УДК 004.023

С.В. Глухарева

Метод оценки уровня благонадежности сотрудников в системе кадровой безопасности предприятия (на примере предприятий критической информационной инфраструктуры (КИИ))

Рассматривается метод оценки уровня благонадежности, основанный на составлении профиля компетенций. Данный метод дает качественную оценку компетенций сотрудников и был применен к сотрудникам, занятым на предприятиях критической информационной инфраструктуры. Данные предприятия играют большую роль в рамках обеспечения национальной безопасности, поэтому большое внимание отводится оценке персонала. Предложенный метод оценки компетенций основан на составлении профиля компетенций, учитывающий особенности конкретной должности, изменения требований к должности, включающий оценку когнитивных способностей и профессиональных компетенций. В основе метода лежит модель, позволяющая учитывать не только уровень владения компетенциями, но и образование и стаж. Приводятся данные апробации, показана согласованность экспертной оценки. Данный метод показал свою эффективность и внедрен на предприятия КИИ.
Ключевые слова: профиль компетенций, кадровая безопасность, уровень благонадежности, предприятия КИИ.
DOI: 10.21293/1818-0442-2022-25-2-59-67

Целью программы «Цифровая экономика» [1] является «создание экосистемы цифровой экономики, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан». Развитие цифровой экономики в РФ осуществляется в соответствии с Указом Президента РФ от 09.05.2017 г. № 203 [2].

В условиях цифровой трансформации и перехода к цифровой экономике все большую популярность набирают цифровые решения в виде автоматизированных информационных программ или платформ, которые представляют собой интеллектуальную систему принятия решений.

Развитие цифровой среды предполагает разработку цифровых платформ, автоматизированных информационных систем, информационных телекоммуникационных систем, информационных технологий и т.п. Уязвимость данных платформ и систем, хакерские атаки приводят к усилению мер по обеспечению безопасности объектов.

Особую уязвимость в РФ имеют предприятия критической информационной инфраструктуры (КИИ). Функционирование предприятий КИИ является важным как для экономики государства, так и для национальной безопасности.

С 2022 г. вводится запрет на покупку иностранного программного обеспечения для целей использования на значимых объектах КИИ, а с 2025 г. вводится запрет на использование иностранного программного обеспечения и программно-аппаратных комплексов на значимых объектах КИИ. Основной целью является обеспечение применения преимущественно отечественного оборудования и программно-аппаратных комплексов на значимых объектах КИИ.

К сотрудникам, занятым на предприятиях критической информационной инфраструктуры, работодатели предъявляют высокие требования, так как сотрудники обеспечивают безопасность объектов КИИ. Сотрудникам необходимо обладать целым комплексом компетенций, в том числе и компетенциями безопасности.

За последние пять лет число и масштаб экономических преступлений внутри компании существенно выросли, сотрудники компании имеют доступ к конфиденциальной информации, к которой относятся: хищение ресурсов, промышленный шпионаж, разглашение коммерческой тайны, что в итоге может нанести колоссальный вред экономике предприятия. Корпоративное мошенничество, инсайдинг, комплаенс-риски встречаются очень часто и напрямую связаны с внутренними угрозами предприятия. Несмотря на их распространенность, до сих пор нет четкого представления о том, как с этим бороться. Часто применяются отдельные инструменты и методы по борьбе с отдельными видами угроз, что ведет к тому, что нейтрализуются последствия проблем.

Удаленная работа во время пандемии, непрофессионализм сотрудников, неконтролируемые каналы передачи информации, ошибки и просчеты в деятельности сотрудников КИИ, хищения, мошеннические действия, разглашение сведений ограниченного доступа и т.п. увеличивают риски безопасности. Основной угрозой является неблагонадежный персонал.

В связи с этим встает остро проблема оценки сотрудников на благонадежность. В настоящее время существующие методы оценки не позволяют дать качественную оценку компетенциям сотрудников в изменяющихся условиях и определить уровень благонадежности.

Специфика предприятий КИИ

Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной

системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [3] является отправной точкой по организации работ по защите информационной инфраструктуры в РФ. В июле 2017 г. был подписан Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4], который вступил в силу с 1 января 2018 г.

Законодательство Российской Федерации определяет критическую информационную инфраструктуру как «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». Объектами КИИ являются: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ [4]. Объекты КИИ подлежат защите в соответствии с законодательством РФ [5].

Субъектами КИИ являются государственные органы, государственные учреждения, юридические лица или индивидуальные предприниматели, которым принадлежат объекты КИИ, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности [4]. Данные сферы являются стратегически важными для государства, так как обеспечивают безопасность и обороноспособность страны, решают государственные задачи.

На предприятиях КИИ отсутствуют в настоящее время специалисты, имеющие диплом в области КИИ. Подготовка данных специалистов является приоритетной. Сегодня специалист по информационной безопасности не всегда имеет глубокие знания в области КИИ. Специалист с глубокими знаниями, в том числе и в области КИИ, и высоким уровнем владения необходимыми компетенциями является основой кадровой безопасности предприятия.

Кадровая безопасность организации

Кадровая безопасность является составной частью системы общей безопасности организации наряду с другими составляющими – финансовой, силовой, информационной, технико-технологической, правовой, экологической и др.

На основе анализа понятий, применяемых к кадровой безопасности, выделяются следующие:

– как процесс предупреждения негативных воздействий на безопасность [6, 7];

– как элемент экономической безопасности [8–10];

– как состояние защищенности [11, 12];

– как элемент кадровой политики (или кадровой работы) [13, 14];

– как фактор обеспечения конкурентных преимуществ [15];

– как система взаимодействия [16, 17];

– как элемент национальной безопасности [18, 19].

В западной литературе используется понятие personnel security [20], или «кадровая безопасность» (безопасность персонала, безопасность личности). В некоторых странах, таких как Норвегия, Япония, безопасность личности включена в официальные документы по внутренней и внешней политике.

Под кадровой безопасностью понимается «система предприятия, связанная с эффективной работой персонала и функционированием организации (предприятия) в условиях безопасности и направленная на развитие самой организации в целом и каждого сотрудника в отдельности» [21].

