УПРАВЛЕНИЕ ПЕРСОНАЛОМ
HUMAN RESOURCE MANAGEMENT

DOI: 10.18287/2542-0461-2023-14-4-134-140

НАУЧНАЯ СТАТЬЯ

УДК 338.46

Дата поступления: 22.06.2023
рецензирования: 28.08.2023
принятия: 30.11.2023

Некоторые аспекты оценки кадровой составляющей экономической безопасности ИТ-компаний в России

М.Е. Цибарева
Самарский национальный исследовательский университет
имени академика С.П. Королева, г. Самара, Российская Федерация
E-mail: cibareva.me@ssau.ru. ORCID: https://orcid.org/0000-0001-8559-1839

Аннотация: Быстро развивающаяся отрасль информационных технологий в условиях ухода с российского рынка также известных ИТ-брендов, как Intel, IBM, Avast и других, столкнулась с проблемой нехватки квалицированных специалистов, инвестиций, оборудования и программного обеспечения. В условиях ограниченности ресурсов ИТ-компании должны предложить отечественным организациям новое программное обеспечение, которое сможет в полном объеме заменить иностранные аналоги. В рамках импортозамещения, обеспечения технологической независимости и безопасности критической информационной инфраструктуры (КИИ) России были подписаны нормативно-правовые акты, по которым организации, в том числе государственные и ведомственные, обязаны перейти на использование российского программного обеспечения (ПО), в том числе на объектах КИИ. Для решения данной проблемы необходимо обеспечить ИТ-отрасль квалифицированными специалистами, потребность в которых растет не только в количественном отношении, но и в профессиональном. Кадровый голод в ИТ-сфере подрывает экономическую безопасность компаний и может свети на ноль все усилия руководства по противостоянию иностранным информационным технологиям. Данное обстоятельство определило тему исследования – провести оценку кадровой составляющей экономической безопасности ИТ-компаний России с целью выявления проблем и способов развития ИТ-отрасли. Определены компоненты кадровой составляющей экономической безопасности (далее кадровой безопасности): интеллектуальные (количество обученных); эффективность персонала; динамика и движение персонала; физическая безопасность; мотивация персонала. Наиболее уязвимыми оказались компоненты: эффективность труда; физическая безопасность. Анализ данных компонентов позволил определить направления по обеспечению кадровой безопасности, среди которых: повышение ответственности сотрудников за разглашение информации; информирование сотрудников о мерах киберзащиты; обучение (в том числе тренинги) сотрудников с целью повышения их квалификации; раннее воспитание и подготовка молодежи для реализации творческих и инновационных инициатив в ИТ-сфере.

Ключевые слова: кадровая безопасность; информационная инфраструктура; кибербезопасность; активы; кибератаки; физическая безопасность; обучение персонала; оценка кадровой безопасности.

Цитирование. Цибарева М.Е. Некоторые аспекты оценки кадровой составляющей экономической безопасности ИТ-компаний в России // Вестник Самарского университета. Экономика и управление Vestnik of Samara University. Economics and Management. 2023. Т. 14, № 4. С. 134–140. DOI: http://doi.org/10.18287/2542-0461-2022-14-4-134-140.

Информация о конфликте интересов: авторы заявляют об отсутствии конфликта интересов.

Марина Евгеньевна Цибарева – кандидат экономических наук, доцент кафедры управления человеческими ресурсами, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34.

