УДК 004.9

# МЕТОДИЧЕСКИЙ ПОДХОД К АНАЛИЗУ РИСКОВ, ВОЗНИКАЮЩИХ В ПРОЦЕССЕ ВЗАИМОДЕЙСТВИЯ ЦЕНТРОВ ОБРАБОТКИ ЗНАНИЙ

**Авдонин Р.Ю.**

*Федеральное государственное учреждение «Федеральный исследовательский центр «Информатика и управление» Российской академии наук», 119333, Россия, Москва, ул. Вавилова 44, корп.2, e-mail: ft.99@yandex.ru*

**Предложен подход к обоснованию системных решений по удержанию рисков в допустимых пределах для возможных сценариев угроз, возникающих в процессе управления знаниями. Использование подхода позволяет оценить воздействие различных угроз на реализацию процесса управления знаниями в центрах обработки знаний. Работоспособность предложенного подхода продемонстрирована на примерах.**

Ключевые слова: анализ, безопасность, прогнозирование, риск, система, управление.

# METHODOLOGICAL APPROACH TO THE ANALYSIS OF RISKS ARISING IN THE PROCESS OF INTERACTION OF KNOWLEDGE PROCESSING CENTERS

**Avdonin R. Yu.**

*Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS), Vavilova Street 44, bld. 2, 119333 Moscow, Russia,e-mail: ft.99@yandex.ru*

**An approach is proposed to justify systemic solutions to keep risks within acceptable limits for possible scenarios of threats that arise in the process of knowledge management. Using the approach allows assessing the impact of various threats on the implementation of the knowledge management process in knowledge processing centers. The efficiency of the proposed approach is demonstrated by examples**

Keywords: analysis, safety, forecasting, risk, system, management.

## 1. Введение

В настоящее время процесс управления знаниями использует в своей работе всё больше предприятий. Это касается разрабатываемых и эксплуатируемых систем, подсистем и процессов. Само предприятие также может быть системой, в интересах которой осуществляется управление знаниями. Целью процесса управления знаниями является повышение эффективности и качества системы, ее безопасности, а также связанных с ней систем за счет приобретения, создания, распространения, применения и сохранения полезных знаний в их жизненном цикле.

В процессе управлении знаниями создаются и приобретаются новые знания, формируются базы и центры обработки знаний (ЦЗн). Происходит взаимодействие ЦЗн, как с человеческими ресурсами, так и взаимодействие между ЦЗн. В этой связи возникает вопрос обеспечения сохранности знаний от разнородных угроз, способных повлиять на надежность реализации процесса взаимодействия ЦЗн. Защита информации, направлена на

обеспечение конфиденциальности, целостности и доступности защищаемой информации, предотвращение несанкционированных и непреднамеренных воздействий на защищаемую информацию.

При достаточном количестве работ по управлению рисками, см., например, [1-10] вопрос прогнозирования рисков, выбора системных способов снижения и удержания рисков в допустимых пределах продолжает оставаться актуальным. Методы анализа рисков для процесса управления знаниями рассматривались в [3,5].

Предлагаемый подход позволяет оценить влияние различных угроз на надежность процесса управления знаниями при взаимодействии ЦЗн, позволяет прогнозировать риски с учетом сложности моделируемой системы и мер по противодействию угрозам в каждом элементе, в результате чего повышается надежность и эффективность процесса взаимодействия.

**2. Общие положения**

Предлагается оценивать риск нарушения надежности реализации процесса управления знаниями, включающий в себя риски выполнения отдельных действий процесса, таких как надежность выполнения процесса (соблюдение сроков доставки приобретенных и созданных полезных знаний и допустимый уровень дефектов в них), достоверность создания и распространения знаний и обобщенный риск нарушения надежности реализации процесса управления знаниями с учетом дополнительных специфических системных требований – см. ГОСТ Р 59993-2022. В качестве примера дополнительных специфических системных требований выступают требования по защите информации. Обобщенный риск нарушения надежности реализации процесса управления знаниями с учетом дополнительных специфических системных требований это сбалансированные действия по обеспечению надежности реализации процесса управления знаниями и заданных дополнительных специфических системных требований, направленных на сохранение рисков в допустимых пределах.

**3. Порядок прогнозирования рисков**

Для прогнозирования рисков предлагается выполнить следующие шаги:

определить моделируемую систему и задать анализируемые объекты прогнозирования рисков

Процесс определения моделируемой системы описан в [3]. Для прогнозирования рисков предлагается определить следующие объекты:

- состав выходных результатов и выполняемых действий процесса управления знаниями и используемых при этом активов;
- перечень потенциальных угроз и возможные сценарии возникновения и развития угроз для выходных результатов;
- технологии противодействия угрозам, используемые в процессе управления знаниями в заданной среде применения системы;
- формализованные требования или условия по завершению необходимых действий процесса управления знаниями, соблюдению сроков поставки знаний, отсутствию брака в приобретаемых и создаваемых знаниях, распространению и применению полезных знаний;
- установить конкретные цели прогнозирования рисков.