В настоящее время кадровая безопасность рассматривается как взаимодействие работодателя и сотрудников. Работодатель со своей стороны предоставляет сотруднику условия труда в соответствии с установленными требованиями законодательства, в том числе и в области КИИ, а также в соответствии с установленной на предприятии кадровой политикой и корпоративной культурой. В свою очередь, сотрудник обеспечивает выполнение основных задач, возложенных на него в силу владения определенным набором компетенций и характеристик, требуемых в рамках выполнения служебных обязанностей.

Для обеспечения кадровой безопасности предприятия наиболее важным аспектом являются правильно подобранные благонадежные кадры, обладающие требуемыми компетенциями, так как именно на них возложена обязанность по обеспечению безопасности объектов КИИ в рамках требований, установленных законодательством.

Благонадежность сотрудников имеет важное значение для организации. Несмотря на то, что благонадежность является динамичным процессом, подверженным влиянию внутренних и внешних причин, она обеспечивает предсказуемое поведение сотрудника.

Благонадежный сотрудник – это «надежный сотрудник, отвечающий профессиональным требованиям работодателя, разделяющий ценности компании и общества, а также готовый работать на развитие себя и компании в целом» [22].

Благонадежность сотрудника проявляется только в его деятельности. Уровень благонадежности персонала – это уровень владения компетенциями, отражающими все аспекты деятельности сотрудника.

В настоящее время нет единой методики оценки благонадежности сотрудника. В последнее время появляются работы по оценке благонадежности контрагентов [23–25].

С целью определения уровня благонадежности сотрудника была разработана система кадровой безопасности предприятия, включающая оригинальную методику [26], и разработан программный комплекс [27]. Данная система представляет собой программный комплекс для оценки уровня благонадежности сотрудника, позволяющий проводить оценку персонала и принимать управленческие решения.

Значения от 0–0,449 говорят о низком уровне благонадежности сотрудников, от 0,45–0,749 – о среднем уровне, от 0,75–1 свидетельствуют о высоком уровне благонадежности сотрудника.

Метод оценки уровня благонадежности в системе кадровой безопасности предприятия

В отечественной науке используются несколько методов оценки квалифицированных специалистов: комплексный, интеграционный, функциональный, динамический, воспроизводственный, процессный, нормативный, количественный, поведенческий, ситуационный, системный, структурный, программно-целевой, компетентностный, психологический методы. Данные методы нашли отражение в работах таких авторов, как Ю.Н. Постоева [28], Н.Н. Мехтиханова [29], В.К. Гунин и Д.В. Лестев [30], А. Вучкович-Стадник [31], А.Я. Кибанов [32], И.Г. Дадиверин, М.Д. Розенбаум [33], М.Ф. Мизинцева, А.Р. Сардарян [34], А.Я. Маслова, Н.В. Бардукова [35].

Наряду с исследованиями отечественных ученых, данная тематика оценки квалифицированных специалистов и административно-управленческого персонала исследована и зарубежными учеными, такими как Д. МакКлелланд, Р. Бояцис [36], Г. Читхэм, Дж. Чиверс [37], E. Knasel, J. Meed [38], И. Масааки [39].

Отечественная и зарубежная науки отличаются, также значительные отличия имеет менталитет, что особенно влияет на оценку персонала. Недостатки рассмотренных методов: результаты оценки недостаточно хорошо отображают перспективы развития сотрудника, необъективная оценка в случае стресса сотрудника, неполная информация об уровне развития личностно-деловых качеств сотрудника, необходимость привлечения экспертов с другого предприятия. Данные методы оценки персонала не учитывают уровень благонадежности сотрудника и могут оценивать только личные или профессиональные компетенции, а в некоторых странах используется только статусность.

В основе методики и программного комплекса лежит разработанный автором метод оценки уровня благонадежности в системе кадровой безопасности. Оценка персонала – это процесс выявления необходимых характеристик с целью принятия управленческого решения в отношении сотрудника. Метод оценки – способ измерения объекта оценки (сотрудника) в соответствии с установленными критериями. Данная методика может применяться для действующих сотрудников, а также для претендентов на должности в процессе рекрутинга. В качестве критериев в разработанном методе выступают компетенции сотрудника (К), уровень его основного и дополнительного образования (О) и стаж работы по специальности (Сп).

В системе кадровой безопасности определяются 9 типов компетенций [40]: личные (A), профессиональные (B), корпоративные (C), компетенции безопасности (D), специальные (E), компетенции будущего (F), поведенческие (G), социально-психологические (H), успешности (I). Следовательно,

$$К \in (A, B, C, D, E, F, G, H, I). \quad (1)$$

Каждая из этих компетенций представляет собой сумму компетенций.

Весовые категории для основного (базового) образования (О) составляют 0,2; для стажа (Ст) – 0,3; для компетенций (К) – 0,5.

Модель для определения уровня благонадежности выглядит следующим образом:

$$УБ = 0{,}2 \times О + 0{,}3 \times Ст + 0{,}5 \times К. \quad (2)$$

Данный метод был применен на предприятии КИИ. На первом этапе для сотрудников были разработаны профили компетенций по каждой должности. В составлении профиля участвовали 5 экспертов (табл. 1).

Таблица 1

Состав экспертной группы

Должность	Стаж	Образование	Опыт оценки персонала и определения компетенций
Начальник HR-отдела	15	Управление персоналом	15
Психолог	18	Психология	18
Специалист по КБ	7	Менеджмент организации / Управление персоналом	7
Специалист по оценке персонала	9	Управление персоналом	8
Начальник отдела оценки и аттестации персонала	8	Управление персоналом	7

Для составления профиля использовались профессиональные стандарты, должностные инструкции, нормативная правовая база организации в области организации и деятельности персонала, метод наблюдения и собеседования, форсайт-технологии.

Личные компетенции (A):

$$A = \{a_1, a_2, \ldots, a_n\}. \quad (3)$$

Среди этих компетенций: a_1 – способность быстро реагировать на ситуацию; a_2 – высокий уровень персональной ответственности; a_n – способность к стрессоустойчивости.

Профессиональные компетенции:

$$B = \{b_1, b_2, \ldots, b_q\}, \quad (4)$$

К ним относились: b_1 – способность работать в информационных системах; b_2 – способность управлять объектами КИИ; b_q – способность проводить мониторинг угроз.