SCIENTIFIC ARTICLE

Submitted: 22.06.2023
Revised: 28.08.2023
Accepted: 30.11.2023

Some aspects of the assessment of the personnel component of the economic security of IT companies in Russia

M.E. Tsibareva
Samara National Research University, Samara, Russian Federation
E-mail: cibareva.me@ssau.ru. ORCID: https://orcid.org/ 0000-0001-8559-1839

Abstract: The rapidly developing information technology industry, in the conditions of withdrawal from the Russian market of well-known IT brands such as Intel, IBM, Avast and others, faced the problem of a shortage of qualified specialists, investments, equipment and software. In conditions of limited resources, IT companies must offer domestic organizations new software that can fully replace foreign analogues. As part of import substitution, ensuring technological independence and security of Russia's critical information infrastructure (CII), regulatory legal acts were signed, according to which organizations, including state and departmental ones, are obliged to switch to using Russian software (software), including at CII facilities. To solve this problem, it is necessary to provide the IT industry with qualified specialists, the need for whom is growing not only quantitatively, but also professionally. The personnel shortage in the IT sector undermines the economic security of companies and can bring to naught all the efforts of the leadership to resist foreign information technologies. This circumstance determined the topic of the study – to assess the personnel component of the economic security of IT companies in Russia in order to identify problems and ways of developing the IT industry. The components of the personnel component of economic security (hereinafter referred to as personnel security) are defined: intellectual (number of trained); personnel efficiency; dynamics and movement of personnel; physical safety; staff motivation. The most vulnerable components were: labor efficiency; physical safety. The analysis of these components made it possible to identify areas for ensuring personnel security, including: increasing the responsibility of employees for disclosing information; informing employees about cyber defense measures; training (including trainings) of employees to improve their skills; early education and training of young people for the implementation of creative and innovative initiatives in the IT field.

Key words: personnel security; information infrastructure; cybersecurity; assets; cyber assets; physical security; personnel training; personnel security assessment.
Citation. Tsibareva M.E. Some aspects of the assessment of the personnel component of the economic security of IT companies in Russia. *Vestnik Samarskogo universiteta. Ekonomika i upravlenie Vestnik of Samara University. Economics and Management*, 2023, vol. 14, no. 4, pp. 134–140. DOI: http://doi.org/10.18287/2542-0461-2022-14-4-134-140. (In Russ.)
Information on the conflict of interest: author declares no conflict of interest.

Marina E. Tsibareva – Candidate of Economics, associate professor of the Department of Human Resource Management, Samara National Research University, 34, Moskovskoe shosse, Samara, 443086, Russian Federation.

Введение

Кадровое управление является составным элементом экономической безопасности организации и способствует повышению устойчивости ее деятельности к внешним и внутренним угрозам. Внешние и внутренние угрозы связаны с управлением персонала, наращиванием и развитием человеческого капитала, формированием гармоничных социально-трудовых отношений в коллективе.

К актуальным проблемам, стоящих перед кадровым менеджментом, можно отнести: нехватка квалифицированных кадров; низкая мобильность граждан; информационная пропаганда; структурные сдвиги (названы перспективные отрасли экономики, среди которых IT-направления); мотивационные аспекты (низкие заработные платы на фоне роста цен), и другие.

Цель исследование – провести оценку кадровой составляющей экономической безопасности ИТ-компаний России с целью выявления проблем и способов развития данной отрасли.

В работе дано теоретическое обоснование кадровой составляющей экономической безопасности. Раскрыты особенности реализуемого кадрового менеджмента ИТ-компаний. Представлена методология оценки кадровой составляющей экономической безопасности. Выявлены проблемы и способы развития ИТ-отрасли.

В процессе выполнения исследования автором были использованы методы сравнительного анализа, статистического анализа, аналитического, логического, и экономико-математического. Данные методы позволили автору дать объективную оценку кадровой составляющей экономической безопасности ИТ-компаний России, установить проблемы и предложить способы развития ИТ-отрасли.

В качестве информационной базы использованы материалы Федеральной службы государственной статистики, ИТ-компании из официальных источников, Федеральной налоговой службы, нормативно-правовой базы.

Теоретическая и методологическая основа кадровой составляющей экономической безопасности построена на работах российских и зарубежных авторов. Анализ информационной базы ИТ-компании позволил сделать основные выводы исследования.

