью даже при наличии в информационной системе реализованных защитных мер и средств остается необходимость дальнейшей обработки остаточных неприемлемых рисков. Это обусловлено тем, что в рассматриваемой системе может иметь место неполное внедрение всех необходимых мер (например, из-за ограниченности выделяемого на безопасность бюджета), регулярное появление обходных мер, отсутствие полной нейтрализации рисков имеющимися мерами и средствами и прочее. В любом случае существующий остаточный риск необходимо уменьшать путем внедрения дополнительных средств защиты информации или совершенствования имеющихся. Этот процесс потребует дополнительных затрат, но при этом его реализация позволит уменьшать этот риск (или, как минимум, не давать ему увеличиваться), и, как следствие, организация будет нести меньше дополнительных убытков, связанных с реализацией этого ущерба.

2. АНАЛИЗ СТАНДАРТОВ ПО СИСТЕМНОЙ ИНЖЕНЕРИИ

В 2021 году было принято 29 стандартов по системной инженерии: с ГОСТ Р 59329–2021 по ГОСТ Р 59357–2021 – разработанные на основе ГОСТ Р 57193–2016, в которых описана оценка рисков, возникающих на разных этапах жизненного цикла. В рамках исследуемой темы были рассмотрены стандарты, описывающие процессы на стадии эксплуатации, поэтому из исследования были исключены следующие стандарты:

- ГОСТ Р 59345–2021 «Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы» [22];
- ГОСТ Р 59357–2021 «Системная инженерия. Защита информации в процессе изъятия и списания системы» [34].

Список всех госстандартов и соответствующих им процессов приведен в таблице.

Стандарты по системной инженерии

System engineering standards

Стандарт системной инженерии	Системные процессы
ГОСТ Р 59329–2021 [6]	Процессы приобретения и поставки продукции и услуг для системы
ГОСТ Р 59330–2021 [7]	Процесс управления моделью жизненного цикла системы
ГОСТ Р 59331–2021 [8]	Процесс управления инфраструктурой системы
ГОСТ Р 59332–2021 [9]	Процесс управления портфелем проектов
ГОСТ Р 59333–2021 [10]	Процесс управления человеческими ресурсами системы
ГОСТ Р 59334–2021 [11]	Процесс управления качеством системы
ГОСТ Р 59335–2021 [12]	Процесс управления знаниями о системе
ГОСТ Р 59336–2021 [13]	Процесс планирования проекта
ГОСТ Р 59337–2021 [14]	Процесс оценки и контроля проекта
ГОСТ Р 59338–2021 [15]	Процесс управления решениями
ГОСТ Р 59339–2021 [16]	Процесс управления рисками для системы
ГОСТ Р 59340–2021 [17]	Процесс управления конфигурацией системы
ГОСТ Р 59341–2021 [18]	Процесс управления информацией системы
ГОСТ Р 59342–2021 [19]	Процесс измерений системы
ГОСТ Р 59343–2021 [20]	Процесс гарантии качества для системы
ГОСТ Р 59344–2021 [21]	Процесс анализа бизнеса или назначения системы
ГОСТ Р 59345–2021 [22]	Процесс определения потребностей и требований заинтересованной стороны для системы
ГОСТ Р 59346–2021 [23]	Процесс определения системных требований
ГОСТ Р 59347–2021 [24]	Процесс определения архитектуры системы
ГОСТ Р 59348–2021 [25]	Процесс определения проекта
ГОСТ Р 59349–2021 [26]	Процесс системного анализа
ГОСТ Р 59350–2021 [27]	Процесс реализации системы
ГОСТ Р 59351–2021 [28]	Процесс комплексирования системы
ГОСТ Р 59352–2021 [29]	Процесс верификации системы
ГОСТ Р 59353–2021 [30]	Процесс передачи системы
ГОСТ Р 59354–2021 [31]	Процесс аттестации системы
ГОСТ Р 59355–2021 [32]	Процесс функционирования системы
ГОСТ Р 59356–2021 [33]	Процесс сопровождения системы
ГОСТ Р 59357–2021 [34]	Процесс изъятия и списания системы

Для прогнозирования рисков применяют методы вычисления количественных показателей. В большинстве ГОСТов распространены следующие количественные показатели:

- риск нарушения надежности реализации процесса без учета требований по защите информации, который характеризуется:

– риском невыполнения необходимых действий процесса, определяемым вероятностью невыполнения необходимых действий процесса;

– риском нарушения сроков выполнения необходимых действий, определяемым вероятностью нарушения сроков выполнения необходимых действий;

- риск нарушения требований по защите информации в процессе;
- интегральные риски нарушения реализации процесса с учетом требований по защите информации.