Корпоративные компетенции:

$$C = \{c_1, c_2 \ldots c_m\}. \quad (5)$$

В корпоративные компетенции вошли: c_1 – готовность к кооперации с коллегами; c_2 – способность соблюдать регламент и нормы предприятия и пр.

Аналогичным образом были подобраны экспертным путем остальные 6 типов компетенций.

Компетенции безопасности:

$$D = \{d_1, d_2. \ldots, d_i\}, \quad (6)$$

d_1 – способность к оценке рисков; d_2 – способность выполнять должностные обязанности по обеспечению законности и правопорядка, безопасности личности, общества и государства; d_i – способность проявлять психологическую устойчивость в сложных и экстремальных условиях.

Специальные компетенции:

$$E = \{e_1, e_2 \dots e_l\}, \quad (7)$$

e_1 – способность принимать решения в условиях неопределенности; e_2 – аналитическое мышление; e_l – способность проводить анализ данных, аналитику.

Компетенции будущего:

$$F = \{f_1, f_2 \dots f_k\}, \quad (8)$$

f_1 – способность моделировать развитие событий, ситуаций; f_2 – способность к использованию методов проектирования, построения и управления корпоративной архитектурой, управления ИТ-системами; f_k – способность применять квантовые технологии.

Поведенческие компетенции:

$$G = \{g_1, g_2 \dots g_p\}, \quad (9)$$

g_1 – эмоциональный интеллект; g_2 – способность соблюдать субординацию и др.

Социально-психологические компетенции:

$$H = \{h_1, h_2 \dots h_s\}, \quad (10)$$

h_1 – коммуникативные компетенции; h_2 – способность к сотрудничеству и др.

Компетенции успешности:

$$I = \{i_1, i_2, \dots i_t\}, \quad (11)$$

i_1 – способность извлекать уроки из собственных поступков и поступков других людей; i_2 – способность к саморазвитию и самообучению и др.

После того как составлен профиль компетенций, компетенции вносятся в программный комплекс «Система кадровой безопасности предприятия», и экспертная часть системы Expert определяет набор тестовых заданий, который должен пройти сотрудник. Кроме тестовых заданий, имеющихся в системе, сотрудники проходят анкету и кейсы, специально разработанные для сотрудников КИИ. Кейсы были составлены в соответствии с профилем компетенций сотрудников КИИ и написаны под конкретные категории пользователей информационной системы, такие как пользователи, администратор безопасности и системный администратор.

Комплекс позволяет произвести оценку уровня благонадежности в диапазоне от 0 до 1.

Некоторые виды тестов ограничены по времени прохождения. У кандидата только одна попытка на прохождение теста. В случае если сотрудник не укладывается во времени, ему система ставит – 2.

Экспериментальная часть

Для апробации метода и методики был протестирован 31 сотрудник предприятия КИИ (предприятие «Росатома»). В данной организации для оценки применяется модель компетенций, основанная на отраслевых ценностях корпорации. Для оценки используется система РЕКОРД. Данная система оценивает результативность сотрудника по картам КПЭ, а также профессионально-технические знания, умения и навыки и оценку корпоративных ценностей.

Были получены результаты, представленные в табл. 2.

Таким образом, по итогам анкетирования сотрудники получили уровень благонадежности 0,6, по итогам тестирования – 0,61, по итогам кейса – 0,62. Все показатели входят в диапазон 0,45–0,74, что составляет «средний» уровень благонадёжности сотрудников.

Таблица 2

Результаты анкетирования, тестирования и прохождения кейсов

ID	Уровень благонадежности по итогам анкетирования	Уровень благонадежности по итогам тестирования	Уровень благонадежности по итогам кейсов
111	0,69	0,69	0,70
112	0,59	0,60	0,58
113	0,49	0,50	0,53
114	0,51	0,51	0,49
115	0,58	0,58	0,63
116	0,53	0,54	0,50
117	0,55	0,56	0,55
118	0,57	0,57	0,59
119	0,55	0,55	0,62
120	0,71	0,72	0,69
121	0,70	0,71	0,74
122	0,58	0,58	0,69
123	0,67	0,67	0,69
124	0,49	0,50	0,48
125	0,51	0,51	0,53
126	0,47	0,48	0,61
127	0,49	0,50	0,51
128	0,53	0,54	0,57
129	0,55	0,55	0,59
130	0,54	0,55	0,53
131	0,71	0,72	0,75
132	0,70	0,70	0,73
133	0,68	0,69	0,71
134	0,67	0,67	0,66
135	0,69	0,70	0,71
136	0,64	0,64	0,68
137	0,65	0,66	0,66
138	0,66	0,66	0,67
139	0,59	0,60	0,58
140	0,61	0,64	0,64
141	0,65	0,68	0,67

На основе анкетирования собираются фактические данные о сотруднике, на этапе тестирования определяются компетенции, выявленные в ходе тестирования, но часто сотрудники в ходе тестирования отвечают на вопросы так, как они хотели бы видеть себя, а уже в кейсах проверяется уровень владения компетенциями на основе реальных ситуаций. Следовательно, получена полная характеристика сотрудника.

В программном комплексе на основе правил «если…, то…» определены экспертным путем правила согласно образованию и стажу работы (табл. 3).

Рассмотрим определение уровня благонадежности для конкретного сотрудника, учитывая формулу (2):

$$УБ_{ID141} = 0{,}2 \times 0{,}5 + 0{,}3 \times 0{,}8 + 0{,}5 \times 0{,}67 = 0{,}68.$$

У данного сотрудника базовое образование по информационной безопасности, работает он по специальности в течение 10 лет в системе информационной безопасности, по итогам трех этапов уровень благонадежности составляет 0,67.

Рассчитаем корреляцию с помощью коэффициентов ранговой корреляции Спирмена [41].

Вначале сравним данные по уровню благонадежности по результатам анкетирования с данными по результатам тестирования.