Понятие «безопасность» в ФЗ «О безопасности» представлено, как соблюдение прав и свобод человека, законность применения мер обеспечения безопасности и необходимость взаимодействия с различными государственными и местными органами власти, общественными и иными организациями, гражданами страны [1]. Потребность в обеспечении безопасности личности, экономических субъектов, общества, государства появилась в результате возникновения опасности их существования. При этом любая опасность может привести к экономическим потерям, что подтверждается большим числом публикаций на эту тему. Поэтому важной составляющей безопасности выступает защита экономических интересов личности, общества, государства, что подчеркивает экономический характер безопасности [2].

В зону экономических интересов государства входит также стабильное функционирование организаций и отраслей экономики. На уровне организаций принято рассматривать экономическую или корпоративную безопасность. Некоторые авторы, как Г.Б. Клейнер, экономическую безопасность определяют: «состояние данного хозяйственного субъекта, при котором жизненно важные компоненты структуры и деятельности предприятия характеризуются высокой степенью защищенности от нежелательных изменений» [3, p. 461–462].

Есикова Р.С. приводит данные, что около 80 % правонарушений в организации совершаются своими же работниками [4]. По данным Федеральной службы государственной статистики число дел об административных правонарушениях, возбужденных должностными лицами, существенно выросло, если в 2019 г. показатель составлял 1,9 млн дел, а в 2020 г – 1,2 млн дел, то уже в 2021 г. показатель увеличился до 3,9 млн дел., и в 2022 г. оставался высоким – 3,2 млн дел. Рост показателя за 2019–2022 гг. составил 68 %. При этом раскрываемость дел об административных правонарушениях существенно снизилась, что говорит о сложности дел, и подготовленности злоумышленников. Так раскрываемость дел об административных правонарушениях в 2019 г. составила 1,6 млн дел, в 2020 г. 1,0 млн дел, в 2021 г. 1,6 млн дел, в 2022 г. всего 1,1 млн дел [5]. Если уровень раскрываемости в 2019 г. составлял 80 %, то в 2022 г. он снизился до 34 %.

Данный факт определяет потребность руководства организаций защитить хозяйственную деятельность от вероятных потерь по вине человеческого фактора. Важный вывод заключается в том, что главным направлением экономической безопасности является кадровый аспект. Лейтон Д. определяет риски в кадровом аспекте: «компонент безопасности персонала часто упускается из виду и не рассматривается экспертами подробно» [6]. Среди рисков управления безопасностью персонала автор называет следующие: отсутствие отзывов для новых или переводимых сотрудников; отношение к проверке персональных данных; информационные риски: непонимание сотрудниками своих обязанностей и ролей; риск кражи, мошенничества или неправильного использования оборудования [6]. Следовательно, кадровая составляющая экономической безопасности определяется, как кадровая безопасность, требует оценки и анализа.

Ход исследования

Автор Есикова Р.С. определяет кадровую безопасность: – «процесс, предотвращающий негативные воздействия на экономическую безопасность предприятия за счет снижения рисков и угроз» [4]. В процессе формирования кадровой безопасности необходимо учитывать влияние внешних и внутренних угроз (рисунок 1). Организация кадровых процессов с учетом их результативности и снижения рисков в итоге будет способствовать повышению экономической безопасности организаций.

В последние годы в России можно наблюдать во многих организациях ускоренное внедрение различных информационных технологий. Можно предположить, что по мере распространения в промышленных и финансовых отраслях информационных (в том числе интеллектуальных) технологий экономические риски для потребителей будут значительно возрастать. Риски и угрозы связаны с нанесением вреда активам, в том числе информационной инфраструктуре (в том числе КИИ), кибератривам. Обеспечение безопасности промышленных и финансовых активов невозможно реализовать без наличия высоко квалифицированных специалистов. Так востребованность ИТ-специалистов будет только расти, вместе с ней и ответственность за сохранность данных, уязвимость информационных систем и технологий.