При оценке риска невыполнения необходимых действий процесса вероятность $R_{\text{действий } k}$ невыполнения необходимых действий процесса для k-й группы за задаваемое время $T_{\text{зад } k}$ определяется так:

$$R_{\text{действий } k}(T_{\text{зад } k}) = G_{\text{наруш } k}(T_{\text{зад } k}) / G_k(T_{\text{зад } k}), \quad (1)$$

где $G_{\text{наруш } k}(T_{\text{зад } k})$ и $G_k(T_{\text{зад } k})$ – соответственно количество случаев нарушений при выполнении необходимых действий процесса и общее количество необходимых действий из k-й группы, подлежащих выполнению за заданное время $T_{\text{зад } k}$ согласно статистическим данным.

Вероятность $R_{\text{действий}}(T_{\text{зад } k})$ невыполнения необходимых действий процесса по всему множеству действий согласно статистическим данным:

- для варианта, когда учитывают все действия (как с завершенным выполнением, так и с их невыполнением):

$$R_{\text{действий}}(T_{\text{зад}}) = 1 - \sum_{k=1}^{K} W_k (1 - R_{\text{действий } k}(T_{\text{зад } k})) \Big/ \sum_{k=1}^{K} W_k ; \quad (2)$$

- для варианта, когда учитывают лишь те случаи, для которых необходимые действия процесса не были выполнены или завершены требуемым образом (именно они определяют возможные ущербы от невыполнения процесса):

$$R_{\text{действий}}(T_{\text{зад}}) = 1 - \sum_{k=1}^{K} W_k (1 - R_{\text{действий } k}(T_{\text{зад } k})) Ind_{\text{действий}}(\alpha_k) \Big/ \sum_{k=1}^{K} W_k , \quad (3)$$

где $T_{\text{зад}}$ – задаваемое суммарное время на реализацию процесса для всего множества действий из различных групп, включающее в себя все частные значения $T_{\text{зад}\,k}$ с учетом их наложений; W_k – количество учитываемых действий из k-й группы при многократных реализациях процесса.

Для k-й группы учитывают требование к выполнению действий процесса с использованием индикаторной функции $Ind(u) = Ind_{\text{действий}}(\alpha_k)$, которая позволяет учесть последствия, связанные с невыполнением необходимых действий процесса:

$$Ind(\alpha) = \begin{cases} 1, \text{ если условие } \alpha \text{ выполнено,} \\ 0, \text{ если условие } \alpha \text{ не выполнено.} \end{cases} \quad (4)$$

Условие α_k означает совокупность условий выполнения в требуемом объеме и завершения всех действий процесса при соблюдении ограничений на задаваемое время $T_{\text{зад}\,k}$.

Оценка рисков нарушения сроков выполнения необходимых действий процесса (определяемая вероятностью нарушения сроков выполнения $R_{\text{с.в}}$) вычисляется аналогичным образом по формулам (1) – (4).

Определение вероятности риска нарушения требований по защите информации в моделируемой системе $R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$ в течение периода прогноза $T_{\text{зад}}$ осуществляется по формуле

$$R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}}) =$$

$$= 1 - P(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}}), \quad (5)$$

где $P_{\text{возд}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$ – вероятность отсутствия нарушений по защите информации в моделируемой системе в течение периода $T_{\text{зад}}$.