Конкретные практические цели прогнозирования рисков устанавливают заказчик системного анализа и/или аналитик моделируемой системы при выполнении работ системной инженерии. Прогнозирование рисков осуществляется в интересах решения определенных задач системного анализа – см. ГОСТ Р 59335-2021;

создать список возможных угроз. Принять решение представить моделируемую систему в виде «Черного ящика» или в виде сложной структуры, разложенной на составные элементы.

Согласно ГОСТ Р 59335-2021 перечень угроз безопасности информации в процессе управления знаниями может включать (в части, свойственной этому процессу):

- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию – по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275;
- угрозы безопасности функционированию программного обеспечения, оборудования и коммуникаций, используемых в процессе работы – по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 54124, ГОСТ Р 56939, ГОСТ Р 58412;
- угрозы безопасности информации при подготовке и обработке документов – по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51583;
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (разработчика, производителя) к конкретному заказчику, информация и информационные системы которого были скомпрометированы;
- угрозы, связанные с приобретением или предоставлением знаний с использованием облачных услуг, которые могут оказать влияние на информационную безопасность организаций, использующих эти услуги;
- угрозы, связанные с нарушением интеллектуальной собственности, а также с несанкционированным распространением знаний о системе за пределы системы;
- угрозы, связанные с неопределенностью ответственности за обеспечение защиты информации в процессе управления знаниями о системе;
- угрозы распространения ложной информации о знаниях, используемых в организации;
- прочие соответствующие угрозы безопасности информации, связанные с человеческим фактором, для информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов из Банка данных угроз, сопровождаемого государственным регулятором;

выбрать расчетные показатели и подходящие математические модели и методы (включая методы повышения их адекватности).

Для прогнозирования рисков предлагается использовать следующие количественные показатели:

$\boldsymbol{R}_{\text{надеж}}(\boldsymbol{T}_{\text{зад}})$ — риск нарушения надежности реализации процесса управления знаниями в течение задаваемого периода прогноза Тзад;

$\boldsymbol{R}_{\text{наруш}}(\boldsymbol{T}_{\text{зад}})$ — риск нарушения требований по защите информации в процессе управления знаниями в течение задаваемого периода прогноза Тзад.;

$\boldsymbol{R}_{\text{обобщ}}(\boldsymbol{T}_{\text{зад}})$ — обобщенный риск нарушения надежности реализации процесса управления знаниями с учетом дополнительных специфических системных требований в течение задаваемого периода прогноза Тзад. Обобщенный риск нарушения производительности процесса управления знаниями зависит от нарушения надежности производительности процесса или от нарушения требований к защите информации, или от того и другого, с серьезностью возможного ущерба.

Предлагаемые методы обоснования системных решений, снижения рисков и/или удержания их в приемлемых пределах представлены ниже в сочетании с примерами и практическими интерпретациями результатов расчетов.

**4. Методы расчетов, примеры**

Для достижения целей по развитию неизученных территорий Российской Федерации перспективных на открытия месторождений необходимо системно решать многочисленные задачи в области социально-экономического развития, развития инфраструктуры, науки и технологий, охраны окружающей среды и экологической безопасности, обеспечения защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, обеспечения безопасности, сохранности и защиты информации. Системное решение всего комплекса задач построено на управлении знаниями, основанном на аналитической обработке разнородных данных мониторинга и обеспечивающем совершенствование, накопление и своевременное применение возникающих знаний. Учитывая сложность и многообразность решаемых практических задач создание нескольких ЦЗн неизбежно. В ситуации реальных и потенциальных угроз безопасности критической информационной инфраструктуры защита информации в ЦЗн имеет приоритетное значение. Не вдаваясь в детали и специфику разнородных знаний, подлежащих интеграции и применению, некоторые практические проблемы, связанные с использованием этого методического подхода, касаются:

- для решения профильных задач обеспечения экологически безопасной морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях (профильные задачи 1-го типа);

- для решения специализированных задач обеспечения комплексной безопасности операций на континентальном шельфе, включая мониторинг и прогнозирование экстремальных ситуаций природного и техногенного характера (профильные задачи 2-го типа);

- для решения специализированных задач по предотвращению и ликвидации аварийных разливов нефти в ледовых условиях, включая создание технологий обнаружения нефти подо льдом (профильные задачи 3-го типа);

- для решения профильных задач разработки технологий комплексного гидрометеорологического и экологического мониторинга опасных природных явлений (профильные задачи 4-го типа);

- для решения профильных задач разработки технологий дистанционного исследования Земли, включая мониторинг окружающей среды, оценку ресурсов и прогнозирование состояния окружающей среды (профильные задачи 5-го типа).

Методический подход иллюстрируется примерами прогнозов:

- риск нарушения надежности выполнения процесса управления знаниями;

- риск нарушения требований по защите информации;

-обобщенный риск нарушения надежности реализации процесса управления знаниями с учетом дополнительных специфических системных требований.

