DOI: 10.55648/1998-6920-2023-17-2-84-92 УДК 004.054.53

Метод оценивания рисков в системах принятия решений с учетом защиты информации

В. В. Селифанов, А. Ю. Солдатов, Е. Ю. Солдатов, А. П. Подлегаев, В. С. Скориков

Сибирский государственный университет геосистем и технологий

Аннотация: В статье предложен подход, с помощью которого возможно осуществлять анализ влияния защищенности информации на процесс управления решениями. Использование подхода в жизненном цикле системы приведет к снижению рисков и будет способствовать выявлению «узких мест», в том числе в области информационной безопасности. Работоспособность показана на примерах.

Ключевые слова: информационная безопасность, анализ рисков, защита информации, управление решениями.

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

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Оценивание рисков и подходы к моделированию

Ключевой целью процесса управления решениями служит обеспечение аналитической основы для определения, характеристики и оценки большинства предпочтительных и наилучших решений, а также вектор действий на каждом этапе жизненного цикла системы.

В процессе управления решением могут возникать угрозы нарушения требуемых условий, необходимых для защиты информации (требований к защите информации системы). Эти риски обычно связаны с объективными и субъективными факторами, ориентированными на защищаемые активы и информацию, в том числе с неопределенностью ответственности за обеспечение защиты информации во время принятия решений [1].

Под риском информационной безопасности понимается возможность того, что угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Итогом процесса управления решениями служат следующие результаты:

– варианты решений, требующие альтернативного системного анализа;

– альтернативные варианты действий;

– предпочтительные решения и вектор действий;

– документально зафиксированные обоснования решений и принятые в обосновании предложения и допущения [2].

Применительно к проектируемой системе, которая в нашем случае представляет собой модель «черного ящика», расчетные показатели следующие [3]:

– риск нарушения надежности реализации процесса управления решениями в течение периода прогноза $R_{\text{надежн}}\left(T_{\text{зад}}\right)$ рассчитывают по моделям и рекомендациям В.2 ГОСТ 59338-2021;

– риск нарушения требований информационной безопасности в процессе управления решениями $R_{наруш}\left(T_{зад}\right)$ рассчитывают по моделям и рекомендациям В.3 ГОСТ 59338-2021 ($T_{\text{зад}}$ – заданный период прогноза);

– интегральный риск нарушения реализации процесса управления решениями с учетом требований по защите информации.

Исследуемые системы могут рассматриваться в виде простой или сложной структуры. В данном исследовании представлена система, построенная по принципу «черного ящика». В данной системе внешнему наблюдателю предоставлены исключительно входные и выходные данные, а структура и внутренние составляющие неизвестны. В случае с моделью системы сложной структуры учитывается совокупность взаимосвязанных элементов, каждый из которых представлен в виде «черного ящика».

2. Интегральный риск

Прогнозирование интегрального риска оценивается в сопоставлении с возможными потерями по следующей формуле [4]:

$$R_{\text{интегр.уч}}\left(T_{\text{зад}}\right)=1-\left[1-R_{\text{надеж}}\left(T_{\text{зад}}\right)\right]\cdot[\,1-R_{\text{наруш}}\left(T_{\text{зад}}\right)],$$

где $R_{\text{надежн}}\left(T_{\text{зад}}\right)$ – риск нарушения надежности реализации процесса управления решениями при периоде прогноза $T_{\text{зад}}$ без учета требований защиты информации и $R_{\text{наруш}}\left(T_{\text{зад}}\right)$ – риск нарушения требований защиты информации в процессе управления решениями в течение периода прогноза $T_{\text{зад}}$.

Сами значения рисков $R_{\text{надежн}}\left(T_{\text{зад}}\right)$ и $R_{\text{наруш}}\left(T_{\text{зад}}\right)$ предлагается рассчитывать по методам, подробно описанным в литературе.