Таблица 3

Правила для определения коэффициента по критериям «Образование» и «Стаж работы по специальности»

Образование				
Если	Без образования	то	=	0
Если	Полное средние образование	то	=	0,1
Если	Среднее специальное	то	=	0,2
Если	Бакалавриат	то	=	0,3
Если	Магистратура	то	=	0,4
Если	Специалитет	то	=	0,5
Если	Кандидат наук	то	=	0,6
Если	Доктор наук	то	=	0,7
Если	PhD	то	=	0,8
Если	С базовым высшим профильным образованием + курсы повышения квалификации	то	=	0,9
Если	С базовым высшим профильным образованием + дополнительное образование в области КИИ	то	=	1
Стаж работы				
Если	Без опыта	то	=	0
Если	До 1 года	то	=	0,2
Если	От 1 до 3 лет	то	=	0,4
Если	От 3 до 6 лет	то	=	0,6
Если	От 6 до 10 лет	то	=	0,8
Если	Свыше 10 лет	то	=	1

Среди значений признаков x и y имеются несколько одинаковых, это говорит о том, что образуются связанные ранги. Следовательно, коэффициент Спирмена рассчитаем по формуле

$$p = 1 - \frac{\sum 6d^2 + A + B}{n^3 - n}, \qquad (12)$$

где

$$A = \frac{1}{12}\sum (A_j^3 - A_j), \qquad (13)$$

$$B = \frac{1}{12}\sum (B_k^3 - B_k), \qquad (14)$$

j – номера связок по порядку для признака x; A_j – число одинаковых рангов в j-й связке по x; k – номера связок по порядку для признака y; B_k – число одинаковых рангов в k-й связке по y.

$A = [(23–2) + (23–2) + (33–3) + (23–2) + (23–2) + (23–2) + (33–3) + (23–2) + (23–2) + (23–2) + (23–2)]/12 = 8,5;$

$B = [(23–2) + (23–2) + (33–3) + (23–2) + (23–2) + (23–2) + (33–3) + (23–2) + (23–2) + (23–2) + (23–2) + (23–2)]/12 = 9;$

$$D = A + B = 8,5 + 9 = 17,5;$$

$$p = 1 - \frac{6 \cdot 24,5 + 17,5}{31^3 - 31} = 0,994.$$

В результате вычисления значение коэффициента корреляции равно 0,99, что говорит о сильной связи. Аналогично сравниваем данные по тестированию и кейсам. Получаем значение 0,89, что говорит также о сильной связи.

Как видим, процедура получения данных табл. 2 показывает зависимость выборок по столбцам. Применим поэтому к данным табл. 2 W-критерий Уилкоксона [42, 43].

Имеем при попарном сравнении столбцов $W_{13} = 67,5$; $p_{13} = 0,0007$; $W_{23} = 119,0$; $p_{23} = 0,032$. Принимаем уровень $p < 0,05$. Тогда для числа наблюдений $n = 31$ критическое значение из таблицы [44] равно 163, и нет оснований для отклонения нулевой гипотезы. Результаты тестирования и анкетирования дополняют друг друга при исследовании благонадёжности, применимость данного метода для оценки персонала обоснована. Заметим также, что, так как $p_{23} = 0,032$, то повышение ожиданий к уровню значимости ($p < 0,01$) при применении данной методики было бы не обосновано.

Полученные данные говорят о том, что оценку уровня благонадежности необходимо применять с использованием методов анкетирования, тестирования и кейсов, а, следовательно, можно говорить о применимости данного метода для оценки персонала. Данный метод был внедрен на предприятия КИИ и данные подтверждены актами внедрения. Данные оценки сотрудников предприятия КИИ в целом коррелируют с оценками, полученными в применяемых на предприятии отраслевых системах оценки персонала (система РЕКОРД). На основании полученных данных система позволяет формировать индивидуальные траектории развития сотрудников предприятия.

Заключение

Система кадровой безопасности предприятия позволяет проводить регулярную оценку персонала предприятия для определения уровня благонадежности.

Метод оценки уровня благонадежности сотрудников позволяет применить дифференцированный индивидуальный подход, учитывающий требования безопасности, распределения ролей в организации, полномочий при работе с объектами КИИ. Данная оценка позволяет формировать индивидуальные планы развития и повышения квалификации сотрудников, занятых на объектах КИИ.

Комплексная оценка персонала с использованием метода оценки сотрудников на основе профиля компетенций способствует укреплению кадровой безопасности предприятия, минимизируя риски, связанные с персоналом, а также дает качественную оценку.

Литература

1. Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р «Программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf, свободный (дата обращения: 15.03.2022).

2. Указ Президента Российской Федерации от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71670570/, свободный (дата обращения: 15.03.2022).

3. Указ Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс]. – Режим доступа:

http://static.kremlin.ru/media/acts/files/0001201301210012.pdf, свободный (дата обращения: 22.03.2022).

4. Федеральный закон Российской Федерации от 26.07.2017 № 187–ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/, свободный (дата обращения: 10.03.2022).

5. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202203300001, свободный (дата обращения: 10.04.2022).

6. Гречишкина А.А. Сущность понятия «кадровая безопасность» предприятий железнодорожного транспорта // Научный вестник Херсонского гос. ун-та. Сер.: Экономические науки. – 2014. – Вып. 6, ч. 2. – С. 144–146.

7. Козаченко А.В. Экономическая безопасность предприятия: сущность и механизмы обеспечения / А.В. Козаченко, В.П. Пономарев, О.М. Ляшенко. – Киев: Либра, 2003. – 280 с.

8. Васильчак С.В. Кадровая безопасность предпринимательства – основа экономического развития // Научный вестник НЛТУ Украины. – 2009. – Вып. 19.12. – С. 122–128.

9. Калиниченко Л.Л. Методологический подход к управлению персоналом предприятий железнодорожного транспорта в условиях реформирования отрасли. – Харьков: УкрДазт, 2012. – 382 с.

10. Махеда Н.Г. Социально-мотивационные составляющие кадровой безопасности / Н.Г. Махеда, А.И. Маренич // Финансовый журнал: междунар. науч.-практ. журнал / Черкасский институт банковского дела НБУ (г. Киев). – 2012. – № 2(6). – С. 38–45.

11. Борисов И.А. Кадровая безопасность России: ключевые проблемы и пути решения / И.А. Борисов, С.Б. Гиниева // Достойный труд – основа стабильного общества: матер. VI Междунар. науч.-практ. конф.: в 2 т. – Т. 1. – Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2014. – 290 с.