Для определенности с точки зрения системной инженерии для эффективной защиты информации рассматриваются два варианта: создание и эксплуатация пяти автономных специализированных ЦЗн, каждый из которых специализируется на решении своих профильных задач (вариант 1), и добавление единого ЦЗн, объединяющего возможности всех автономных ЦЗн (вариант 2). Принимая во внимание возможные убытки, цели прогнозирования рисков формулируются следующим образом. В условиях существующей неопределенности:

- количественно оценить риск нарушение надежности выполнения процесса управления знаниями;

- количественно оценить риск нарушения требований по защите информации (как по частям для каждого ЦЗн, так и для комплекса всех ЦЗн);

- выявить критические условия при развитии различных угроз;

- количественно оценить обобщенный риск нарушения надежности реализации процесса управления знаниями с учетом дополнительных специфических системных требований;

- определить такой период, в течение которого сохраняются гарантии не превышения допустимых рисков.

Примеры 1-3 показывают оценку риска нарушение надежности выполнения процесса управления знаниями (без учета требований к защите информации). Предполагая соизмеримость возможного ущерба, примеры оценивают вероятности нарушение надежности приобретения и создания полезных знаний и вероятность нарушение надежности распространения приобретенных или созданных полезных знаний и их своевременного применения.

**Пример 1**

В примере показана оценка рисков нарушение надежности выполнения процесса получения знаний.

При оценке рисков нарушение надежности выполнения процесса получения знаний методы системного анализа адаптируются с точки зрения оценки:

- риск неполного выполнения необходимых действий для предоставления приобретенных знаний;

- риск нарушения сроков доставки полученных знаний;

- риск недопустимого уровня дефектов в полученных знаниях (аналитические ошибки, описания, необоснованные выводы и/или рекомендации).

С точки зрения расчетов модели для оценки вышеуказанных рисков идентичны, поскольку при оценке каждого из рисков вычисленные вероятностные меры сравниваются с возможным ущербом, вызванным несоблюдением условий получения знаний.

В приведенном ниже примере показана оценка нарушения надежности своевременной доставки полученных знаний. Оценка неполноты выполнения необходимых действий для предоставления полученных знаний и наличия недопустимого дефекта в полученных знаниях (аналитические ошибки, описания, необоснованные выводы и/или рекомендации) производится по аналогии.

Вероятность $R_{\text{св}\,i}(T_{\text{зад}\,i})$ нарушения условий разовой поставки для знания i-го типа за заданное время $T_{\text{зад}\,i}$ рассчитывается по формуле

$$R_{св\,i}(T_{зад\,i}) = N_{наруш\,i}(T_{зад\,i})/N_i(T_{зад\,i}), \qquad (1)$$

где

$\boldsymbol{N}_{\text{наруш}\,\boldsymbol{i}}\boldsymbol{(T}_{\text{зад}\,\boldsymbol{i}}\boldsymbol{)}$ и $\boldsymbol{N_i(T}_{\text{зад}\,\boldsymbol{i}}\boldsymbol{)}$ – соответственно количество нарушений сроков поставки и общее количество поставок за заданное время $\boldsymbol{T}_{\text{зад}\,\boldsymbol{i}}$ для знаний i-го типа согласно статистическим данным.

Показатель выполнения сроков поставки для знаний k-го типа определен следующим образом

$$Z_{\text{срок}\,i}\,(T_{\text{зад}\,i}) = \begin{cases} 0, & \text{если условия сроков поставки выполнены;} \\ R_{\text{св}\,i}(T_{\text{зад}\,i}) \text{ по формуле (1)}, & \text{если условия не выполнены или не заданы.} \end{cases} \qquad (2)$$

Условие выполнения сроков поставки знаний k-го типа определено как условие непревышения максимально допустимого уровня $\boldsymbol{R}_{\text{доп.св i}}(\boldsymbol{T}_{\text{зад i}})$, задаваемого для вероятности нарушения сроков однократной поставки. Это условие выражается в форме: $\boldsymbol{R}_{\text{св i}}(\boldsymbol{T}_{\text{зад i}}) \leq \boldsymbol{R}_{\text{доп.св i}}(\boldsymbol{T}_{\text{зад i}})$. В выражении для обобщенного риска показатель выполнения сроков поставки для процесса приобретения знаний i-го типа $\boldsymbol{Z}_{\text{срок i}}(\boldsymbol{T}_{\text{зад i}})$ обозначен как $\boldsymbol{Z}(\text{пр})_{\text{срок i}}(\boldsymbol{T}_{\text{зад i}})$.

Вероятность нарушения сроков поставки по всему множеству знаний различных типов, реализуемых в процессе согласно статистическим данным с учетом множественности поставок, характеризуемых исходными данными по каждому из типов знаний, вычисляют по формуле

$$R_{св}(T_{зад}) = 1 - \sum_{i=1}^{I} M_i[1 - R_{св\,i}(T_{зад\,i})] \Big/ \sum_{i=1}^{I} M_i; \qquad (3)$$

Здесь $\boldsymbol{T}_{\text{зад}}$ – задаваемое суммарное время поставки всего множества знаний различных типов, включающее в себя все частные значения $\boldsymbol{T}_{\text{зад}\,\boldsymbol{i}}$ с учетом их наложений, $\boldsymbol{M}_{\boldsymbol{i}}$ – количество учитываемых поставок знаний i-го типа при множественных поставках, в выражении для обобщенного риска применительно к процессу приобретения использовано обозначение M(пр) i , i = 1,…,I(пр).

