DOI: 10.6060/ivecofin.2024613.694
УДК: 004.02

ВЫБОР ВЕСОВЫХ КОЭФФИЦИЕНТОВ ДЛЯ МОДЕЛИ ОЦЕНКИ УРОВНЯ БЛАГОНАДЕЖНОСТИ СОТРУДНИКОВ В СИСТЕМЕ КАДРОВОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (КИИ)

С.В. Глухарева, М.М. Немирович-Данченко, А.А. Шелупанов

Светлана Владимировна Глухарева* (ORCID 0000-0002-7155-329X), Михаил Михайлович Немирович-Данченко (ORCID 0000-0002-4510-8045), Александр Александрович Шелупанов (ORCID 0000-0003-2393-6701)
Томский государственный университет систем управления и радиоэлектроники, пр. Ленина, 40, Томск, 634050, Россия
E-mail: samantases@mail.ru*, michnd@mail.ru, saa@tusur.ru

В статье проведен анализ существующих методов выбора весовых коэффициентов для модели оценки уровня благонадежности сотрудников в системе кадровой безопасности на предприятиях критической информационной инфраструктуры. В настоящее время в качестве основных характеристик для оценки персонала используют образование, стаж и компетенции, поэтому эти характеристики были выбраны для модели оценки уровня благонадежности сотрудников в системе кадровой безопасности на предприятиях критической информационной инфраструктуры (КИИ). Следующим шагом стало определение весовых коэффициентов для выбранной модели оценки сотрудников. Приведено три метода выбора весовых коэффициентов для модели оценки уровня благонадежности в системе кадровой безопасности на предприятиях КИИ. Прежде всего, это экспертный метод, в основе применения которого лежит использование опыта высококвалифицированных специалистов. При использовании этого метода обоснованность суждений экспертов подтверждается анализом независимости их суждений и предпочтений, а также оценкой уровня согласованности экспертов с помощью коэффициента конкордации. Второй метод - это сочетание эксперимента с применением аддитивного критерия оптимальности. Построенная система вариантов частных критериев сравнивается с существующей на предприятиях КИИ методикой оценки персонала, что позволяет выбрать наиболее приемлемый вариант. И, наконец, третий метод – метод анализа иерархий (Т. Саати). Для метода Т. Саати проведены сравнения критериев оценки уровня благонадежности и вычислены итоговые компоненты вектора предпочтений. В статье более подробно рассмотрен подход метода анализа иерархий. Обсуждаются проблемы экспертного сравнения количественных и качественных величин. Все три метода показали равнозначные весовые коэффициенты модели, что доказывает эффективность применения данной модели для оценки уровня благонадежности сотрудников в системе кадровой безопасности на предприятиях КИИ.

Ключевые слова: уровень благонадежности, модель оценки уровня благонадежности, кадровая безопасность, критическая информационная инфраструктура, экспертная оценка, метод анализа иерархий, аддитивный коэффициент.

SELECTION OF WEIGHTING COEFFICIENTS FOR A MODEL FOR ASSESSING THE LEVEL OF EMPLOYEE RELIABILITY IN THE PERSONNEL SECURITY SYSTEM AT ENTERPRISES OF CRITICAL INFORMATION INFRASTRUCTURE (CII)

S.V. Glukhareva, M.M. Nemirovich-Danchenko, A.A. Shelupanov

Svetlana V. Glukhareva* (ORCID 0000-0002-7155-329X), Mikhail M. Nemirovich-Danchenko (ORCID 0000-0002-4510-8045), Alexander A. Shelupanov (ORCID 0000-0003-2393-6701)
Tomsk State University of Control Systems and Radioelectronics, Lenin Ave., 40, Tomsk, 634050, Russia
E-mail: samantases@mail.ru*, michnd@mail.ru, saa@tusur.ru