Риск нарушения надежности реализации процесса управления решениями в течение периода прогноза $T_{\text{зад}}$ вычисляется по формуле:

$$R_{\text{надежн}}\left(T_{\text{зад}}\right)=1-P_{\text{возд}}(\sigma,\,\beta,\,T_{\text{меж}},\,T_{\text{диаг}},\,T_{\text{зад}}),\qquad(1)$$

где σ – частота возникновения источников угроз в моделируемой системе с точки зрения нарушения надежности реализации процесса управления решениями,

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

$T_{\text{меж}}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{\text{диаг}}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{\text{зад}}$ – задаваемая длительность периода прогноза.

При соблюдении условий независимости исходных данных риск отсутствия нарушений надежности реализации процесса управления решениями в течение заданного периода прогноза рассчитывают по формуле (вариант 1) [3]:

$$R_{\text{возд}(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1} \left\{\sigma \cdot \exp(-T_{\text{зад}} / \beta) - \beta^{-1} \exp(-\sigma \cdot T_{\text{зад}})\right\}, \text{ если } \sigma \neq \beta^{-1} \\ \exp(-\sigma \cdot T_{\text{зад}})\left[1 + \sigma \cdot T_{\text{зад}}\right], \text{ если } \sigma = \beta \end{cases} \quad (2)$$

В случае следующего варианта при соблюдении условия независимости исходных данных вероятность отсутствия нарушений надежности проведения процесса управления решениями в течение периода прогноза рассчитывают по формуле:

$$P_{\text{возд}(2)} = P_{\text{серед}} \times P_{\text{кон}}, \quad (3)$$

где $P_{\text{серед}}$ – вероятность отсутствия нарушений надежности проведения процесса управления решениями в течение всех заданных периодов между системными контролями, полностью вошедшими в рамки заданного периода времени $T_{\text{зад}}$, вычисляемая по формуле:

$$P_{\text{серед}} = P^{N}_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}} + T_{\text{диаг}}), \quad (4)$$

где N – число периодов между диагностиками, которые полностью вошли в рамки заданного периода времени $T_{\text{зад}}$, с округлением до целого числа.

Вероятность отсутствия нарушений надежности реализации процесса управления решениями после последнего системного контроля вычисляется по формуле:

$$P_{\text{кон}} = P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}}), \quad (5)$$

где $T_{\text{ост}}$ – остаток времени в общем заданном периоде $T_{\text{зад}}$ по завершении N полных периодов, вычисляемый по формуле:

$$T_{\text{ост}} = P_{\text{зад}} - N\left(T_{\text{меж}} + T_{\text{диаг}}\right). \quad (6)$$

3. Пример расчета интегрального риска

В рамках примера при оценке риска были выбраны такие модели, как (рис. 1):

– модели ГОСТ Р 59338-2021 для анализа действий, связанных с планированием управления решениями (действие 1), принятием решений и управлением решениями (действие 3);

– модели, связанные со сбором, обработкой и анализом информации для принятия решений (действие 2), – по ГОСТ Р 59341.

Данное итоговое описание позволяет спроектировать моделируемую систему как структуру следующих последовательных элементов, связанных с действиями процесса управления решениями (рис. 2) [5]:

▪ для планирования процесса управления решениями:

– 1-й элемент – действие 1 для производственного процесса;

– 2-й элемент – действие 1 для процесса технического обслуживания;

– 3-й элемент – действие 1 для процесса контроля качества;

– 4-й элемент – действие 1 для процесса инвентаризации;

▪ для принятия решений и управления решениями:
– 5-й элемент – действие 2 для производственного процесса;
– 6-й элемент – действие 2 для процесса технического обслуживания;
– 7-й элемент – действие 2 для процесса контроля качества;
– 8-й элемент – действие 2 для процесса инвентаризации.