Возможны два варианта:

- вариант 1 – заданный период прогноза $T_{\text{зад}}$ меньше периода между окончаниями соседних контролей ($T_{\text{зад}} < T_{\text{меж}} + T_{\text{диаг}}$);
- вариант 2 – заданный период прогноза $T_{\text{зад}}$ больше или равен периоду между окончаниями соседних контролей ($T_{\text{зад}} \geq T_{\text{меж}} + T_{\text{диаг}}$), то есть за это время заведомо произойдет один или более контролей системы с восстанов-

лением нарушенного выполнения требований по защите информации (если нарушения имели место к началу контроля).

В первом случае при условии независимости исходных характеристик вероятность $P_{\text{возд}(1)}(\sigma,\ \beta,\ T_{\text{меж}},\ T_{\text{диаг}},\ T_{\text{восст}},\ T_{\text{зад}})$ отсутствия нарушений требований по защите информации в моделируемой системе в течение периода прогноза $T_{\text{зад}}$ вычисляют по формуле

$$P_{\text{возд}(1)} = \begin{cases} (\sigma - \beta^1)^1 \left(\sigma e^{T_{\text{зад}} 1\beta} - \beta^1 e^{\sigma T_{\text{зад}}} \right), \text{ если } \sigma \neq \beta^1, \\ e^{\sigma T_{\text{зад}}} [1 + \sigma T_{\text{зад}}], \text{ если } \sigma \neq \beta^1. \end{cases} \quad (6)$$

Во втором случае данную величину определяют по формуле

$$P_{\text{возд}(2)} = P_{\text{серед}} - P_{\text{кон}}, \quad (7)$$

где $P_{\text{серед}}$ – вероятность отсутствия нарушений требований по защите информации в системе в течение всех периодов между системными контролями, целиком вошедшими в границы времени $T_{\text{зад}}$, вычисляемая по формуле

$$P_{\text{серед}} = P^N_{\text{возд}(1)}(\sigma,\ \beta,\ T_{\text{меж}},\ T_{\text{диаг}},\ T_{\text{меж}} + T_{\text{диаг}}), \quad (8)$$

где N – число периодов между диагностиками, которые целиком вошли в границы времени $T_{\text{зад}}$ с округлением до целого числа, $N = [T_{\text{зад}} / T_{\text{меж}} + T_{\text{диаг}}]$ – целая часть; $P_{\text{кон}}$ – вероятность отсутствия нарушений по защите информации после последнего системного контроля в конце периода прогноза до истечения времени $T_{\text{зад}}$, получаемая по формуле

$$P_{\text{кон}} = P_{\text{возд}(1)}(\sigma,\ \beta,\ T_{\text{меж}},\ T_{\text{диаг}},\ T_{\text{ост}}), \quad (9)$$

где $T_{\text{ост}}$ – остаток времени в общем заданном периоде $T_{\text{зад}}$ по завершении N полных периодов, определяемый по формуле [7]

$$T_{\text{ост}} = T_{\text{зад}} - N(T_{\text{меж}} + T_{\text{диаг}}). \quad (10)$$

Расчет риска нарушения требований по защите информации для систем сложной структуры осуществляется четырьмя инженерными способами.

Первый способ позволяет использовать одни и те же модели для расчетов различных показателей по области их приложения. Поскольку модели математические, то путем смыслового переопределения исходных данных возможно использование одних и тех же моделей для оценки показателей, различающихся по смыслу, но идентичных по методу их расчета

Второй способ позволяет переходить от оценок моделируемых систем или отдельных элементов, представляемых в виде «черного ящика», к оценкам систем сложной параллельно-последовательной логической структуры. В формируемой структуре исходя из реализуемых технологий для моделируемой системы, состоящей из двух элементов, взаимовлияющих на сохранение выполнения требований по защите информации в системе, указывается характер их логического соединения. Если два элемента соединяются последовательно, что означает логическое соединение «И», то в контексте защиты информации это интерпретируется так: «система обеспечивает выполнение требований по защите информации в течение времени *t*, если 1-й элемент “И” 2-й элемент сохраняют свои возможности по выполнению требований по защите информации в течение этого времени». Если два элемента соединяются параллельно, что означает логическое соединение «ИЛИ», это интерпретируется так: «система сохраняет возможности по выполнению требований по защите информации в течение времени *t*, если 1-й элемент “ИЛИ” 2-й элемент сохраняют свои возможности по выполнению требований по защите информации в течение этого времени». Рекурсивное применение соотношений логических элементов «И» и «ИЛИ» «снизу вверх» обеспечивает получение соответствующих вероятностных оценок для сколь угодно сложной логической структуры с параллельно-последовательным логическим соединением элементов.