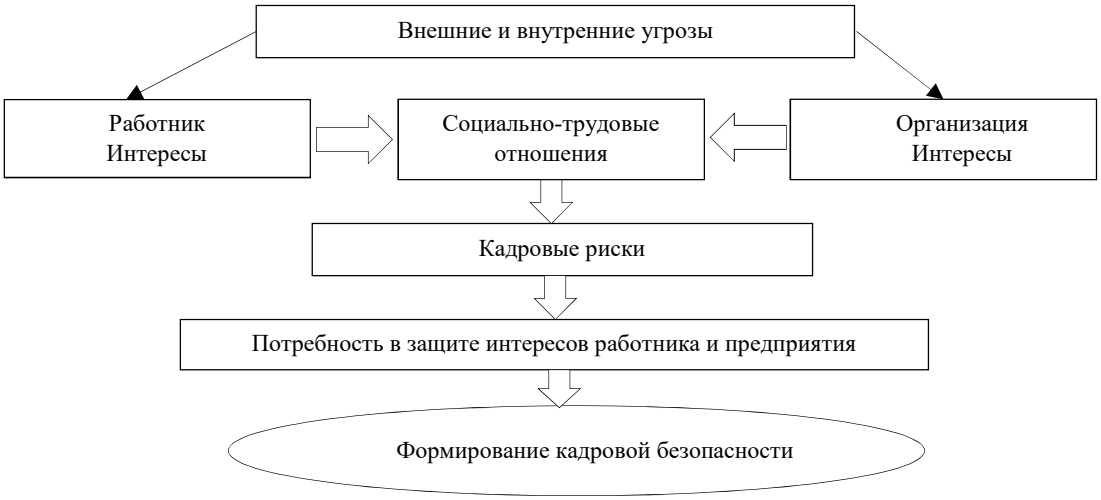

Рисунок 1 – Процесс формирования кадровой безопасности социально-трудовых отношений
Figure 1 – The process of formation of personnel security of social and labor relations

ИТ-компании должны обеспечить безопасность всех активов, в том числе киберкактивов и активов критической информационной инфраструктуры. Активы могут быть как «физическими» – маршрутизатор, сервер и другое, так и «логическими» – база данных, программное обеспечение и другое [7]. КИИ относится к активам, выведение из строя которой окажет пагубное воздействие на безопасность отрасли, национальную безопасность. В 2017 г. вступил в силу ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», где к объектам КИИ отнесены: «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры» [8]. В 2023 г. утверждены методические рекомендации по переходу на использование отечественного программного обеспечения на объектах КИИ, а также на объектах государственных и ведомственных информационных систем. Следовательно, спрос на ИТ-услуги повысится, а потребность в квалифицированных специалистах возрастет. В этой связи необходимо пересмотреть политику и процедуры по обеспечению кадровой безопасности в ИТ-отрасли.

Кадровая безопасность ИТ-компаний должна затрагивать направления оценки безопасности персонала и физической безопасности. Данный подход описывают Флик Т. и Морхаус Д. [9]. С точки зрения безопасности персонала, необходимо проводить: во-первых, регулярно информировать сотрудников об информационных угрозах, новых стандартах, требованиях, административной ответственности в профессиональной деятельности; во-вторых, направлять сотрудников на обучение по кибербезопасности; в-третьих, проводить оценку кадровых рисков (причинение ущерба организации) в отношении всех сотрудников, и особенно тех, которые имеют физический доступ к критической информационной инфраструктуре; в-четвертых, регулярно обновлять списки доступа к информационных системам. В результате в каждой ИТ-компании должны быть разработаны программы: по осведомленности персонала; по обучению персонала; по оценке кадровых рисков [9].

Для обеспечения кадровой безопасности обязательным условием является разработка и внедрение программы физической безопасности по защите информационной инфраструктуры. К мерам физической безопасности можно отнести такие, как идентификацию (в том числе биоиндентификацию) и контроль доступа ко всем объектам информационной инфраструктуры, возможно использование карточек-ключей, специальных замков, создание службы безопасности, сигнализации, наблюдения, и другое.