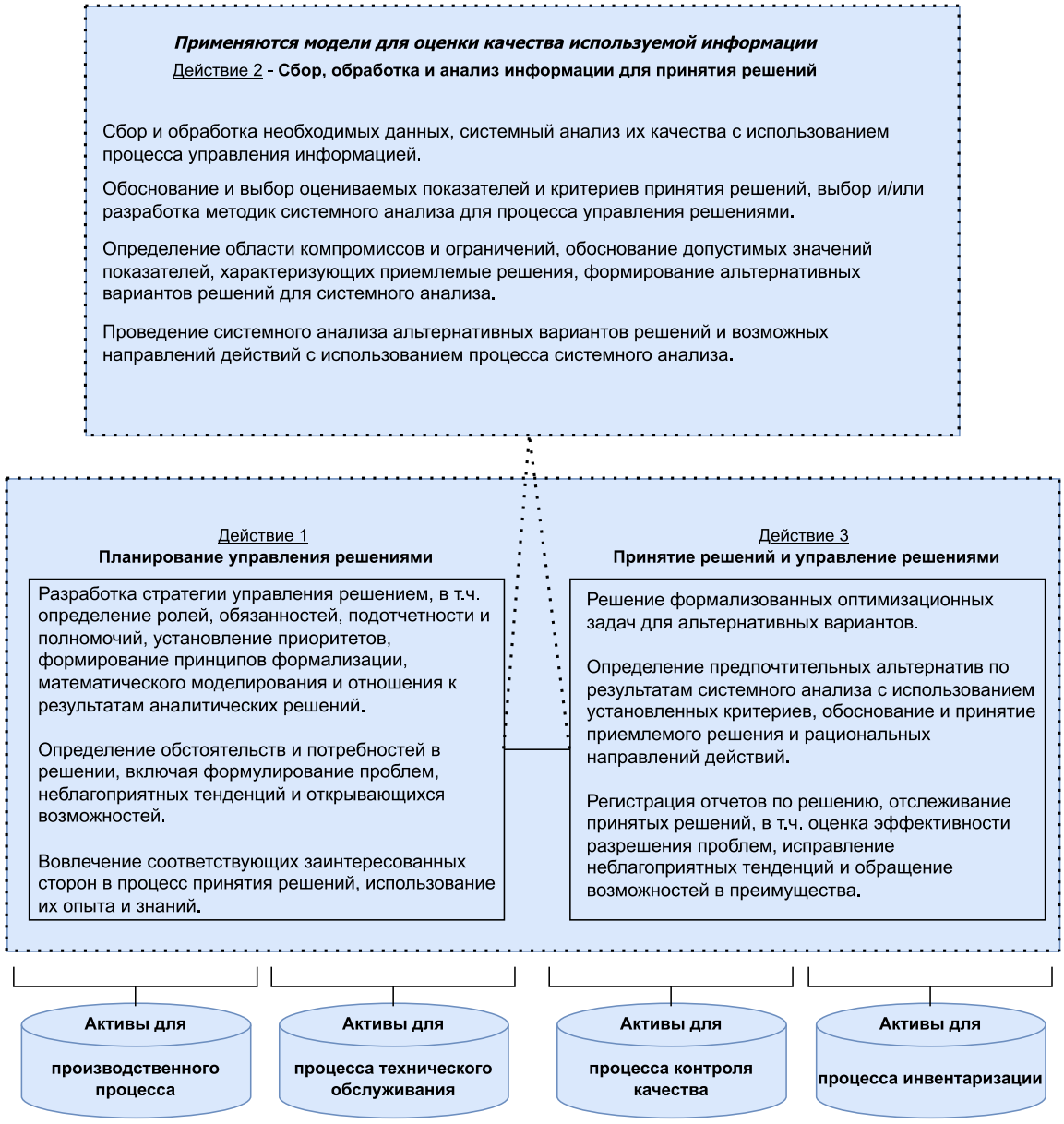

Рис. 1. Представление комплекса действий для оценки риска нарушения надежности

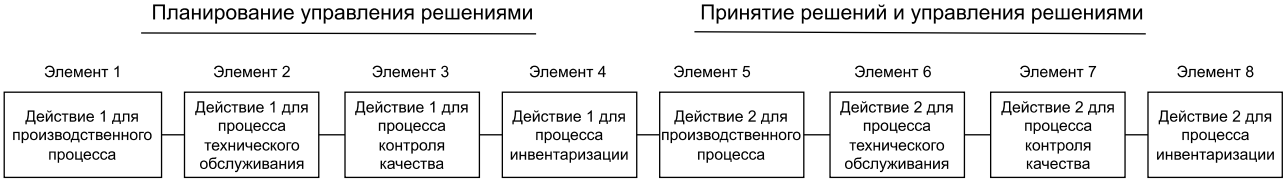

Рис. 2. Структура моделируемой системы без учета требований
по защите информации

В табл. 1 представлены исходные данные для каждого составного элемента.