12. Кадровая безопасность как один из ключевых факторов экономической безопасности региона / С.Н. Митяков, М.В. Ширяев, Н.Н. Яковлева, Ц. Чжао // Экономическая безопасность России: проблемы и перспективы: матер. II Междунар. науч.-практ. конф. – Нижний Новгород: Нижегородский гос. техн. ун-т им. Р.Е. Алексеева, 2014. – С. 216–221.

13. Кадровая безопасность в системе экономической безопасности / Г.Е. Крохичева, Э.Л. Архипов, М.А. Виноградова, Д.Е. Деточка // Интернет-журнал «Науковедение». – Т. 8, № 3 (2016) [Электронный ресурс]. – Режим доступа: http://naukovedenie.ru/PDF/94EVN316.pdf (дата обращения: 15.03.2022).

14. Назарова Г. Предпосылки создания системы кадровой безопасности предприятия // Региональные аспекты развития производительных сил Украины: науч. журн. / Терноп. нац. экон. ун-т. – 2010. – Вып. 15. – С. 34–37.

15. Алавердов А.Р. Управление кадровой безопасностью организации: учеб. – 2-е изд., доп. и перераб. – М.: Университет «Синергия», 2020. – 460 с.

16. Кадровая безопасность предприятия: подходы, диагностика, направления совершенствования / В.А. Фурсов, Н.В. Лазарева, Е.Н. Кущ, К.Г. Аветова // Вестник Алтайской академии экономики и права. – 2020. – № 4-2. –С. 270–276.

17. Щелоков В.Ф. Кадровая безопасность корпорации в системе глобальной безопасности России // Проблемы обеспечения геополитической безопасности России: матер. Всерос. науч.-практ. конф., Екатеринбург, 24–25 сентября 2009 г. / Законодат. Собрание Свердл. обл.; Урал. отд. РАН; Урал. гос. ун-т им. А.М. Горького и др.; науч. ред. Н.Н. Целищев. – Екатеринбург: УрГУ, 2009. – С. 141–142.

18. Анализ современного состояния научных исследований в сфере кадровой безопасности / Е.А. Астахова, Н.А. Ларионова, Л.Н. Панькова, Д.Б. Чупрова // Вестник Северо-Кавказского фед. ун-та. – 2018. – № 5 (68). – С. 31–40.

19. Нефедов В.А. Кадровая политика как фактор национальной безопасности: региональный аспект: дис. ... канд. полит. наук: 23.00.02. Сев.-Кавказ. акад. гос. службы. – Ростов н/Д, 2009. – 138 с.

20. Personnel security risk assessment a guide [Электронный ресурс]. – Режим доступа: https://www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf (дата обращения: 21.03.2022).

21. Глухарева С.В. Методика подбора персонала на должности, связанные с обработкой конфиденциальной информации // Безопасность информационного пространства – 2017: XVI Всерос. науч.-практ. конф. студентов, аспирантов, молодых ученых. Екатеринбург, 12 декабря 2017 г. – Екатеринбург: Изд-во Урал. ун-та, 2018. – С. 154–158.

22. Глухарева С.В., Абросимова М.Е. Благонадежный сотрудник в системе кадровой безопасности предприятия [Электронный ресурс]. – Режим доступа: https://storage.tusur.ru/files/115519/2018_4.pdf (дата обращения: 10.03.2022).

23. Степовая А.Ю. Критерии оценки благонадежности контрагентов как элемент методики внутреннего налогового контроля торговой организации // Современные проблемы развития экономики России и Китая: матер. междунар. науч.-практ. конф., посвященной 20-летию экономического фак-та АмГУ. – Благовещенск: Изд-во Амур. гос. ун-та, 2021. – С. 169–172.

24. Секриеру В. Оптимизация процесса проверки контрагента на благонадежность // Актуальные проблемы и перспективы развития экономики: российский и зарубежный опыт. – 2020. – № 3. – С. 28. – Режим доступа: https://www.elibrary.ru/item.asp?id=42918900 (дата обращения: 21.03.2022).

25. Дедова Е.С. Тренды развития технологии оценки благонадежности контрагентов // Экономическая безопасность: концепция, стандарты. – 2017. – 192 с. – Режим доступа: https://www.elibrary.ru/download/elibrary_30694904_29082925.pdf (дата обращения: 21.03.2022).

26. Шелупанов А.А. Оценка благонадежности сотрудника в системе кадровой безопасности предприятия / А.А. Шелупанов, С.В. Глухарева, М.М. Немирович-Данченко // Доклады ТУСУР. – 2021. – Т. 24, № 4. – С. 52–57. DOI: 10.21293/1818–0442–2021–24–4–52–57.

27. Св-во о рег. программы для ЭВМ RU 2019616940, 30.05.2019. Система кадровой безопасности предприятия / С.В. Глухарева, А.А. Шелупанов, Е.В. Мареева, М.Е. Абросимова, А.С. Еременко, В.Е. Мальцев. Заявка № 2019616011 от 24.05.2019.

28. Постоева Ю.Н. Современные методы к оценке профессиональных компетенций сотрудников организации // Инновационные технологии в образовании и науке: матер. II Междунар. науч.-практ. конф., Чебоксары, 10 сент. 2017 г. – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 376–381.

29. Мехтиханова Н.Н. Психологическая оценка персонала: учеб. пособие. – Ярославль: ЯрГУ, 2013. – 116 с.

30. Гунин В.К. Современные методы оценки персонала в процессе отбора / В.К. Гунин, Д.В. Лестев // Экономика и управление: анализ тенденций и перспектив развития. – 2014. – № 13. – С. 39–42.

31. Вучкович-Стадник А. Оценка персонала. Четкий алгоритм действий и качественные практические решения [Электронный ресурс]. – Режим доступа: https://www.litres.ru/alla-vuchkovich-stadnik/ocenka-personala-chetkiy-algoritm-deystviy-i-kachestvennye-prakticheskie-resheniya/ (дата обращения: 10.04.2022).

32. Кибанов А.Я. Управление персоналом организации: актуальные технологии найма, адаптации и аттестации: учеб. пособие / А.Я. Кибанов, И.Б. Дуракова. – 2-е изд., стер. – М.: КНОРУС, 2012. – 368 с.