The article analyzes the existing methods of selecting weighting coefficients for a model for assessing the level of employee reliability in the personnel security system at enterprises of critical information infrastructure. Currently, education, experience and competencies are used as the main characteristics for personnel assessment, therefore these characteristics were chosen for a model for assessing the level of employee reliability in the personnel security system at enterprises of critical information infrastructure (hereinafter referred to as CII). The next step was to determine the weighting coefficients for the selected employee evaluation model. Three methods of selecting weighting coefficients for the model of assessing the level of reliability in the personnel security system at CII enterprises are given. The first one is an expert method based on the use of experience of highly qualified specialists. When using this method, the validity of experts' judgments is confirmed by analyzing the independence of their judgments and preferences, as well as evaluating the level of consistency of experts using the concordance coefficient. The second method is a combination of an experiment using an additive optimal criterion. The constructed system of variants of private criteria is compared to the existing methodology of personnel assessment at CII enterprises, which makes it possible to choose the most acceptable option. And finally, the third method is the method of analytic hierarchy process (T. Saati). For T. Saati's method, comparisons of criteria for assessing the level of reliability were carried out and the final components of the preference vector were calculated. The article discusses the approach of analytic hierarchy process in more detail. The problems of expert comparison of quantitative and qualitative values are discussed. All three methods show equivalent weighting coefficients of the model, which proves the effectiveness of using this model to assess the level of employee reliability in the personnel security system at CII enterprises.

Keywords: reliability level, reliability assessment model, personnel security, critical information infrastructure, expert assessment, analytic hierarchy process, additive coefficient.

Для цитирования:
Глухарева С.В., Немирович-Данченко М.М., Шелупанов А.А. Выбор весовых коэффициентов для модели оценки уровня благонадежности сотрудников в системе кадровой безопасности на предприятиях критической информационной инфраструктуры (КИИ). *Известия высших учебных заведений. Серия «Экономика, финансы и управление производством» [Ивэкофин]*. 2024. № 03(61). С.97-103. DOI: 10.6060/ivecofin.2024613.694

For citation:
Glukhareva S.V., Nemirovich-Danchenko M.M., Shelupanov A.A. Selection of weighting coefficients for a model for assessing the level of employee reliability in the personnel security system at enterprises of critical information infrastructure (CII). *Ivecofin.* 2024. N 03(61). C.97-103. DOI: 10.6060/ivecofin.2024613.694 (in Russian)

ВВЕДЕНИЕ

В современных условиях важную ценность представляют нематериальные активы в виде информации. Разглашение информации неблагонадежными сотрудниками может нанести организации значительный ущерб. Увеличивается и количество кибератак на объекты КИИ. От своевременного реагирования и внимательности сотрудников зависит также социальная безопасность. Этим обусловлено повышение внимания исследователей к вопросам безопасности на предприятиях КИИ, в том числе и к вопросам кадровой безопасности [1, 2, 3].

Сегодня около четверти всех экономических преступлений совершается сотрудниками компаний [4]. По данным Генпрокуратуры и МВД России, злоумышленники все чаще присваивают и растрачивают чужое имущество и занимаются мошенничеством. За последние 5 лет финансовый ущерб от киберпреступлений составил порядка 500 млрд рублей, при этом только в 2023 г. сумма достигла 156 млрд рублей [5]. 50% российских компаний столкнулись с корпоративным мошенничеством в 2023 г. [6]. В 71% организаций сотрудники пытались украсть корпоративную информацию [7]. 28 декабря 2010 г. был принят Федеральный закон № 390-ФЗ «О безопасности», который определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации [8]. 26 июля 2017 г. вышел Федеральный закон № 187-ФЗ «О безопасности критиче-

ской информационной инфраструктуры Российской Федерации», который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак [9]. Только в 2023 г. на объектах КИИ было отражено порядка 65 000 кибератак [10]. Реализация угроз может привести к прекращению или нарушению функционирования значимого объекта и обеспечивающего (управляемого, контролируемого) им процесса, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации) [2]. Кроме того, на российском рынке труда в информационной безопасности в 2022–2024 гг. сформировался острый дефицит специалистов, в том числе под давлением вопросов технологического суверенитета и национальной безопасности [11]. Все вышесказанное требует доработки, а, возможно, и пересмотра системы оценивания сотрудников, работающих на предприятиях КИИ. Количественная оценка уровня благонадежности сотрудников предприятий КИИ – это необходимый шаг для защиты критически важных данных и систем от угроз безопасности. Правильное проведение оценки позволяет выявить потенциальные риски и принять меры для их минимизации.