В соответствии с поставленными задачами по развитию территорий предполагается приобретение нескольких видов знаний i-го типа. Приобретение всех видов знаний за исключением одного проходит без нарушения сроков поставки, т. е. в этом случае $\boldsymbol{Z}_{\text{срок}\,\boldsymbol{i}}(\boldsymbol{T}_{\text{зад}}) = 0$. Следовательно, при оценке риска учитывается только вид приобретаемых знаний, для которого сроки поставки нарушены.

С учетом статистических данных по развитию территорий для определенности условно принимается, что за заданное время $\boldsymbol{T}_{\text{зад}\,\boldsymbol{i}}$ = 1 год для знаний i-го типа общее количество поставок $\boldsymbol{N}_{\boldsymbol{i}}$ = 100, количество нарушений сроков поставки $\boldsymbol{N}_{\text{наруш}\,\boldsymbol{i}}$ = 3, что составляет 3% от общего количества поставок, а количество множественных поставок Mi = 1.

Результаты оценки нарушения надежности реализации процесса создания полезных знаний о системе полностью идентичны результатам этого примера.

**Пример 2**

Пример иллюстрирует оценку рисков нарушение надежности реализации процесса распространения полезных знаний.

Предположим, что с учетом статистических данных частота существенного изменения полезности знаний об условиях в развиваемых территориях, хранящихся в базе знаний системы, составит не более одного изменения в 10 лет, т.е. $\boldsymbol{\xi}$ = 10 лет. Среднее время для приобретения или создания и размещения новых знаний в базе знаний системы (от создателей или распространителей знаний) составит около трех месяцев, т.е. $\boldsymbol{T}_{\text{база знаний}}$ = 3 месяца, что в переводе на те же единицы измерения составляет 0,25 года. Обновления из ЦЗн доставляются потребителям системы ежемесячно, т.е. q = 1 месяц или 0,083 года. Кроме того, накладывается ограничение на вероятность нарушения надежности распространения полезных знаний сверху: эта вероятность не должна превышать максимально допустимый уровень $\boldsymbol{R}_{\text{доп.распред}}(\boldsymbol{T}_{\text{зад}})$ = 0,10.

Таким образом, оценка риска для дисциплины распространения знаний сразу после их приобретения или создания определяется по формуле

$$R_{\text{распред}} = 1 - \frac{\xi}{\xi + T\text{база знаний}} = 1\text{-}10/(10+0{,}25) = 0{,}024 \quad (4)$$

А оценка риска для дисциплины периодического распространения знаний вне зависимости от сроков их приобретения или создания, т. е. по регламенту (с подтверждением полезности существующих хранимых знаний при отсутствии изменений) определяется по формуле

$$R_{\text{распред}} = 1 - \frac{\xi^2}{q(\xi + T\text{база знаний})}\left[1 - \exp\left(-\frac{q}{\xi}\right)\right] =$$

$$= 1\text{-}\ 102\cdot[1\text{-}\exp(-0{,}083/10)]/0{,}083\cdot(10+0{,}25)=0{,}060 \quad (5)$$

Так как выполнено условие непревышения максимально допустимого уровня $R_{\text{распред}}(T_{\text{зад}}) \le R_{\text{доп.распред}}(T_{\text{зад}})$, то данным показателем при дальнейших расчетах можно пренебречь, т. е. $Z_{\text{полезн}}(T_{\text{зад}}) = 0$, условия по распространению знаний выполнены, см. формулу (6). Для периода $T_{\text{зад}}$, для которого определены исходные данные $\xi$, Тбаза знаний, $q$, показатель надежности распространения полезных знаний, предполагающий своевременность их последующего применения, определен следующим образом

$$Z_{\text{полезн}}(T_{\text{зад}}) = \begin{cases} 0, & \text{если условия по распространению и применению знаний выполнены;} \\ R_{\text{распред}}(T_{\text{зад}}) \text{ по формулам (4)и (5)}, & \text{если условия не выполнены или не заданы.} \end{cases} \quad (6)$$