Для комплексной оценки в приложении к сложным системам используются рассчитанные на моделях вероятности нарушения требований по защите информации каждого из составных элементов за заданное время *t*. Тогда для простейшей структуры из двух независимых элементов вероятность нарушения требований по защите информации за время *t* определяют по формулам:

- для моделируемой системы из двух последовательно соединенных элементов

$$P(t) = 1 - [1 - P_1(t)] \cdot [1 - P_2(t)]; \qquad (11)$$

- для моделируемой системы из двух параллельно соединенных элементов

$$P(t) = P_1(t) \cdot P_2(t), \qquad (12)$$

где $P_m(t)$ – вероятность нарушения требований по защите информации m-го элемента за заданное время t, $m = 1, 2$ [18].

При прогнозировании интегрального риска вычисляется вероятность нарушения надежности реализации процесса без учета требований по защите информации $R_{\text{интегр}}(T_{\text{зад}})$. В случае учета всех действий (с выполненными и нарушенными условиями по выполнению необходимых действий процесса и соблюдению сроков их выполнения) вероятность определяется по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - \left\{ \sum_{k=1}^{K} W_k (1 - R_{\text{действий } k}(T_{\text{зад } k})) + \right.$$

$$\left. + \sum_{i=1}^{I} M_i (1 - R_{\text{св } i}(T_{\text{зад } i})) \right\} \Bigg/ \left(\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i \right). \qquad (13)$$

При учете только тех случаев, для которых условия по выполнению необходимых действий процесса и/или соблюдению сроков их выполнения были нарушены (именно они определяют возможные ущербы) вероятность считается по формуле

$$R_{\text{интегр}}(T_{\text{зад}}) = 1 - \left\{ \sum_{k=1}^{K} W_k (1 - R_{\text{действий } k}(T_{\text{зад } k})) Ind_{l\text{действий}}(\alpha_k) + \right.$$

$$\left. + \sum_{i=1}^{I} M_i (1 - R_{\text{св } i}(T_{\text{зад } i})) Ind_{l\text{действий}}(\alpha_i) \right\} \Bigg/ \left(\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i \right). \qquad (14)$$

Интегральную вероятность нарушения реализации процесса управления жизненным циклом системы с учетом требований по защите информации $R_{\text{интегр.уч}}(T_{\text{зад}})$ в течение периода прогноза $T_{\text{зад}}$ вычисляют по формуле [7]

$$R_{\text{интегр.уч}}(T_{\text{зад}}) = 1 - [1 - R_{\text{интегр}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})]. \qquad (15)$$

Перечисленные количественные показатели позволяют прогнозировать риски с учетом параметров функционирования системы.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критиче-

ски важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

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

3. Постановление Правительства Российской Федерации от 01.11.2012 № 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.

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

5. ГОСТ Р ИСО/МЭК 27005–2022. Информационная безопасность, кибербезопасность и защита частной жизни. Руководство по управлению рисками информационной безопасности. Требования и руководства: проект, первая редакция. – М.: РСТ, 2023. – 100 с.

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

7. ГОСТ Р 59330–2021. Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы. – М.: Стандартинформ, 2021. – 24 с.

8. ГОСТ Р 59331–2021. Системная инженерия. Защита информации в процессе управления инфраструктурой системы. – М.: Стандартинформ, 2021. – 40 с.

9. ГОСТ Р 59332–2021. Системная инженерия. Защита информации в процессе управления портфелем проектов. – М.: Стандартинформ, 2021. – 28 с.

10. ГОСТ Р 59333–2021. Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы. – М.: Стандартинформ, 2021. – 36 с.

11. ГОСТ Р 59334–2021. Системная инженерия. Защита информации в процессе управления качеством системы. – М.: Стандартинформ, 2021. – 26 с.