Формирование программы кадровой безопасности ИТ-компаний следует начать с оценки ее уровня. Для этого создается модель из количественных и качественных показателей. В оценке кадровой безопасности применяются различные методы: интегральный метод, метод индикаторов, эталонный метод, средневзвешенных величин, балльный метод.

В зависимости от целей организации определяется система показателей кадровой безопасности. Можно отметить, что авторы предлагают различные показатели в качестве основных. Сергее А.А. определил в качестве главного показателя кадровой безопасности произведение отклонений производительности труда и рентабельности деятельности, формула (1) [10].

$$Q = \sqrt{\Delta\alpha \cdot \Delta\beta}, \quad (1)$$

где Q – произведение отклонения результирующих показателей; $\Delta\alpha \cdot \Delta\beta$ – произведение относительных отклонений производительности труда и рентабельности деятельности, факта от плана [10].

Романова Ю.А. к показателям кадровой безопасности относит: производительность труда; коэффициент использования рабочего времени; рентабельность персонала [11].

Изученные теоретические и методологические аспекты оценки кадровой безопасности позволили определить ее компоненты: интеллектуальные (количество обученных); эффективность персонала; динамика и движение персонала; физическая безопасность; мотивация персонала. Составлена интегральная модель, формула (2).

$$F = f(i_n). \quad (2)$$

В настоящее время ИТ-отрасль в России бурно развивается. Аналитический центр TAdviser назвал крупные ИТ-компании: Ростех, Группа Т1, OCS, Ростелеком, МТС Диджитал, ИКС Холдинг, Huawei и другие [12].

Проведена оценка кадровой безопасности одной из ИТ-компаний (рисунок 2).

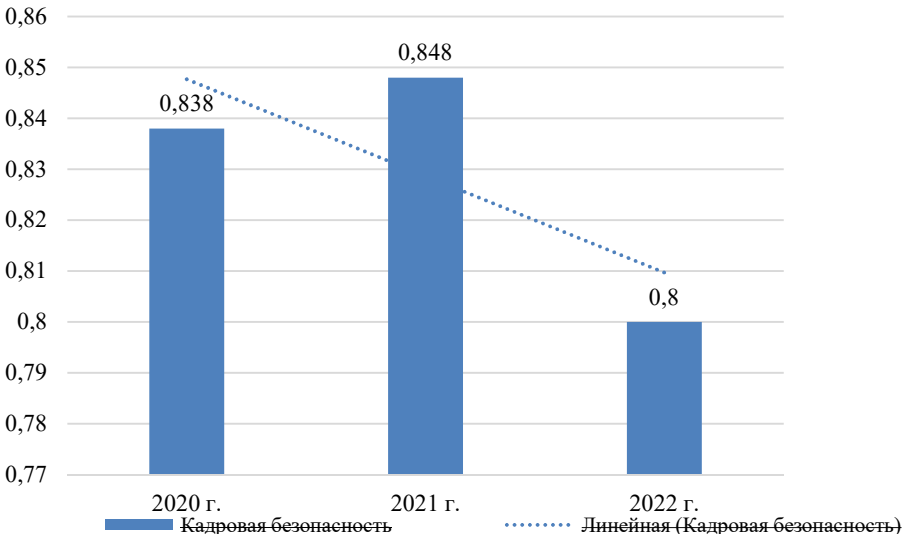

Рисунок 2 – Уровень кадровой безопасности ИТ-компании
Figure 2 – The level of personnel security of an IT company

Уровень кадровой безопасности ИТ-компании составил 80 %, и он определяется как высокий. Но наблюдается более низкий уровень по следующим компонентам: эффективность труда; физическая безопасность (см. таблицу).