Таблица 1. Исходные данные для прогнозирования риска нарушения надежности реализации процесса управления решениями

Значения и комментарии		
Исходные данные	для 1-го / 2-го / 3-го / 4-го элементов	для 5-го / 6-го / 7-го / 8-го элементов
σ – частота появления источников угроз нарушения надежности процесса	5 раз в год / 1 раз в год / 1 раз в год / 1 раз в год – это угрозы антропогенных и технических ошибок	2 раза в год / 1 раз в год / 1 раз в год / 1 раз в год – это частота угроз потерь от неразумных действий
β – время от начала возникновения источника угрозы до нарушения с возможными потерями	2 недели / 1 год	6 месяцев / 6 месяцев
$T_{\text{меж}}$ – среднее время между диагностиками возможностей конкретного элемента	8 часов / 8 часов / 8 часов / 8 часов	1 час / 1 неделя / 1 неделя / 1 неделя
$T_{\text{диаг}}$ – среднее время диагностики состояния элемента	10 минут / 10 минут / 10 минут / 10 минут – время обследования перед работой	полминуты – контроль целостности оборудования / 1 час – диагностика / полминуты – длительность контроля / полминуты – длительность инвентаризации
$T_{\text{восст}}$ – среднее время восстановления элемента после выявления нарушений	полчаса / полчаса / полчаса / полчаса – это время, потраченное на замену сотрудника, который был отстранен от работы	4 часа – время, затраченное на восстановление конкретного оборудования / 8 часов – время, затраченное на восстановление тех. процесса / полчаса — время, затраченное на переустановку ПО / 8 часов – время, затраченное на восстановление инвентаризации
$T_{\text{зад}}$ – задаваемая длительность периода прогноза	от 1 месяца до 1 года период, в течение которого сохраняется уверенность в отсутствии превышения риска нарушения надежности	

Единцы измерения всех исходных данных табл. 1 приводятся к тем единицам измерения, которые указаны при задаваемой длительности периода прогноза $T_{\text{зад}}$.

Используя формулы (1–6) и исходные данные табл. 1, мы можем определить вероятность нарушения надежности реализации процесса управления решениями для элемента 1. Подставив значения и проведя математические вычисления, получаем $R_{\text{надежн}}\left(T_{\text{зад}}\right) = 0.067$. Повторяем действия для каждого элемента системы.

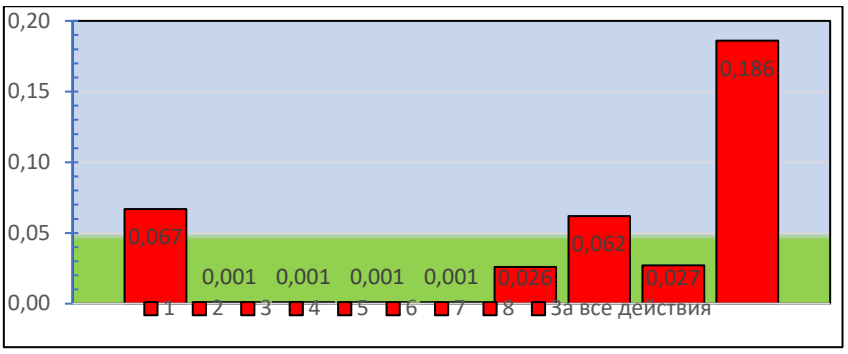

Рис. 3. Риск без учета качества используемой информации

Сложив значения всех элементов, получим значение риска нарушения надежности реализации процесса управления решениями, равное 0.186 (рис. 3). Получаем для 1-го элемента значение 0.067, а для последнего элемента 0.062, что совместно составляет более 69 % от общего риска по всем элементам.

Исходные данные по каждому из 8 элементов, которые учитывают в себе вероятные уязвимости, представлены в табл. Г.2 ГОСТ Р 59338-2021.