МАТЕРИАЛЫ И МЕТОДЫ

Обеспечение безопасности сотрудниками КИИ - это ключевой аспект защиты критически важной инфраструктуры от угроз кибербезопасности. Сотрудники являются одним из самых важных элементов системы безопасности [12], поскольку они имеют доступ к конфиденциальным данным, критическим системам и инфраструктуре. Функции обеспечения безопасности объектов КИИ возложены на сами предприятия. В рамках кадровой безопасности предприятий КИИ основой являются благонадежные кадры, обладающие требуемыми компетенциями. Авторами среди требуемых компетенций были рассмотрены способность к обеспечению устойчивого функционирования значимых объектов КИИ, навыки принятия решений в условиях неопределенности и в то же время умение выполнять инструкции. Выявлялся также высокий уровень внимательности и стрессоустойчивости, а также эмоциональная и социальная гибкость и т.п. Сотрудники предприятий КИИ обеспечивают безопасность, стабильность и бесперебойность работы как самого предприятия КИИ, так в целом и безопасность государства.

Благонадежность сотрудника проявляется только в его деятельности. В системе кадровой безопасности предприятия благонадежность рассматривается как совокупная характеристика образования О, стажа Ст и уровня владения компетенциями К [13]. В системе кадровой безопасности определяются 9 типов компетенций: личные (A), профессиональные (B), корпоративные (C), компетенции безопасности (D), специальные (E), компетенции будущего (F), поведенческие (G), социально-психологические (H), успешности (I) [14]. Каждая из этих компетенций представляет собой сумму компетенций. Образование играет важную роль в жизни каждого человека. Знания сегодня быстро устаревают, поэтому необходимо постоянное их обновление. Стаж является количественным показателем, а опыт качественным показателем в деятельности сотрудника. Стаж характеризуют: место работы, профессиональный рост, продолжительность работы. Опыт включает в себя достижения в должности, профессиональный рост сотрудника. В настоящее время основными требованиями при приеме на работу являются наличие базового образования, опыт работы по специальности, набор компетенций, а также другие формальные требования). Данные требования определяются профессиональными стандартами и нормативными требованиями предприятия. О.Е. Подвербных вводит коэффициент профессиональной перспективности, куда входят данные об образовании кандидата, его стаже и возрасте [15], что делает возможность использования данных об образовании и стаже в разрабатываемой модели:

$$УБ = Z_1 О + Z_2 Ст + Z_3 К \quad (1)$$

где О – образование;

Ст – стаж;

К – компетенции;

Z_1 – весовой коэффициент для образования;

Z_2 - весовой коэффициент для стажа;

Z_3 - весовой коэффициент для компетенций.

В отношении этих коэффициентов должно выполняться равенство:

$$Z_1 + Z_2 + Z_3 = 1 \quad (2)$$

Выбор весовых коэффициентов для модели оценки уровня благонадежности сотрудников - это важный этап, который напрямую влияет на точность и объективность результатов. Существует несколько подходов к определению весовых коэффициентов: экспертная оценка, статистический анализ, гибридный подход.

РЕЗУЛЬТАТЫ

Выбор весовых коэффициентов определялся тремя методами: экспертным, выбором аддитивного критерия оптимальности и методом анализа иерархий (метод Т. Саати). Выбор весовых коэффициентов экспертным методом ранее был описан в [13].

Экспертный метод - один из способов определения весовых коэффициентов, основанный на мнении специалистов в области безопасности, кадрового менеджмента, психологии [16]. Оценивание, проводимое экспертами, предполагает сравнение интенсивности изучаемых факторов (стажа, образования и владения компетенциями) у альтернатив. Поэтому применительно к обсуждаемым задачам экспертная оценка проводилась высококвалифицированными специалистами, имеющими опыт в оценке персонала: начальником HR-отдела предприятия КИИ, психологом, специалистом по оценке персонала, доктором экономических наук, профессором и экспертом-аналитиком, которые смогли оценить относительную важность каждого фактора, влияющего на уровень благонадежности и имеющие знания о специфике деятельности предприятий КИИ. При проведении экспертной оценки были соблюдены все правила для независимости суждений и предпочтений. После выставления оценок экспертами была проведена проверка их мнений на согласованность с помощью коэффициента конкордации Кендалла [17], который получился равным 0,83, что говорит о наличии высокой степени согласованности мнений экспертов. Таким образом, весовые коэффициенты составили:

- для образования $Z_1 = 0,2$;
- для стажа $Z_2 = 0,3$;
- для компетенций $Z_3 = 0,5$.