12. ГОСТ Р 59335–2021. Системная инженерия. Защита информации в процессе управления знаниями о системе. – М.: Стандартинформ, 2021. – 40 с.

13. ГОСТ Р 59336–2021. Системная инженерия. Защита информации в процессе планирования проекта. – М.: Стандартинформ, 2021. – 24 с.

14. ГОСТ Р 59337–2021. Системная инженерия. Защита информации в процессе оценки и контроля проекта. – М.: Стандартинформ, 2021. – 28 с.

15. ГОСТ Р 59338–2021. Системная инженерия. Защита информации в процессе управления решениями. – М.: Стандартинформ, 2021. – 41 с.

16. ГОСТ Р 59339–2021. Системная инженерия. Защита информации в процессе управления рисками для системы. – М.: Стандартинформ, 2021. – 42 с.

17. ГОСТ Р 59340–2021. Системная инженерия. Защита информации в процессе управления конфигурацией системы. – М.: Стандартинформ, 2021. – 24 с.

18. ГОСТ Р 59341–2021. Системная инженерия. Защита информации в процессе управления информацией системы. – М.: Стандартинформ, 2021. – 58 с.

19. ГОСТ Р 59342–2021. Системная инженерия. Защита информации в процессе измерений системы. – М.: Стандартинформ, 2021. – 26 с.

20. ГОСТ Р 59343–2021. Системная инженерия. Защита информации в процессе гарантии качества для системы. – М.: Стандартинформ, 2021. – 42 с.

21. ГОСТ Р 59344–2021. Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы. – М.: Стандартинформ, 2021. – 26 с.

22. ГОСТ Р 59345–2021. Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы. – М.: Стандартинформ, 2021. – 41 с.

23. ГОСТ Р 59346–2021. Системная инженерия. Защита информации в процессе определения системных требований. – М.: Стандартинформ, 2021. – 62 с.

24. ГОСТ Р 59347–2021. Системная инженерия. Защита информации в процессе определения архитектуры системы. – М.: Стандартинформ, 2021. – 38 с.

25. ГОСТ Р 59348–2021. Системная инженерия. Защита информации в процессе определения проекта. – М.: Стандартинформ, 2021. – 26 с.

26. ГОСТ Р 59349–2021. Системная инженерия. Защита информации в процессе системного анализа. – М.: Стандартинформ, 2021. – 70 с.

27. ГОСТ Р 59350–2021. Системная инженерия. Защита информации в процессе реализации системы. – М.: Стандартинформ, 2021. – 26 с.

28. ГОСТ Р 59351–2021. Системная инженерия. Защита информации в процессе комплексирования системы. – М.: Стандартинформ, 2021. – 27 с.

29. ГОСТ Р 59352–2021. Системная инженерия. Защита информации в процессе верификации системы. – М.: Стандартинформ, 2021. – 24 с.

30. ГОСТ Р 59353–2021. Системная инженерия. Защита информации в процессе передачи системы. – М.: Стандартинформ, 2021. – 24 с.

31. ГОСТ Р 59354–2021. Системная инженерия. Защита информации в процессе аттестации системы. – М.: Стандартинформ, 2021. – 27 с.

32. ГОСТ Р 59355–2021. Системная инженерия. Защита информации в процессе функционирования системы. – М.: Стандартинформ, 2021. – 36 с.

33. ГОСТ Р 59356–2021. Системная инженерия. Защита информации в процессе сопровождения системы. – М.: Стандартинформ, 2021. – 42 с.

34. ГОСТ Р 59357–2021. Системная инженерия. Защита информации в процессе изъятия и списания системы. – М.: Стандартинформ, 2021. – 24 с.

35. *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.

36. *Ерохин С.Д., Петухов А.Н., Пилюгин П.Л.* Принципы и задачи асимптотического управления безопасностью критических информационных инфраструктур // T-Comm: Телекоммуникации и транспорт. – 2019. – Т. 13, № 12. – С. 29–35. – DOI: 10.24411/2072-8735-2018-10330.