33. Дадиверин И.Г. Комплексная психологическая оценка профессионализма персонала производственного объединения / И.Г. Дадиверин, М.Д. Розенбаум // Психологический журнал. – 1995. – Т. 16, № 3.

34. Мизинцева М.Ф. Оценка персонала: учебник и практикум для бакалавров / М.Ф. Мизинцева, А.Р. Сардарян. – М.: Юрайт, 2014. – 378 с.

35. Маслова А.Я. Разработка системы комплексной оценки в концепции управления по результатам / А.Я. Маслова, Н.В. Бардукова // Инновационные технологии в науке и образовании. – 2016. – № 44. – С. 92–96.

36. Boyatzi, R.E. The competent manager: A model for effective performance. – New York: WileyInterscience. Brewster, 1982. – 340 p.

37. Cheetham G. The reflective (and competent) practitioner: A model of professional competence which seeks to harmonise the reflective practitioner and competence-based approaches / G. Cheetham, Dg. Chivers [Электронный ресурс]. – Режим доступа: http://www.smithsrisca demon.co.uk/PSYcheethametal1998.html (дата обращения: 21.03.2022).

38. Knasel E.G. Learn for Your Life: A Blueprint for Continuous Learning, Financial Times Prentice Hall / E.G. Knasel, J. Meed, A. Rossetti. – L.: DfEE, 2000. – 272 p.

39. Масааки И.К. Ключ к успеху японских компаний Kaizen: The Key to Japan's Competitive Success. – М.: Альпина Паблишер, 2009. – 280 с.

40. Глухарева С.В. Определение востребованных на рынке труда компетенций // Современное образование: повышение конкурентоспособности университетов: матер. междунар. науч.-метод. конф.: в 2 ч. – Томск, 2021. – С. 109–113.

41. Кремер Н.Ш. Эконометрика: учеб. для вузов / Н.Ш. Кремер, Б.А. Путко; под ред. Н.Ш. Кремера. – М.: ЮНИТИ-ДАНА, 2002. – 311 с. [Электронный ресурс]. – Режим доступа: https://matematem.ru/wp-con-tent/uploads/2016/02/Kremer-Ekonometrika-1.pdf (дата обращения: 10.03.2022).

42. Fitzgerald Sh. The basics of nonparametric statistics. Work (Reading, Mass.) / Sh. Fitzgerald, D. Dimitrov, Ph. Rumrill. – 2001. – No. 16. – P. 287–292.

43. Kolassa J.E. An Introduction to Nonparametric Statistics. – Taylor & Francis Ltd, 2020. – 212 p.

44. Runyon R.P. Nonparametric statistics: a contemporary approach. – Reading, MA: Addison Wesley, 1977. – P. 218.

Глухарева Светлана Владимировна
Ст. преп. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-913-889-48-42
Эл. почта: gsv@fb.tusur.ru

Glukhareva S.V.

A method for assessing the level of reliability of employees in the personnel security system of an enterprise (using the example of CII enterprises)

The article discusses a method for assessing the level of trustworthiness based on the compilation of a competence profile. This method provides a qualitative assessment of employee competencies and has been applied to employees employed at critical information infrastructure enterprises. The article presents the approbation data, shows the consistency of the expert assessment.

Keywords: competence profile, personnel security, level of trustworthiness, CII enterprises.
DOI: 10.21293/1818-0442-2022-25-2-59-67

References

1. *Rasporyazheniye pravitel'stva Rossiyskoy Federatsii ot 28 iyulya 2017 g. № 1632-r «Programma «Tsifrovaya ekonomika Rossiyskoy Federatsii»* [Decree of the Government of the Russian Federation dated July 28, 2017 No. 1632-r «Program «Digital Economy of the Russian Federation». Available at: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (accessed: March 15, 2022), free (accessed: March 15, 2022) (in Russ.).

2. *Ukaz Prezidenta Rossiyskoy Federatsii ot 09.05.2017 № 203 «O strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017-2030 gody»* [Decree of the President of the Russian Federation dated 09.05.2017 No. 203 «On the Strategy for the development of the Information Society in the Russian Federation for 2017-2030»]. Available at: https://base.garant.ru/71670570/, free (accessed: March 15, 2022) (in Russ.).

3. *Ukaz Prezidenta Rossiyskoy Federatsii ot 15.01.2013 g. № 31s «O sozdanii gosudarstvennoy sistemy obnaruzheniya, likvidatsii i likvidatsii posledstviy komp'yuternykh atak na resursy Rossiyskoy Federatsii»* [Decree of the President of the Russian Federation No. 31c dated 15.01.2013 «On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation»]. Available at: http://static.kremlin.ru/media/acts/files/0001201301210012.pdf, free (accessed: March 22, 2022) (in Russ.).

4. *Federal'nyy zakon Rossiyskoy Federatsii ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoy informatsii konfidentsial'noy informatsii Rossiyskoy Federatsii»* [Federal Law of the Russian Federation No. 187-FZ dated 26.07.2017 «On the Security of the Critical Information Infrastructure of the Russian Federation»]. Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/, free (accessed: March 10, 2022) (in Russ.).

5. Ukaz Prezident Rossiyskoy Federatsii ot 30.03.2022 № 166 «O merakh po poisku tekhnologicheskoy nezavisi-mosti i bezopasnosti Rossiyskoy kriticheskoy informatsionnoy infrastruktury Federatsii» [Decree of the President of the Russian Federation No. 166 dated 30.03.2022 «On Measures to Ensure the Technological Independence and Security of the Critical Information Infrastructure of the Russian Federation»]. Available at: http://publication.pravo.gov.ru/Docu-ment/View/0001202203300001, free (accessed: March 10, 2022) (in Russ.).

6. Grechishkina A.A. *Sushchnost' ponyatiya «kadrovaya bezopasnost'« predpriyatiy zheleznodorozhnogo transporta* [The essence of the concept of «personnel safety» of railway transport enterprises]. *Scientific Bulletin of Kherson State University. The series «Economic Sciences»*, 2014, iss. 6, part. 2, pp. 144–146 (in Russ.).