**Пример 3**

В примере представлена оценка риска нарушения надежности реализации процесса управления знаниями, которая определяется по формуле

$$R_{надеж}(T_{зад}) = 1 - [1 - Z_{полезн}(T_{зад})] \cdot$$

$$\cdot\{\sum_{k=1}^{K(пр)} W(пр)_k[1 - Z(пр)_{действий\,k}(T_{зад\,k})] + \sum_{k=1}^{K(созд)} W(созд)_k[1 - Z(созд)_{действий\,k}(T_{зад\,k})] +$$

$$+\sum_{i=1}^{I(пр)} M(пр)_i[1 - Z(\text{пр})_{срок\,i}(T_{зад\,i})] + \sum_{i=1}^{I(созд)} M(созд)_i[1 - Z(созд)_{срок\,i}(T_{зад\,i})] + \quad (7)$$

$$+\sum_{j=1}^{J(пр)} L(пр)_j[1 - Z(пр)_{брака\,j}(T_{зад\,j})$$

$$+\sum_{j=1}^{J(созд)} L(созд)_j[1 - Z(\text{созд})_{брака\,j}(T_{зад\,j})]\}\ \ /\ [\sum_{k=1}^{K(пр)} W(пр)_k + \sum_{i=1}^{I(пр)} M(пр)_i$$

$$+\sum_{j=1}^{J(пр)} L(пр)_j + \sum_{k=1}^{K(созд)} W(созд)_k + \sum_{i=1}^{I(созд)} M(созд)_i + \sum_{j=1}^{J(созд)} L(созд)_j],$$

где $\boldsymbol{T}_{\text{зад}}$ – задаваемое суммарное время, включающее в себя все частные значения $\boldsymbol{T}_{\text{зад}\,k}$, $\boldsymbol{T}_{\text{зад}\,i}$, $\boldsymbol{T}_{\text{зад}\,j}$

$R_{\text{надеж}}(T_{\text{зад}}) =$ 1-[1·(1-0,03)+1·(1-0,03)+1·(1-0,03)+1·(1-0,03)+1·(1-0,03) +1·(1-0,03)]/(1+1+1+1+1+1) = 0,03.

В итоге риск нарушения надежности реализации процесса управления знаниями в прогнозируемом периоде 1 год составит приблизительно 0,03.

**Пример 4**

Пример демонстрирует прогнозирование риска нарушения требований по защите информации в нескольких автономных ЦЗн. Элементами моделируемой системы являются

элементы 1-5, формально ассоциируемые с активами и выходными результатами решения профильных задач соответственно 1-го – 5-го типов.

По определению отсутствие нарушений требований по защите информации в моделируемой системе считается обеспеченным в течение заданного периода прогноза, если в течение этого периода отсутствуют нарушения во всех автономных ЦЗн. Сам период прогноза для отдельного элемента может быть интерпретирован как относящийся к стадии создания (по угрозам, свойственным этой стадии), так и к стадии эксплуатации в будущем (по потенциально возможным угрозам).

Выполняя шаг 3 методики, выявлено множество критичных угроз, влияющих на безопасность каждого из структурных элементов моделируемой системы. Гипотетичные исходные данные по каждому из пяти элементов моделируемой системы с кратким обоснованием в комментариях представлены в Таблице 1.

Таблица1 ─ Гипотетичные исходные данные для прогнозирования риска нарушения требований по защите информации в процессе управления знаниями

| Исходные данные | Элементы | Значения и комментарии |
|---|---|---|
| | | |
| σ – частота возникновения источников угроз нарушения требований по защите информации | 1 | четыре раза в год, что соизмеримо с возникновением угроз, связанных с субъективными факторами и ошибками специалистов средней квалификации в области ИТ при решении задач обеспечения экологически безопасной морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях |
| | 2 | два раза в год, что соизмеримо со временем наработки на отказ программно-технического оборудования для обеспечения комплексной безопасности работ на континентальном шельфе, включая мониторинг и прогнозирование экстремальных ситуаций природного и техногенного характера |
| | 3 | один раз в год, что соизмеримо с возникновением угроз, связанных с причинами человеческих ошибок на уровнях принятия решений по предотвращению и ликвидации аварийных разливов нефти в ледовых условиях, включая создание технологий обнаружения нефти подо льдом |
| | 4 | один раз в два года, что соизмеримо с возникновением угроз от использования не декларируемых возможностей программного обеспечения в технологиях комплексного гидрометеорологического и экологического мониторинга опасных природных явлений в развиваемых регионах |

| Исходные данные | Элементы | Значения и комментарии |
|---|---|---|
| | 5 | один раз в два года, что соизмеримо с возникновением угроз от использования не декларируемых возможностей программного обеспечения в технологиях дистанционного исследования Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды |
| β – среднее время развития угроз с момента возникновения источников угроз до нарушения требований по защите информации | 1–5 | 1 сут<br>(предполагается, что из-за источника угроз активизируются не сразу, а с некоторой задержкой не менее суток)<br>– это время до возможного ущерба после возникновения признаков угроз |
| $T_{меж}$ – среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации | 1 | 1 ч<br>- определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при сменной работе в части морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях |
| | 2 | 1 ч<br>- определяется регламентом контроля целостности программного обеспечения и активов при мониторинге экстремальных ситуаций природного и техногенного характера |
| | 3 | 2 ч<br>- определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при сменной работе в части предотвращения и ликвидации аварийных разливов нефти в ледовых условиях |
| | 4 | 1 ч<br>- определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при комплексном гидрометеорологическом и экологическом мониторингах опасных природных явлений в арктических регионах |
| | 5 | 8 ч<br>- определяется регламентом контроля целостности программного обеспечения и активов ЦЗн при сменной работе в части дистанционного исследование Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды |
| $T_{диаг}$ – среднее время диагностики состояния | 1–5 | 30 с |