Далее был проведен эксперимент и применен аддитивный коэффициент оптимальности для выбора весовых коэффициентов для разработанной модели [18]. Аддитивный коэффициент оптимальности (АКО) – это один из методов, позволяющий определить весовые коэффициенты, учитывая относительную важность каждого критерия. Критерии уже были определены экспертным путем: образование, стаж и компетенции. Также учитывалась специфика предприятия (предприятия КИИ) и уровень чувствительности к безопасности. Оценивалась важность каждого критерия по шкале от 0 до 1, где 0 означает минимальную важность, а 1 – максимальную: 0; 0,1; 0,2; … 0,9; 1 (с шагом 0,1). Некоторые значения частных критериев приведены в табл. 1.

На предприятиях КИИ в текущей работе уже используются системы оценивания работников [19]. Наборы показателей, приведенные в табл. 1, сравнивались с оценками, полученными с предприятий КИИ. Наиболее близкий к оценкам предприятий КИИ набор весовых коэффициентов оказался вариант №6: для образования 0,2; для стажа 0,3; для компетенций 0,5.

Таблица 1. Значения частных критериев оценки благонадежности
Table 1. Values of particular criteria for assessing reliability

Варианты (стратегии)	Критерий благонадежности №1	Критерий благонадежности №2	Критерий благонадежности №3
№1	0,6	0,2	0,2
№2	0,1	0,2	0,7
№3	0,3	0,3	0,4
№4	0,4	0,2	0,4
№5	0,5	0,1	0,4
№6	0,2	0,3	0,5
№7	0,7	0,1	0,2
№8	0,8	0,1	0,1
№9	0,2	0,4	0,4
№10	0,3	0,2	0,5

Проблема независимости выбора критериев также была решена. Образование, стаж и компетенции – компоненты модели, оценки которых находятся в одном диапазоне от 0 до 1. Полученными весовыми коэффициентами 0,2; 0,3; 0,5 эти оценки взвешиваются и тогда проблема размерности и разнородности этих сущностей (образования, стажа и компетенций) исчезает. Два критерия - образование и стаж - независимы по предпочтению от критерия компетенций, если предпочтения между альтернативами, различающимися лишь оценками по ним, не зависят от фиксированных значений по другим критериям.

В количественном выражении может быть измерен только стаж (единица измерения - время). Компетенции и образование – не являются количественными единицами измерения, следовательно, стаж тоже сводим к рангам (баллам) и тогда, образование, стаж и компетенции - однородные, однотипные величины, каждая из них измеряется по одной и той же линейке. Данные показатели по-разному влияют на нашу целевую переменную, это уже особенность предлагаемой модели оценки уровня благонадежности сотрудников на предприятиях КИИ.

Следующий метод для выбора весовых коэффициентов – метод анализа иерархий, который используется для попарного сравнения факторов по степени важности и получения весовых коэффициентов. Метод Т. Саати позволяет структурировать сложные задачи и учитывать множество взаимосвязанных факторов при оценке уровня благонадежности сотрудников [20]. Он помогает определить относительную важность каждого критерия оценки с помощью попарных сравнений и получить весовые коэффициенты для каждого критерия. Вначале были выбраны альтернативы. Это критерии метода оценки благонадёжно-

сти: – компетенции (К), стаж (Ст), образование (О) (КСО). В качестве критериев были определены следующие: простота поиска информации для значений критерия (П), интуитивная (из общения с экспертами) корреляция между критерием К, Ст или О и благонадежностью (И), и обоснованность критериев КСО документами (наличие подтверждающих документов) (Д). Вначале сравним между собой КСО по трем критериям (табл. 2, 3, 4). На следующем шаге сравним критерии (П), (И) и (Д) (ПИД) между собой (табл. 5) для получения вектора приоритетов критериев ***Vk***.