7. Kozachenko A.V., Ponomarev V.P., Lyashenko O.M. *Ekonomicheskaya bezopasnost' predpriyatiya: sushchnost' i mekhanizmy obespecheniya* [Economic security of the enterprise: the essence and mechanisms of ensuring]: monograph. Kiyev, Libra, 2003, 280 p. (in Russ.).

8. Vasilchak S.V. *Kadrovaya bezopasnost' predprinimatel'stva – osnova ekonomicheskogo razvitiya* [Personnel security of entrepreneurship – the basis of economic development]. *Scientific Bulletin of NLTU of Ukraine,* 2009, iss. 19.12, pp. 122–128 (in Russ.).

9. Kalinichenko L.L. *Metodologicheskiy podkhod k upravleniyu personalom predpriyatiy zheleznodorozhnogo transporta v usloviyakh reformirovaniya otrasli* [Methodological approach to personnel management of railway transport enterprises in the conditions of industry reform]: monograf. Kharkiv, UkrDazt, 2012, 382 p. (in Russ.).

10. Makeda N.G., Marenich A.I. *Sotsial'no-motivatsionnyye sostavlyayushchiye kadrovoy bezopasnosti* [Sociomotivational components of personnel security]. *Financial Journal: International Scientific and Practical Journal,* Cherkasy Institute of Banking of the NBU, Kiev, 2012, no. 2(6), pp. 38–45 (in Russ.).

11. Borisov I.A., Ginieva S.B. Kadrovaya bezopasnost' Rossii: osnovnyye problemy i puti resheniya [Personnel security of Russia: key problems and solutions]. *Decent work is the basis of a stable society: materials of the VI International Scientific and Practical Conference*: in 2 vols, Yekaterinburg, Publishing House of the Ural State Economy. un-ta, 2014, vol. 1, 290 p. (in Russ.).

12. Mityakov S.N. *Kadrovaya bezopasnost' kak odin iz klyuchevykh faktorov ekonomicheskoy bezopasnosti regiona* [Personnel security as one of the key factors of economic security of the region]. *Economic security of Russia: problems and prospects: materials of the II International Scientific and Practical Conference*, Nizhny Novgorod, Nizhny Novgorod State Technical University named after R.E. Alekseev, 2014, pp. 216–221 (in Russ.).

13. Krokhicheva G.E. *Kadrovaya bezopasnost' v sisteme ekonomi-cheskoy bezopasnosti* [Personnel security in the system of economic security]. *Online journal «Science»,* 2016, *v*ol. 8, no. 3. Available at: http://naukovedenie.ru/PDF/94EVN316.pdf, (Accessed: March 15, 2022) (in Russ.).

14. Nazarova G. *Predposylki sozdaniya sistemy kadrovoy bezopasnosti predpriyatiya* [Prerequisites for the creation of a personnel security system of the enterprise]. *Regional aspects of the development of the productive forces of Ukraine*: *Scientific Journal of Ternopol National Economic University*, 2010, iss. 15, pp. 34–37 (in Russ.).

15. Alaverdov A.R. *Upravleniye kadrovoy bezopasnosti organizatsii* [Personnel security management of the organization] textbook, Moscow, The University of «Sinergia», 2020, 460 p. (in Russ.).

16. Fursov V.A., Lazareva N.V., Kushch E.N., Avezova K.G. *Kadrovaya bezopasnost' predpriyatiya: podkhody, diagnostika, napravleniya s otravleniyem* [Personnel security of the enterprise: approaches, diagnostics, directions of improvement]. *Bulletin of the Altai Academy of Economics and Law*, 2020, no. 4-2, pp. 270–276 (in Russ.).

17. Shchelokov B.F. *Kadrovaya bezopasnost' korporatsii v sisteme global'noy bezopasnosti Rossii* [Personnel security of the corporation in the global security system of Russia], *Problems of ensuring the geopolitical security of Russia : Materials of the All-Russian Scientific and Practical Conference*, Yekaterinburg, September 24–25, 2009, pp. 141–142 (in Russ.).

18. Astakhova E.A., Larionova N.A., Pankova L.N., Chuprova D.B. *Analiz sovremennogo sostoyaniya nauchnykh issledovaniy v sfere kadrovoy bezopasnosti* [Analysis of the current state of scientific research in the field of personnel security]. *Bulletin of the North Caucasus Federal University,* 2018, no. 5 (68), p. 31–40 (in Russ.).

19. Nefedov V.A. *Kadrovaya politika kak faktor natsional'noy bezopasnosti: regional'nyy aspect* [Personnel policy as a factor of national security: regional aspect]: dissertation, Candidate of Political Sciences: 23.00.02, Rostov-on-Don, 2009, 138 p. (in Russ.).

20. *Personnel security risk assessment a guide.* Available at: https://www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf (accessed: March 15, 2022).

21. Glukhareva S.V. *Metodika podbora personala na dolshnosti, svjazannie sobrabotkoi konfidenzialnoi informazijei* [Methods of personnel selection for tasks related to the processing of confidential information]. *Security of the Information Space.* XVI All-Russian Scientific and Practical Conference of students, postgraduates, young scientists. Yekaterinburg, 2017. Ural University Publishing House, 2018, pp. 154–158 (in Russ.).

22. *Glukhareva S.V., Abrosimova M.E. Blagonadezhnyy sotrudnik v sisteme kadrovoy bezopasnosti predpriyatiya* [Trustworthy employee in the personnel security system of the enterprise]. Available at: https://storage.tusur.ru/files/115519/2018_4.pdf (accessed: March 10, 2022) (in Russ.).

23. Stepovaya A.Yu. *Kriterii otsenki blagonadezhnosti kontragentov kak metodologiya vnutrennego nalogovogo kontrolya torgovoy organizatsii* [Criteria for assessing the reliability of counterparties as an element of the methodology of internal tax control of a trade organization]. *Modern problems of economic development in Russia and China. Materials of the International Scientific and Practical Conference dedicated to the 20th anniversary of the Faculty of Economics of Moscow State University*, Blagoveshchensk, Amur State University, 2021, pp. 169–172.

24. Secrieru V. *Optimizatsiya proverki protsessa kontragenta na blagonadezhnost'* [Optimization of the counterparty verification process for reliability]. *Actual problems and prospects of economic development: Russian and foreign experience,* 2020, no. 3, p. 28. Available at: https://www.elibrary.ru/item.asp?id=42918900 (accessed: March 21, 2022) (in Russ.).