| Исходные данные | Элементы | Значения и комментарии |
|---|---|---|
| активов и самой системы | | что соизмеримо с длительностью автоматического контроля целостности программного обеспечения и активов ЦЗн |
| $T_{восст}$ – среднее время восстановления требуемой нормы эффективности защиты информации после выявления нарушений | 1–5 | 5 мин включая перезагрузку программного обеспечения и восстановление данных ЦЗн |
| $T_{зад}$– задаваемая длительность периода прогноза | 1–5 | от одного месяца до двух лет (для определения периода, при котором сохраняются гарантии непревышения допустимого риска нарушения требований по защите информации) |

Анализ результатов моделирования показал, что в вероятностном выражении риск нарушения требований по защите информации в течение года составит за весь комплекс центров знаний около 0,222 ─ см. Рис. 1, составляя для 1-го элемента – 0,080 («узкое место»), для 2-го – 4-го элементов не превышая 0,041, а для 5-го элемента – 0,072 («узкое место»). При изменении длительности периода прогноза от одного до четырех месяцев риск возрастает от 0,020 до 0,080. Для допустимого риска на уровне 0,050 обоснован период до 2,5 мес, при котором сохраняются гарантии непревышения допустимого риска для всего комплекса ЦЗн, характеризуемых условиями примера из Таблицы 1 – см. Рис. 2.

Уровни рисков для угроз выходным результатам ЦЗн1 (связанным с субъективными факторами и ошибками специалистов средней квалификации в области ИТ при решении задач обеспечения экологически безопасной морской разведки, добычи и транспортировки различных видов полезных ископаемых в экстремальных природно-климатических условиях - элемент 1) и угроз выходным результатам ЦЗн2 (связанным с использованием недекларируемых возможностей программного обеспечения в технологиях дистанционного исследования Земли, включая экологический мониторинг, оценку ресурсов и прогнозирование состояния окружающей среды - элемент 5) являются определяющими в общем риске нарушения требований по защите информации за год. Причем причиной того, что элемент 1 представляет собой своеобразное «узкое место» в комплексе ЦЗн, является сравнительно высокая частота возникновения источников угроз совершения человеческих ошибок (4 раза в год). А для элемента 5 причиной является сравнительно большое среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы в части выполнения требований по защите информации (через 8 ч) – см. Таблицу 1.

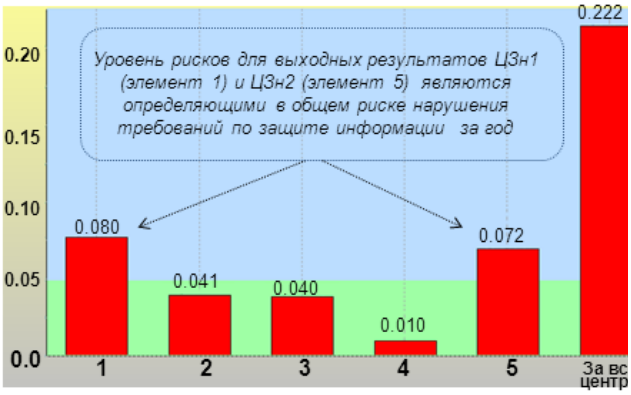



Рис. 1 - Оценки риска нарушения требований по защите информации в течение года

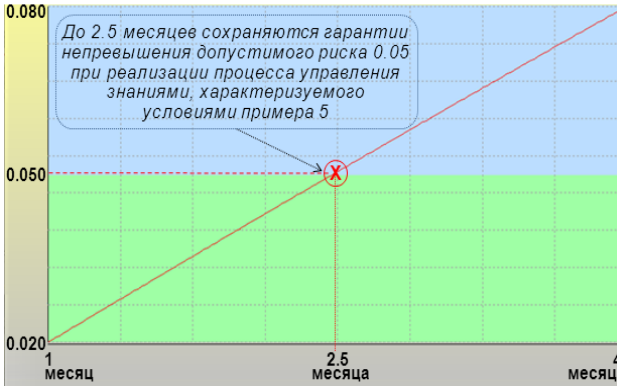



Рис. 2 - Зависимость риска за все центры знаний от периода прогноза длительностью от одного до четырех месяцев

**Пример 5**

Пример демонстрирует прогнозирование риска нарушения требований по защите информации с добавлением единого ЦЗн, интегрирующего возможности всех автономных ЦЗн и исполняющего функции резервного центра при различного рода отказах в профильных ЦЗн.

Рассмотрены два случая:

- случай 1: частота возникновение источников угроз возрастает до 1 раза в месяц, что ненамного превышает суммарную частоту возникновения различных источников угроз для ЦЗн1 – ЦЗн5 по Таблице 1;

- случай 2: частота возникновение источников угроз возрастает до 1 раза в сутки, что в 30 раз превышает частоту по сравнению со случаем 1 и сравнимо с умышленными компьютерными атаками на единый ЦЗн.