Таблица 2. Сравнение альтернатив КСО по критерию П
Table 2. Comparison of CEE alternatives by criterion S

П	К	Ст	О		Корень из произведения	Веса нормированные по критерию (П)
К	1	0,2	0,111111		0,281144	**0,062941**
Ст	5	1	0,333333		1,185631	**0,265433**
О	9	3	1		3	**0,671625**
				Суммы	4,466775	**1**

Таблица 3. Сравнение альтернатив КСО по критерию И
Table 3. Comparison of CEE alternatives by criterion I

И	К	Ст	О		Корень из произведения	Веса нормированные по критерию (И)
К	1	3	9		3	**0,692308**
Ст	0,333333	1	3		1	**0,230769**
О	0,111111	0,333333	1		0,333333	**0,076923**
				Суммы	**4,333333**	**1**

Таблица 4. Сравнение альтернатив КСО по критерию Д
Table 4. Comparison of CEE alternatives according to criterion D

Д	К	Ст	О		Корень	Веса нормированные по (Д)
К	1	0,166667	0,2		0,32183	**0,075132**
Ст	6	1	4		2,884499	**0,67339**
О	5	0,25	1		1,077217	**0,251478**
				Суммы	4,283546	**1**

Таблица 5. Сравнение критериев ПИД между собой
Table 5. Comparison of SID criteria among themselves

	П	И	Д			Вектор приоритетов для ПИД ***Vk***
П	1	0,25	1		0,629961	**0,166667**
И	4	1	4		2,519842	**0,666667**
Д	1	0,25	1		0,629961	**0,166667**
					3,779763	**1**

Составим итоговые столбцы весов приоритетов из первых трех таблиц в одну матрицу $\boldsymbol{M_{КСО}}$:

$$\boldsymbol{M_{КСО}} = \begin{matrix} 0{,}062941 & 0{,}692308 & 0{,}075132 \\ 0{,}265433 & 0{,}230769 & 0{,}67339 \\ 0{,}671625 & 0{,}076923 & 0{,}251478 \end{matrix}$$

Затем умножим эту матрицу на столбец весов ПИД (используется умножение матрицы справа на вектор):

$$\boldsymbol{M}_{\text{КСО}} \times \vec{\boldsymbol{V}}\boldsymbol{k} = \begin{matrix} 0{,}484551 \\ 0{,}310317 \\ 0{,}205133 \end{matrix}$$

Итак, получаем следующие значения:

К = 0,4845

Ст = 0,3103

О = 0,205

Таким образом, методом анализа иерархий также получились весовые коэффициенты для компетенций, стажа и образования, близкие к весовым коэффициентам, полученным другими способами.

ЗАКЛЮЧЕНИЕ

Оценка уровня благонадежности сотрудников предприятий КИИ - это комплексный процесс, направленный на выявление потенциальных рисков, связанных с доступом к критически важным данным и системам. Она необходима для минимизации угроз безопасности, связанных с несанкционированным доступом, несанкционированной деятельностью, диверсией и шпионажем. Выбор весовых коэффициентов в модели оценки уровня благонадежности сотрудников - задача, требующая комплексного подхода, учитывающего специфику работы предприятия и его чувствительность к угрозам безопасности. Экспертный метод позволяет определить весовые коэффициенты для модели оценки уровня благонадежности сотрудников, учитывая специфику работы предприятия и опыт специалистов. Сначала определялись весовые коэффициенты экспертным методом, а затем с помощью аддитивного коэффициента оптимальности и методом анализа иерархий. Весовые коэффициенты были рассчитаны тремя методами и составили для образования – 0,2; для стажа – 0,3 и для компетенций – 0,5. Модель и весовые коэффициенты соответствуют требованиям работодателя, предъявляемым к конкретной должности. Соответствие занимаемой должности, формальные требования и экспериментальные данные, а также сравнение с данными по оценке сотрудников, применяемыми на предприятии КИИ, показали, что предлагаемая модель оценки уровня благонадежности может быть применена для оценки сотрудников предприятий КИИ.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflict of interest.