25. Dedova E.S. *Tendentsii razvitiya tekhnologiy otsenki blagonadezhnosti kontragentov* [Trends in the development of technology for assessing the reliability of counterparties]. *Economic security: concept, standards,* 2017, p. 192. Available at: https://www.elibrary.ru/download/elibrary_30694904_29082925.pdf (accessed: March 21, 2022) (in Russ.).

26. Shelupanov A.A. *Otsenka blagonadezhnosti sotrudnikov v sisteme kadrovoy bezopasnosti predpriyatiya* [Assessment of employee reliability in the personnel security system of the enterprise]. *Proceedings of TUSUR University,* 2021, vol. 24, no. 4, pp. 52–57. DOI: 10.21293/1818-0442-2021-24-4-52-57 (in Russ.).

27. Certificate of registration of the computer program RU 2019616940, 30.05.2019. *Sistema kadrovoi bezopasnosti predprijatija* [Personnel security system of the enterprise] / Glukhareva S.V., Shelupanov A.A., Mareeva E.V., Abrosimova M.E., Eremenko A.S., Maltsev V.E. Application no. 2019616011, dated 24.05.2019 (in Russ.).

28. Postoyeva YU. N. *Sovremennyye metody k otsenke professional'nykh kompetentsiy sotrudnikov organizatsii* [Modern methods for assessing the professional competencies of employees of the organization]. *Innovative technologies in education and science : materials of the II International Scientific and Practical Conference* (Cheboksary, September 10, 2017) / Editorial Board: O.N. Shirokov et al., Cheboksary, CNS «Interactive Plus», 2017, pp. 376–381 (in Russ.).

29. Mehtikhanova N.N. *Psikhologicheskaya otsenka personala: ucheb. posobiye* [Psychological assessment of personnel: studies. Manual]. Yaroslav State University named after P.G. Demidov, Yaroslavl, YarGU, 2013, 116 p. (in Russ.).

30. Gunin V.K., Lesteva D.V. *Sovremennyye metody otsenki personala v protsesse otbora* [Modern methods of personnel evaluation in the selection process] // *Economics and Management: Analysis of Trends and Development Prospects,* 2014, no. 13, pp. 39–42 (in Russ.).

31. Vuchkovich-Stadnik A. *Otsenka personala. Chetkiy algoritm deystviy i kachestvennyye prakticheskiye resheniya* [Personnel assessment. A clear algorithm of actions and high-quality practical solutions]. Available at: https://www.litres.ru/alla-vuchkovich-stadnik/ocenka-personala-chetkiy-algoritm-deystviy-i-kachestvennye-prakticheskie-resheniya (accessed: March 21, 2022) (in Russ.).

32. Kibanov A.Ya. *Upravleniye personalom organizatsii: aktu-al'nyye tekhnologii nayma, adaptatsii i attestatsii: uchebnoye posobiye* [Personnel management of the organization: actual technologies of hiring, adaptation and certification: a textbook]. Moscow, KNORUS, 2012, 368 p. (in Russ.).

33. Dadiverin I.G., Rosenbaum M.D. *Kompleksnaya psikhologicheskaya otsenka professionalizma personala proizvodstvennogo ob'yedineniya* [Complex psychological assessment of the professionalism of the staff of the production association]. *Psychological Journal*, 1995, vol.16, no. 3 (in Russ.).

34. Mizintseva M. F. *Otsenka personala* [Personnel assessment: textbook and workshop for bachelors]. Moscow, Yurayt Publishing House, 2014, 378 p. (in Russ.).

35. Maslova A.Ya., Bardukova N.V. *Razrabotka sistemy kompleksnoy otsenki v kontseptsii upravleniya po rezul'tatam* [Development of an integrated assessment system in the management concept based on results]. *Innovative Technologies in Science and Education,* 2016, no. 44, pp. 92–96 (in Russ.).

36. Boyatzis R.E. *The competent manager: A model for effective performance*. New York: WileyInterscience. Brewster, 1982, 340 p.

37. Cheetham G., Chivers, Dg. *The reflective (and competent) practitioner: A model of professional competence which seeks to harmonise the reflective practitioner and competence-based approaches.* Available at: http://www.smiths-risca demon.co.uk/PSYcheethametal1998.html (accessed: March 10, 2022).

38. Knasel E., Meed J., Rossetti A. *Learn for Your Life: A Blueprint for Continuous Learning*. Financial Times Prentice Hall, DfEE, 2000, 272 p.

39. Masaaki I.K. *Klyuch k uspekhu yaponskikh kompaniy Kaizen: The Key to Japan's Competitive Success* [The Key to the success of Japanese companies Kaizen: The Key to Japan's Competitive Success]. Moscow, Alpina Publisher, 2009, 280 p. (in Russ.).

40. Glukhareva S.V. *Opredeleniye vostrebovannykh na rynke truda kompetentsiy* [Definition of competencies in demand on the labor market]. *Modern Education: Increasing the Competitiveness of Universities. Materials of the International Scientific and Methodological Conference,* in 2 parts, Tomsk, 2021, pp. 109–113 (in Russ.).

41. Kremer N.S., Putko B.A. *Ekonometrika* [Econometrics]: Textbook for universities. Moscow, UNITY-DANA, 2002, 311 p. Available at: https://matematem.ru/wp-content/uploads/2016/02/Kremer-Ekonometrika-1.pdf (accessed: March 10, 2022) (in Russ.).

42. Fitzgerald Sh., Dimitrov D., Rumrill Ph. *The basics of nonparametric statistics.* Work (Reading, Mass.), 2001, 16, pp. 287–292.

43. Kolassa J.E. *An Introduction to Nonparametric Statistics*, Taylor & Francis Ltd, 2020, 212 p.

44. Runyon R.P. *Nonparametric statistics: a contemporary approach. Reading*. MA, Addison Wesley, 1977, 218 p.

Svetlana V. Glukhareva
Senior Lecturer, Department of Complex Information Security of Computer Systems, Tomsk State University of Control Systems and Radioelecronics
40, Lenin pr., Tomsk, Russia, 634050
Phone: +7-913-889-48-42
Email: gsv@fb.tusur.ru