37. *Erokhin S., Petukhov A., Pilyugin P.* Critical information infrastructure security modeling // 2019 24th Conference of Open Innovations Association (FRUCT), Moscow, Russia. – IEEE, 2019. – P. 82–88. – DOI: 10.23919/FRUCT.2019.8711960.

Мартыненко Кирилл Кириллович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: k.martynenko.2019@stud.nstu.ru

Ценина Анна Валерьевна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность, компьютерные системы. E-mail: cenina.2020@stud.nstu.ru

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

DOI: 10.17212/2782-2230-2024-1-23-41

Some issues of risk management of information security threats*

K.K. Martynenko[1], A.V. Tsenina[2], V.V. Selifanov[3]

[1] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: k.martynenko.2019@stud.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: cenina.2020@stud.nstu.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Avenue, Novosibirsk, 630073, Russian Federation, senior lecturer of the Department of Information Security. E-mail: sfo1@mail.ru*

The article proposes an approach to assessing the risks of information security of automated technological process control systems, state information systems, municipal information systems, personal data information systems and critical information infrastructure facilities based on the requirements of the legislation of the Russian Federation in the field of protection of these types of information systems, the draft of State Standard R ISO/IEC 27005, planned to be adopted in the near future, and standards for risk assessment within the framework of processes in the life cycle State Standards 59329-59357 published in 2021. These standards are based on State Standard R 57193-2016, which describes the life cycle processes of human-made systems. The problem of processing residual risk in relation to unacceptable risks was considered, after the analysis of which another principle of safety management was proposed. A methodology for assessing confidence in the risk management system was obtained, with the help of which it is necessary to build a risk management system at the objects of critical information infrastructure.

Keywords: critical information infrastructure, state information systems, automated systems, automated process control systems, municipal information systems, personal data information systems, risk, unacceptable risk, residual risk, protection system, information protection, standard, information system

REFERENCES

1. 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).

2. Order of the FSTEC of Russia dated February, 2013 No. 17 "On approval of requirements for the protection of information not constituting a state secret contained in state information systems". (In Russian).

* *Received 11 February 2024.*

3. 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". *Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation*, 2012, no. 45, pt. 4, art. 6257. (In Russian).

4. Decree of the Government of the Russian Federation dated February 08, 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).

5. State Standard R ISO/MEK 27005–2022. *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*. Project, first edition. Moscow, RST Publ., 2023. 100 p. (In Russian).

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

7. State Standard R 59330–2021. *System engineering. Protection of information in system life cycle model management process*. Moscow, Standartinform Publ., 2021. 24 p. (In Russian).

8. State Standard R 59331–2021. *System engineering. Protection of information in system infrastructure management process*. Moscow, Standartinform Publ., 2021. 40 p. (In Russian).

9. State Standard R 59332–2021. *System engineering. Protection of information in project portfolio management process*. Moscow, Standartinform Publ., 2021. 28 p. (In Russian).

10. State Standard R 59333–2021. *System engineering. Protection of information in system human resource management process*. Moscow, Standartinform Publ., 2021. 36 p. (In Russian).

11. State Standard R 59334–2021. *System engineering. Protection of information in system quality management process*. Moscow, Standartinform Publ., 2021. 26 p. (In Russian).

12. State Standard R 59335–2021. *System engineering. Protection of information in knowledge management process about system*. Moscow, Standartinform Publ., 2021. 40 p. (In Russian).

13. State Standard R 59336–2021. *System engineering. Protection of information in project planning process*. Moscow, Standartinform Publ., 2021. 24 p. (In Russian).

14. State Standard R 59337–2021. *System engineering. Protection of information in project assessment and control process*. Moscow, Standartinform Publ., 2021. 28 p. (In Russian).

15. State Standard R 59338–2021. *System engineering. Protection of information in decision management process*. Moscow, Standartinform Publ., 2021. 41 p. (In Russian).

16. State Standard R 59339–2021. *System engineering. Protection of information in risk management process for system*. Moscow, Standartinform Publ., 2021. 42 p. (In Russian).

17. State Standard R 59340–2021. *System engineering. Protection of information in system configuration management process*. Moscow, Standartinform Publ., 2021. 24 p. (In Russian).