ЛИТЕРАТУРА

1. Указ Президента Российской Федерации № 31с от 15.01.2013 «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». http://www.kremlin.ru/acts/bank/36691.
2. Приказ ФСТЭК № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». https://base.garant.ru/71901880/?ysclid= lrtgazwzng826976123.
3. Приказ Федеральной службы по техническому и экспортному контролю № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». https://base.garant.ru/71886248/?ysclid=lrtgir09xq706406046.
4. **Дуболазова Ю.А., Акласова А.А., Кранина А.Д.** Корпоративные преступления и их типология. *Экономические науки: научно-информационный журнал.* 2021. № 5 (198). С. 48-56.
5. Ущерб от киберпреступлений в России за пять лет оценили в 500 млрд рублей. https://www.interfax.ru/russia/962511/.
6. **Ющенко И.Н.** Корпоративное мошенничество в деятельности российских компаний. https://apni.ru/article/9248-korporativnoe-moshennichestvo-v-deyatelnosti-rossijskih-kompanij.
7. Половина компаний РФ сталкиваются с корпоративным мошенничеством. https://itspeaker.ru/news/polovina-kompaniy-rf-stalkivayutsya-s-korporativnym-moshennichestvom/.
8. Закон Российской Федерации № 390-ФЗ от 28.12.2010 «О безопасности». https://www.consultant.ru/document/cons_doc_LAW_108546/?ysclid=lyu0qb0n1j297158776.
9. Федеральный закон № 187 - ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации». http://www.consultant.ru/document/cons_doc_LAW_220885/.

REFERENCES

1. Decree of the President of the Russian Federation N 31c of 01/15/2013 "On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation". http://www.kremlin.ru/acts/bank/36691. (in Russian).
2. FSTEC Order N 239 of 12/25/2017 "On approval of Requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation". https://base.garant.ru/71901880/?ysclid=lrtgazwzng826976123. (in Russian).
3. Order of the Federal Service for Technical and Export Control N 235 of 12/21/2017 "On approval of Requirements for the creation of security systems for significant objects of critical information infrastructure of the Russian Federation and ensuring their functioning". https://base.garant.ru/71886248/?ysclid=lrtgir09xq706406046. (in Russian).
4. **Dubolazova Yu.A., Aklasova A.A., Kranina A.D.** Corporate crimes and their typology. *Economic Sciences : a scientific and informational journal*. 2021. N 5 (198). P. 48-56. (in Russian).
5. Damage from cybercrimes in Russia over five years was estimated at 500 billion rubles. https://www.interfax.ru/ russia/962511/. (in Russian).
6. **Yushchenko I.N.** Corporate fraud in the activities of Russian companies. https://apni.ru/article/9248-korporativnoe-moshennichestvo-v-deyatelnosti-rossijskih-kompanij. (in Russian).
7. Half of Russian companies encounter corporate fraud. https://itspeaker.ru/news/polovina-kompaniy-rf-stalkivayutsya-s-korporativnym-moshennichestvom/. (in Russian).
8. The Law of the Russian Federation N 390-FZ of 12/28/2010 "On security". https://www.consultant.ru/document/cons_doc_LAW_108546 /?ysclid=lyu0qb0n1j297158776 (in Russian).
9. Federal Law N 187 - FZ of 07/26/2017 "On the Security of the Critical Information Infrastructure of the Russian Federation". http://www.consultant.ru/document/cons_doc_LAW_220885 /. (in Russian).