Используя данный ГОСТ для вычисления $R_{\text{наруш}}\left(T_{\text{зад}}\right)$, и исходные данные табл. Г.2, получаем значение 0.0025 для элемента 1. Рассчитывая для остальных элементов системы, в 1 – 5, 7 – 8 – около 0.002. Для 6-го элемента – 0.0005. Анализируя, можно сделать вывод, что все активы защищены равнопрочно.

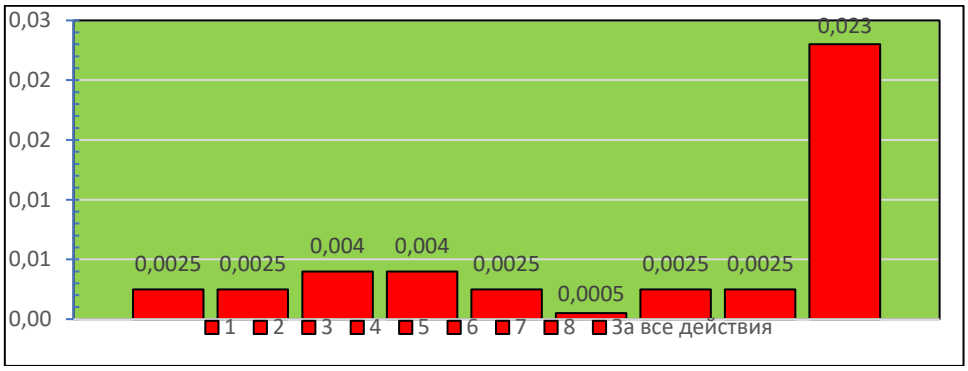

Рис. 4. Риск нарушения требований в течение одного месяца

Основной причиной высокого интегрального риска, значительно превышающего риски повреждения надежного производственного оборудования, является относительно низкий уровень качества используемой информации. Если этот уровень качества будет признан приемлемым или не улучшаемым и клиент (или аналитиком) решит не брать в расчеты качество используемой информации, то может быть использована другая полученная оценка, т.е. в нашем случае 0.012. И тогда, учитывая все вышесказанное, выбираем значение $R_{\text{надежн}}\left(T_{\text{зад}}\right) = 0.012$, а $R_{\text{наруш}}\left(T_{\text{зад}}\right)$ = 0.023. В таком случае:

$$R_{\text{интегр.уч}}\left(T_{\text{зад}}\right) = 1 - \left[1 - 0.012\right] \cdot \left[\ 1 - 0.023\right] = 0.034\,.$$

Таким образом, интегральный риск нарушения реализации процесса управления решениями с учетом требований по защите информации меньше установленного допустимого уровня 0.05, что подтверждает сбалансированность применяемых технических решений с точки зрения достижения целей системной инженерии.

4. Вывод

Данный подход позволяет проводить анализ того, как защищенность информации влияет на реализацию процесса управления решениями. Актуальность и достоверность подтверждена на уровне реализации методов, предложенных в ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе управления решениями».

Литература

1. *Костогрызов А. И., Степанов П. В*. Инновационное управление качеством и рисками в жизненном цикле систем. М.: Изд. «Вооружение, политика, конверсия», 2008. 404 с.
2. *Kostogryzov A.* Probabilistic Modeling in System Engineering // IntechOpen. 2018. 278 p. DOI: 10.5772/intechopen.71396.
3. ГОСТ Р 59338-2021. Системная инженерия. Защита информации в процессе управления решениями. М.: Национальный стандарт РФ, 2021. 45 с.
4. ГОСТ Р 59341-2021. Системная инженерия. Защита информации в процессе управления информационной системы. М.: Национальный стандарт РФ, 2021. 56 с.
5. *Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G*. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. http://www.scirp.org/journal/ajor/

Селифанов Валентин Валерьевич
доцент кафедры информационной безопасности, Сибирский государственный университет геосистем и технологий (СГУГиТ, 630108, Новосибирск, ул. Плахотного, д. 10), e-mail: sfo1@mail.ru, ORCID ID: 0000-0002-6691-5647.