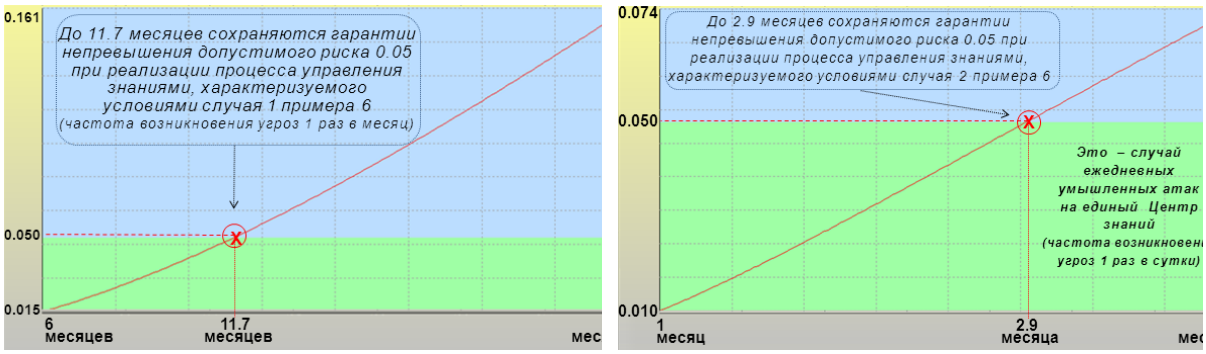
Для обоих случаев среднее время между окончанием предыдущей и началом очередной диагностики возможностей системы по выполнению требований по защите информации составляет 1 ч, что свойственно большинству профильных ЦЗн.

Анализ результатов моделирования для сложной структуры показал следующее.

Для случая 1 в вероятностном выражении суммарный риск нарушения требований по защите информации в течение года составит за весь комплекс центров знаний около 0,051, т. е. уменьшится по сравнению с примером 4 более чем в 4 раза. Это достигнуто за счет резервирования функционирования профильных центров знаний возможностями единого ЦЗн. При изменении длительности периода прогноза от 6 до 24 мес риск возрастает от 0,015 до 0,161. А для допустимого риска на уровне 0,050 обоснован период до 11,7 мес, при котором сохраняются гарантии непревышения допустимого риска для всего комплекса ЦЗн, характеризуемых условиями случая 1 примера 4 (см. Рис. 3а).

Для случая 2, ассоциируемого с ежедневными умышленными атаками на единый ЦЗн, суммарный риск нарушения требований по защите информации в течение года составит за весь комплекс центров знаний около 0,222, т. е. такой же, как для примера 5 с частотой возникновения источников угроз в 30 раз меньшей. При изменении длительности периода прогноза от 1 до 4 мес риск возрастает от 0,010 до 0,074. А для допустимого риска на уровне 0,050 обоснован период до 2,9 мес, при котором сохраняются гарантии непревышения допустимого риска для всего комплекса центров знаний, характеризуемых условиями

случая 2 примера 4
(см. Рис. 3б).




*а)* *б)*

Рис. 3 - Зависимость риска за все ЦЗн от периода прогноза:
а) от 6 до 24 мес (для случая 1) и б) от 1 до 4 мес (для случая 2)

**Пример 6**

Учитывая, что период прогноза $\boldsymbol{T}_{\text{зад}} = 1$ год, по результатам расчетов примеров 1─3 имеет место $\boldsymbol{R}_{\text{надеж}}(\boldsymbol{T}_{\text{зад}}) = 0{,}030$, а по результатам расчетов 5-го примера (случай 2 – умышленные атаки на единый ЦЗн) $\boldsymbol{R}_{\text{наруш}}(\boldsymbol{T}_{\text{зад}}) = 0{,}051$, то

$\boldsymbol{R}_{\text{обобщ}}(\boldsymbol{T}_{\text{зад}}) = 1 - (1-0{,}030)\cdot(1-0{,}051) \approx 0{,}080.$

В итоге обобщенный риск нарушения надежности

реализации процесса управления знаниями в течение года с учетом дополнительных специфических системных требований (требований к защите информации) составит 0,080. При этом риск нарушения требований по защите информации (0,051) в 1,57 раза меньше обобщенного риска нарушения надежности реализации процесса управления знаниями с учетом дополнительных специфических системных требований.

**5. Заключение**

Предложен методический подход, позволяющий формализовать процесс управления знаниями с учетом дополнительных специфических системных требований (требований по защите информации) и осуществлять оценку влияния различных угроз на результативность реализации процесса при взаимодействии центров обработки знаний. Даны рекомендации по методам прогнозирования рисков с учетом сложности моделируемой системы и мер противодействия угрозам в каждом элементе. На примерах проиллюстрированы методы методического обоснования системных решений по снижению рисков и их удержанию в допустимых пределах. Данный методический подход нашел свое отражение в ГОСТ Р 59333-2021.