Снижение эффективности труда связано с нехваткой трудовых ресурсов, предназначенных для реализации творческих и инновационных инициатив, что существенно сокращает качество и количество разработанных и внедренных новых востребованных продуктов на рынке ИТ-услуг. Снижение физической безопасности связано с уязвимостью информационной инфраструктуры, которая подвер-

гается воздействию из вне, в том числе по вине своих сотрудников – утечка конфиденциальной информации, информационный шпионаж.

В качестве основных мер обеспечения кадровой безопасности должны стать следующие: повышение ответственности сотрудников за разглашение информации; информирование сотрудников о мерах киберзащиты; обучение (в том числе тренинги) сотрудников с целью повышения их квалификации; раннее воспитание и подготовка молодежи для реализации творческих и инновационных инициатив в ИТ-сфере.

Таблица – Оценка кадровой безопасности по группам показателей
Table – Assessment of personnel security by groups of indicators

Группы показателей кадровой безопасности	2020 г.	2021 г.	2022 г.
Интеллектуальная группа (обучение персонала)	0,85	0,90	1
Эффективность труда	0,96	0,44	0,57
Движение персонала	0,76	0,99	0,79
Физическая безопасность	0,78	0,95	0,68
Мотивация персонала	0,84	0,96	0,96

ИТ-отрасль в России быстро развивается, что подтверждается следующими данными: за год рынок вакансий ИТ-специалистов увеличился на 18 %; но ожидается дальнейший рост занятости в ИТ-отрасли с 384 тыс. человек в 2021 г. до 420 тыс. человек к 2025 г. Но для реализации планов по распространению и внедрению отечественных информационных продуктов в России этого явно не достаточно. Так занятость в отдельных странах мира в ИТ-сфере составляет в США в 2021 г. 4,6 млн. человек, а к 2025 г. рост планируется до 5,8 млн. человек [13].

Заключение

Развитие ИТ-отрасли необходимо начать с подготовки будущих кадров в школах и усилить обучение в высших учебных заведениях, чтобы выпускники стали фундаментом развития информационной сферы в России. Для этого образование должно быть полным, глубоким, современным. Работающим ИТ-специалистам необходимо предложить программу обучения и повышения квалификации на базе высших учебный заведений.

В обеспечении кадровой безопасности ИТ-компаний ведущую роль должен занять высоко квалифицированный специалист, который способен создавать российское ПО и обеспечивать защищенность информационной инфраструктуры, в том числе КИИ. Только в этом случае Россия сможет занять лидирующую позицию на международном ИТ-рынке.

Библиографический список

1. Нормативно-правовой акт. О безопасности: Федеральный закон от 28.12.2010 № 390-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_108546/247e2ca8fe0f9d1d821eae037dd70806804b0d3c.

2. Нормативно-правовой акт. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400. URL: https://www.consultant.ru/document/cons_doc_LAW_389271.

3. Клейнер Г.Б. Информационная теория факторов управления экономическими организациями // Российский журнал менеджмента. 2022. № 20. С. 461–481. DOI: https://doi .org/10 .21638/spbu18 .2022.401.

4. Есикова Р.С. Кадровая безопасность в системе экономической безопасности // Научные труды Кубанского государственного технологического университета. 2018. № 6. С. 642–651. URL: https:// ntk.kubstu.ru/data/mc/0054/2218.pdf.

5. Административные правонарушения в сфере экономики // Федеральная служба государственной статистики. URL: https://rosstat.gov.ru/pravo.

6. Leighton J. Security Controls Evaluation, Testing, and Assessment Handbook (Second Edition). Academic Press. 2020, pp. 471–536. DOI: https://doi.org/10.1016/B978-0-12-818427-1.00011-2.

7. Knapp E.D., Langill J.T. Industrial Network Security (Second Edition). Syngress. 2015, pp. 9–40. DOI: https://doi.org/10.1016/B978-0-12-420114-9.00002-2.

8. Нормативно-правовой акт. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017. № 187-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_220885.