Солдатов Александр Юрьевич
студент, Сибирский государственный университет геосистем и технологий, e-mail: dglasmann@mail.ru, ORCID ID: 0000-0002-5218-1013.

Солдатов Егор Юрьевич
студент, Сибирский государственный университет геосистем и технологий, e-mail: wilgieforz@mail.ru, ORCID ID: 0000-0002-7937-8502.

Подлегаев Александр Игоревич
студент, Сибирский государственный университет геосистем и технологий, e-mail: sanyi_p@mail.ru, ORCID ID: 0000-0001-8617-9731.

Скориков Виталий Сергеевич
студент, Сибирский государственный университет геосистем и технологий, e-mail: isaac.newton01@mail.ru, ORCID ID: 0000-0001-8218-9529.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Risk Assessment Method in Decision-making Systems Taking into Account Information Protection

Valentin.V. Selifanov, Aleksandr.Yu. Soldatov, Egor.Yu. Soldatov, Aleksandr.P. Podlegaev, Vitaly.S. Skorikov

Siberian State University of Geosystems and Technologies

Abstract: The article suggests an approach by which it is possible to analyze the impact of information security on the decision management process. The use of the approach in the life cycle of the system will reduce risks and contribute to the identification of "bottlenecks" including information security. The efficiency of the approach is demonstrated by examples.

Keywords: information security, risk analysis, information security, decision management.

For citation: Selifanov V. V., Soldatov A. Yu., Soldatov E. Yu., Podlegaev A. P., Skorikov V. S. Risk assessment method in decision-making systems taking into account information protection (in Russisn). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 84-92. https://doi.org/10.55648/1998-6920-2023-17-2-84-92.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. Kostogryzov A. I., Stepanov P. V. *Innovacionnoe upravlenie kachestvom i riskami v zhiznennom cikle sistem* [Innovative quality and risk management in the systems life cycle]. Moscow, Publishing house “Armament, politics, conversion”, 2008. 404 p.
2. A.Kostogryzov. *Probabilistic Modeling in System Engineering*. IntechOpen, London, 2018, 278 p. DOI: 10.5772/intechopen.71396.
3. *GOST R 59338-2021. Sistemnaya inzheneriya. Zashchita informatsii v protsesse upravleniya resheniyami* [Russian Standard No. 59338-2021 System engineering. System engineering. Protecting Information in Decision Management], available at: https://internet-law.ru/gosts/gost/75539/ (accessed 06.11.2022).
4. *GOST R 59341-2021. Sistemnaya inzheneriya. Zashchita informatsii v protsesse upravleniya informatsionnoi sistemy* [Russian Standard No. 59341-2021 System engineering. Protection of information in the process of managing an information system], available at: https://docs.cntd.ru/document/1200179349 (accessed 18.11.2022).
5. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov *G*. Prediction and optimization of system quality and risks on the base of modelling processes. *American Journal of Operation Researches. Special Issue*, 2013, v. 1, pp. 217-244, available at: http://www.scirp.org/journal/ajor/ (accessed 19.11.2022).

Selifanov Valentin Valerievich
Associate Professor, Department of Information Security, Siberian State University of Geosystems and Technologies (SSUGiT, 630108, Novosibirsk, Plakhotnogo St., 10), e-mail: sfo1@mail.ru, ORCID ID: 0000-0002-6691-5647.

Soldatov Alexander Yurievich
Student, Siberian State University of Geosystems and Technologies, e-mail: dglasmann@mail.ru, ORCID ID: 0000-0002-5218-1013.

Soldatov Egor Yurievich
Student, Siberian State University of Geosystems and Technologies, e-mail: wilgieforz@mail.ru, ORCID ID: 0000-0002-7937-8502.

Podlegaev Alexander Igorevich
Student, Siberian State University of Geosystems and Technologies, e-mail: sanyi_p@mail.ru, ORCID ID: 0000-0001-8617-9731.

Skorikov Vitaly Sergeevich
Student, Siberian State University of Geosystems and Technologies, e-mail: isaac.newton01@mail.ru, ORCID ID: 0000-0001-8218-9529.