10. Чернышенко: Россия отразила больше 65 тысяч кибератак на объекты инфраструктуры. https://cont.ws/@volniiveter/2730082.
11. Рынок труда в информационной безопасности в России в 2024–2027 гг.: прогнозы, проблемы и перспективы. https://www.ptsecurity.com/ru-ru/research/analytics/rynok-truda-v-informacz ionnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/.
12. **Семенихин И.** Подготовка кадров для объектов КИИ: опыт и перспективы. https://securitymedia.org/info/podgotovka-kadrov-dlya-obektov-kii-opyt-i-perspektivy.html.
13. **Шелупанов А.А., Глухарева С.В., Немирович-Данченко М.М.** Формализованный подход к оценке уровня благонадежности сотрудников предприятий критической информационной инфраструктуры (КИИ). *Перспективы науки.* 2023. № 4 (163). С. 16-24.
14. **Глухарева С.В.** Метод оценки уровня благонадежности сотрудников в системе кадровой безопасности предприятия (на примере предприятий критической информационной инфраструктуры (КИИ). *Доклады Томского государственного университета систем управления и радиоэлектроники.* 2022. Т. 25. № 2. С. 59-67. DOI: 10.21293/1818-0442-2022-25-2-59-67.
15. **Подвербных О.Е., Соколова Е.Л., Самохвалова С.М.** Инструменты оценки эффективности развития человеческих ресурсов промышленных предприятий. *Экономика труда.* 2020. Том 7. № 12. С. 1165-1180. DOI: 10.18334/et.7.12.111265.
16. **Анохин А.Н.** Методы экспертных оценок: учебное пособие. Обнинск: ИАТЭ. 1996. 148 с.
17. **Трусова А.Ю.** Анализ данных. Многомерные статистические методы: учебное пособие. Самара: СамГУ. 2023. 92 с.
18. **Бельков В.Н., Ланшаков В.Л.** Автоматизированное проектирование технических систем: учебное пособие. https://www.monographies.ru/ru/book/view?id=57.
19. **Шелупанов А.А., Глухарева С.В., Немирович-Данченко М.М.** Оценка благонадежности сотрудника в системе кадровой безопасности предприятия. *Доклады Томского государственного университета систем управления и радиоэлектроники.* 2021. Т. 24. № 4. С. 52-57. DOI: 10.21293/1818-0442-2021-24-4-52-57.
20. **Саати Т.Л.** Принятие решений. Метод анализа иерархий. М.: Радио и связь. 1993. 314 с.

10. Chernyshenko: Russia has repelled more than 65 thousand cyber-attacks on infrastructure facilities. https://cont.ws/@volniiveter/2730082. (in Russian).
11. The information security labor market in Russia in 2024-2027: forecasts, problems and prospects. https://www.ptsecurity.com/ru-ru/research/analytics/rynok-truda-v-informacz i-onnoj-bezopasnosti-v-rossii-v-2024-2027-gg-prognozy-problemy-i-perspektivy/. (in Russian).
12. **Semenikhin I.** Personnel training for CII facilities: experience and prospects. https://securitymedia.org/info/podgotovka-kadrov-dlya-obektov-kii-opyt-i-perspektivy.html. (in Russian).
13. **Shelupanov A.A., Glukhareva S.V., Nemirovich-Danchenko M.M.** A formalized approach to assessing the level of employee reliability in critical information infrastructure (CII) enterprises. *Prospects of science*. 2023. N 4 (163). P. 16-24. (in Russian).
14. **Glukhareva S.V.** Method of assessing the level of employee reliability in the personnel security system of an enterprise (on the example of enterprises of critical information infrastructure). *Reports of the Tomsk State University of Control Systems and Radioelectronics*. 2022. Vol. 25. N 2. P. 59-67. DOI: 10.21293/1818-0442-2022-25-2-59-67. (in Russian).
15. **Podverbnyh O.E., Sokolova E.L., Samokhvalova S.M.** Tools for evaluating the effectiveness of human resource development in industrial enterprises. *Russian Journal of Labor Economics.* 2020. Vol. 7. N 12. P. 1165-1180. DOI: 10.18334/ et.7.12.111265. (in Russian).
16. **Anokhin A.N.** Methods of expert assessment: a textbook. Obninsk: INPE. 1996. 148 p. (in Russian).
17. **Trusova A.Y.** Data analysis. Multidimensional statistical methods: a textbook. Samara: Samara University Press. 2023. 92 p. (in Russian).
18. **Belkov V.N., Lanshakov V.L.** Computer-aided design of technical systems: a textbook. https://www.monographies.ru/ru/book/view?id=57. (in Russian).
19. **Shelupanov A.A., Glukhareva S.V., Nemirovich-Danchenko M.M.** Assessment of employee reliability in the personnel security system of the enterprise. *Reports of the Tomsk State University of Control Systems and Radioelectronics*. 2021. Vol. 24. N 4. P. 52-57. DOI: 10.21293/1818-0442-2021-24-4-52-57. (in Russian).
20. **Saati T.L.** Decision-making. The Analytic Hierarchy Process. Moscow: Radio and communications.1993. 314 p.

Поступила в редакцию 20.07.2024
Принята к опубликованию 03.08.2024

Received 20.07.2024
Accepted 03.08.2024