9. Flick T., Morehouse J. Securing the Smart Grid. Syngress, 2011. P. 85–108. DOI: https://doi.org/10.1016/B978-1-59749-570-7.00006-6.

10. Сергеев А.А. Экономическая безопасность предприятия: учебник и практикум для вузов / А.А. Сергеев. 3-е изд. Москва: Юрайт, 2023. 275 с.

11. Романова Ю.А. Анализ и оценка кадровой составляющей экономической безопасности предприятия // Экономический журнал. 2019. № 4 (56). С. 40–50. DOI: 10.24411/2072-8220-2019-00029.

12. Ранкинг TAdviser100: Крупнейшие ИТ-компании в России 2023 // TADVISER. Государство. Бизнес. Технологии. URL: https://www.tadviser.ru/index.php/Статья:Ранкинг_TAdviser100:_Крупнейшие_ИТ-компании_в_России_2023_.

13. Еще не Кремниевая долина, что тормозит развитие ИТ в России: образование // РБК. Тренды. 2021. URL: https://trends.rbc.ru/trends/education/60df13589a794747177dccc5.

References

1. Regulatory legal act. On safety: Federal Law No. 390-FZ of December 28, 2010. URL: https://www.consultant.ru/document/cons_doc_LAW_108546/247e2ca8fe0f9d1d821eae037dd70806804b0d3c. (In Russ.)

2. Regulatory legal act. On the National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation No. 400 dated 02.07.2021. URL: https://www.consultant.ru/document/cons_doc_LAW_389271. (In Russ.)

3. Kleiner G.B. Information theory of management factors of economic organizations. *Russian Journal of Management*, 2022, no. 20, pp. 461–481. DOI: https://doi .org/10 .21638/spbu18 .2022.401. (In Russ.)

4. Yesikova R.S. Personnel security in the system of economic security. *Scientific works of the Kuban State Technological University*, 2018, no. 6, pp. 642–651. URL: https://ntk.kubstu.ru/data/mc/0054/2218.pdf. (In Russ.)

5. Administrative offenses in the field of economics // Federal State Statistics Service. URL: https://rosstat.gov.ru/pravo. (In Russ.)

6. Leighton J. Security Controls Evaluation, Testing, and Assessment Handbook (Second Edition). Academic Press. 2020, pp. 471–536. DOI: https://doi.org/10.1016/B978-0-12-818427-1.00011-2.

7. Knapp E.D., Langill J.T. Industrial Network Security (Second Edition). Syngress. 2015, pp. 9–40. DOI: https://doi.org/10.1016/B978-0-12-420114-9.00002-2.

8. Regulatory legal act. On the security of the critical Information infrastructure of the Russian Federation: Federal Law No. 187-FZ of 26.07.2017. URL: https://www.consultant.ru/document/cons_doc_LAW_220885. (In Russ.)

9. Flick T., Morehouse J. Securing the Smart Grid. Syngress, 2011, pp. 85-108. DOI: https://doi.org/10.1016/B978-1-59749-570-7.00006-6.

10. Sergeev A.A. Economic security of the enterprise: textbook and workshop for universities. A.A. Sergeev (ed.). 3rd ed. Moscow: Yurayt Publishing House, 2023, 275 p. (In Russ.)

11. Romanova Yu.A. Analysis and evaluation of the personnel component of the economic security of the enterprise. *Economic Journal*, 2019, no. 4 (56), pp. 40–50. DOI: 10.24411/2072-8220-2019-00029. (In Russ.)

12. Ranking TAdviser100: The largest IT companies in Russia 2023. *TADVISER. State. Business. Technologies*. URL: https://www.tadviser.ru/index.php/Статья:Ranking_TAdviser100:_collar_it-company_b_Russia_2023_. (In Russ.)

13. Not yet Silicon Valley, which slows down the development of IT in Russia: education. *RBC. Trends*, 2021. URL: https://trends.rbc.ru/trends/education/60df13589a794747177dccc5. (In Russ.)