Список литературы

1. А. Костогрызов. Прогнозирование рисков для систем искусственного Интеллекта с использованием данных мониторинга. 2019. Том-2603. С. 29-33. URL: http://ceur-ws.org/Vol-2603/short7.pdf

2. В. Кершенбаум, Л. Григорьев, П. Каныгин, А. Нистратов. Вероятностное

моделирование в системной инженерии. Вероятностное моделирование процессов для нефтегазовых систем. IntechOpen, 2018: 55-79.

3. Авдонин Р.Ю., Костогрызов А.И., Нистратов А.А. Методы анализа рисков для процесса управления знаниями о системе. Сборник трудов XI международной научно-технической конференции "Безопасные информационные технологии", 6-7 апреля 2021 г. в Москве в МГТУ им. Н.Э.Баумана. – М.: МГТУ им. Н.Э.Баумана, 2021. сс. 12-19, ISBN 978-5-9906630-7-7

4. А. Бердюгин, П. Ревенков. Подходы к измерению риска кибератак в дистанционных банковских сервисах России. 2019. Том-2603. С. 23-38. URL: http://ceur-ws.org/Vol-2603/short2.pdf

5. Andrey Kostogryzov, Roman Avdonin, Andrey Nistratov Methodical rationale of system solutions to reduce risks and retain them within acceptable limits for knowledge management process, https://doi.org/10.24412/1932-2321-2022-471-50-64

6. Н. Корнеев, В. Меркулов. Интеллектуальный анализ и базовое моделирование сложных угроз. 2019. Том-2603. С. 23-38. URL: http://ceur-ws.org/Vol-2603/paper6.pdf

7. В. Варенница, А. Марков, В. Савченко. Рекомендуемые методы анализа уязвимостей веб-приложений. 2019. Том-2603. С. 75-78. URL: http://ceur-ws.org/Vol-2603/short16.pdf

8. А. Костогрызов, В. Королев. Вероятностные методы когнитивного решения некоторых задач систем искусственного интеллекта. Вероятность, комбинаторика и управление. IntechOpen, 2020, стр. 3-34. URL: https://www.intechopen.com/books/probability-combinatorics-and-control

9. В. Борковская и Д. Пассмор Стратегия снижения рисков и управление рисками на основе оценок качества, Конференция IOP 2020. Сер.:Матер. наук. англ. 869 062051

10. А. Костогрызов, А. Нистратов, Г. Нистратов (2020) Аналитическое прогнозирование рисков. Обоснование Системных превентивных мер для решения проблем качества и безопасности. В: Сухомлин В., Зубарева Е. (ред.) Современные информационные технологии и ИТ-образование. СИТИТО 2018. Коммуникации в информатике и информатике, том 1201. Спрингер, стр.352-364. https://www.springer.com/gp/book/9783030468941

References

1 A. Kostogryzov. Risks Prediction for Artificial Intelligence Systems Using Monitoring Data. 2019. Vol-2603. P. 29-33. URL: http://ceur-ws.org/Vol-2603/short7.pdf

2. V. Kershenbaum, L. Grigoriev, P. Kanygin, A. Nistratov. Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018: 55-79

3. R. Avdonin, A. Kostogryzov, A. Nistratov. Methods of analysis for knowledge management about system. Proceedings and Technical Conference «Secure Information Technologies», April 6-7, 2021 in Moscow at the Bauman Moscow State Technical University. – M.: Bauman Moscow State Technical University, 2021. P. 12-19, ISBN 978-5-9906630-7-7

4 A. Berdyugin, P. Revenkov. Approaches to measuring the risk of cyberattacks in remote banking services of Russia. 2019. Vol-2603. P. 23-38. URL: http://ceur-ws.org/Vol-2603/short2.pdf

5. Andrey Kostogryzov, Roman Avdonin, Andrey Nistratov Methodical rationale of system solutions to reduce risks and retain them within acceptable limits for knowledge management

process, https://doi.org/10.24412/1932-2321-2022-471-50-64

6. N. Korneev, V. Merkulov. Intellectual analysis and basic modeling of complex threats. 2019. Vol-2603. P. 23-38. URL: http://ceur-ws.org/Vol-2603/paper6.pdf

7. V. Varenitca, A. Markov, V. Savchenko. Recommended Practices for the Analysis of Web Application Vulnerabilities. 2019. Vol-2603. P. 75-78. URL: http://ceur-ws.org/Vol-2603/short16.pdf

8. A. Kostogryzov, V. Korolev. Probabilistic methods for cognitive solving some problems of artificial intelligence systems. Probability, combinatorics and control. IntechOpen, 2020, pp. 3-34. URL: https://www.intechopen.com/books/probability-combinatorics-and-control

9. V. Borcovskaya and D. Passmore Risk Reduction Strategy and Risk Management on The Basis of Quality Assessments., 2020 IOP Conf. Ser.:Mater. Sci. Eng. 869 062051

10. A. Kostogryzov, A. Nistratov, G. Nistratov (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, pp.352-364. https://www.springer.com/gp/book/9783030468941