18. State Standard R 59341–2021. *System engineering. Protection of information in system information management process*. Moscow, Standartinform Publ., 2021. 58 p. (In Russian).

19. State Standard R 59342–2021. *System engineering. Protection of information in system measurement process*. Moscow, Standartinform Publ., 2021. 26 p. (In Russian).

20. State Standard R 59343–2021. *System engineering. Protection of information in quality assurance process for system*. Moscow, Standartinform Publ., 2021. 42 p. (In Russian).

21. State Standard R 59344–2021. *System engineering. Protection of information in system business or mission analysis process*. Moscow, Standartinform Publ., 2021. 26 p. (In Russian).

22. State Standard R 59345–2021. *System engineering. Protection of information in stakeholder needs and requirements definition process for system*. Moscow, Standartinform Publ., 2021. 41 p. (In Russian).

23. State Standard R 59346–2021. *System engineering. Protection of information in system requirements definition process*. Moscow, Standartinform Publ., 2021. 62 p. (In Russian).

24. State Standard R 59347–2021. *System engineering. Protection o f information in system architecture definition process*. Moscow, Standartinform Publ., 2021. 38 p. (In Russian).

25. State Standard R 59348–2021. *System engineering. Protection of information in project design definition process*. Moscow, Standartinform Publ., 2021. 26 p. (In Russian).

26. State Standard R 59349–2021. *System engineering. Protection of information in system analysis process*. Moscow, Standartinform Publ., 2021. 70 p. (In Russian).

27. State Standard R 59350–2021. *System engineering. Protection of information in system implementation process*. Moscow, Standartinform Publ., 2021. 26 p. (In Russian).

28. State Standard R 59351–2021. *System engineering. Protection of information in system integration process*. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

29. State Standard R 59352–2021. *System engineering. Protection of information in system verification process*. Moscow, Standartinform Publ., 2021. 24 p. (In Russian).

30. State Standard R 59353–2021. *System engineering. Protection of information in system transition process*. Moscow, Standartinform Publ., 2021. 24 p. (In Russian).

31. State Standard R 59354–2021. *System engineering. Protection of information in system validation process*. Moscow, Standartinform Publ., 2021. 27 p. (In Russian).

32. State Standard R 59355–2021. *System engineering. Protection of information in system operation process*. Moscow, Standartinform Publ., 2021. 36 p. (In Russian).

33. State Standard R 59356–2021. *System engineering. Protection of information in system maintenance process*. Moscow, Standartinform Publ., 2021. 42 p. (In Russian).

34. State Standard R 59357–2021. *System engineering. Protection of information in system disposal process*. Moscow, Standartinform Publ., 2021. 24 p. (In Russian).

35. 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.

36. Erokhin S.D., Petukhov A.N., Pilyugin P.L. Printsipy i zadachi asimptoticheskogo upravleniya bezopasnost'yu kriticheskikh informatsionnykh infrastruktur [Principles and tasks of asymptotic security management of critical information infrastructures]. *T-Comm: Telekommunikatsii i transport = T-Comm*, 2019, vol. 13, no. 12, pp. 29–35. DOI: 10.24411/2072-8735-2018-10330. (In Russian).

37. Erokhin S., Petukhov A., Pilyugin P. Critical information infrastructure security modeling. *2019 24th Conference of Open Innovations Association (FRUCT)*, Moscow, Russia. IEEE, 2019, pp. 82–88. DOI: 10.23919/FRUCT.2019.8711960.

Для цитирования:

Мартыненко К.К., *Ценина А.В.*, *Селифанов В.В.* Некоторые вопросы управления рисками реализации угроз безопасности информации // Безопасность цифровых технологий. – 2024. – № 1 (112). – С. 23–41. – DOI: 10.17212/2782-2230-2024-1-23-41.

For citation:

Martynenko K.K., Tsenina A.V., Selifanov V.V. Nekotorye voprosy upravleniya riskami realizatsii ugroz bezopasnosti informatsii [Some issues of risk management of information security threats]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2024, no. 1 (112). pp. 23–41. DOI: 10.17212/2782-2230-2024-1-23-41.