

А. В. Галлямова¹✉, В. М. Белов¹

Содержание блока психофизических характеристик специалиста в области информационной безопасности

¹ Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: allna.black@yandex.ru

Аннотация. В данной статье рассматривается проблема систематизации психофизических характеристик специалиста в области информационной безопасности (далее – ИБ) как основы для формирования базы знаний искусственного интеллекта (далее – ИИ), которая в свою очередь, сможет оказывать помощь в кадровых вопросах. На основании анализа международных нормативных документов, нормативных документов Российской Федерации, моделей компетенций, а также научной литературы по психологии труда и инженерной психологии определено содержание блока психофизических характеристик, которые могут относиться к профессиональной деятельности в сфере ИБ. Предложена многоуровневая структура блока, включающая когнитивные, личностные, психофизиологические и мотивационно-ценностные компоненты. Выделены профили для основных ролевых категорий согласно таксономии NICE Workforce Framework (National Initiative for Cybersecurity Education Workforce Framework). Результаты могут быть использованы при разработке онтологий предметной области и инструментов для автоматизированной оценки профессиональной пригодности.

Ключевые слова: информационная безопасность, человеческий фактор, психофизические характеристики, профессионально важные качества, база знаний, NICE Framework, психограмма специалиста информационной безопасности

A. V. Gallyamova¹✉, V. M. Belov

Contents of a Set of Psychophysical Characteristics of an Information Security Specialist

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: allna.black@yandex.ru

Abstract. This article examines the problem of systematizing the psychophysical characteristics of an information security (IS) specialist as a basis for developing an artificial intelligence (AI) knowledge base, which in turn can assist in personnel matters. Based on an analysis of international regulatory documents, Russian Federation regulations, competency models, and scientific literature on occupational psychology and engineering psychology, the content of a set of psychophysical characteristics that may be relevant to professional activity in IS is determined. A multi-level structure is proposed for this set, including cognitive, personality, psychophysiological, and motivational-value components. Profiles for key role categories were identified according to the NICE Workforce Framework (National Initiative for Cybersecurity Education Workforce Framework) taxonomy. The results can be used in the development of domain ontologies and tools for automated assessment of professional suitability.

Keywords: information security, human factors, psychophysical characteristics, professionally important qualities, knowledge base, NICE Framework, information security specialist psychogram

Введение

Современная концепция информационной безопасности акцентирует внимание не только на технических средствах, но и на роли человека, многочисленные исследования, в том числе отчеты аналитических компаний и государственных регуляторов, в сфере информационной безопасности, свидетельствуют о том, что множество инцидентов в области ИБ прямо или косвенно обусловлены действиями, бездействием, либо психологической уязвимостью персонала [1, 2], в связи с этим становится актуальной задача научно обоснованного определения требований к психофизическим характеристикам специалистов, деятельность которых непосредственно связана с обеспечением конфиденциальности, целостности и доступности информации.

В Российской и зарубежной практике существуют разносторонние подходы к описанию компетенций специалиста по ИБ, отраженные в профессиональных стандартах, квалификационных требованиях и отраслевых руководствах [3–5], однако в большинстве из них психофизический аспект отсутствует вовсе, либо представлен в обтекаемой и неконкретной форме. Это создает серьезную проблему при попытке построения интеллектуальных систем, в частности баз знаний, ориентированных на поддержку кадрового отбора, оценки и развития персонала в области ИБ [16].

Целью данной статьи является определение и структурирование содержания блока психофизических характеристик специалиста в области информационной безопасности, руководствуясь совокупностью нормативных, теоретических и эмпирических источников. Достижение данной цели позволит в дальнейшем выстраивать соответствующие знания в виде онтологии предметной области, пригодной для использования в системах искусственного интеллекта.

Методы и методики

Методологическая основа исследования состоит из системного анализа научной литературы и нормативно-технической документации в трех пересекающихся предметных областях: психология труда и инженерная психология, информационная безопасность и управление персоналом.

В качестве нормативной базы были использованы следующие документы:

NIST Special Publication 800-181 (NICE Workforce Framework) – наиболее полная на сегодняшний день таксономия рабочих ролей в области ИБ, содержащая детализированные перечни знаний, умений и способностей (KSAs) для каждой роли [3];

профессиональные стандарты Российской Федерации, утвержденные Министерством труда и социальной защиты: «Специалист по информационной безопасности», «Аналитик информационной безопасности», «Аудитор в области информационной безопасности» [4];

– руководящие документы ФСТЭК России и ФСБ России в части требований к персоналу, осуществляющему функции по обеспечению ИБ [5];

– ISO/IEC 27001:2022 и сопутствующие стандарты серии 27000 в части требований к компетентности персонала, вовлеченного в систему менеджмента информационной безопасности.

Теоретический анализ опирался на фундаментальные труды в области психологии профессиональной пригодности [6, 7], психодиагностики функциональных состояний [8], а также классические работы по эргономике и человеческому фактору [9]. Особое внимание уделялось источникам, раскрывающим специфику уязвимостей человеческого сознания в контексте социальной инженерии [10], поскольку они позволяют выявить качества, необходимые для предотвращения сопутствующих угроз безопасности информации.

Методика исследования включала контент-анализ требований к персоналу, зафиксированных в вышеперечисленных документах, с последующим распределением выявленных дескрипторов в категории, соответствующие традиционной структуре психограммы: когнитивные процессы, личностные черты, психофизиологические характеристики, мотивационно-ценностные ориентации. Для каждой ролевой категории, выделенной в NICE Workforce Framework, был составлен профиль соответствующих характеристик с учетом специфики выполняемых задач.

Результаты

Проведенный анализ позволил выделить основную структуру психофизических характеристик, значимых для большинства ролей в области ИБ, а также специфические требования, относящихся к разным функциональным категориям.

1. Основная структура психофизических характеристик специалиста по ИБ **Когнитивный блок:**

– аналитическое и дедуктивное мышление – способность выявлять закономерности при работе с большим объемом информации, строить причинно-следственные связи, видеть систему в целом. Для аналитиков угроз данная характеристика является критической, поскольку напрямую влияет на способность распознавания и выявления подозрительных событий ИБ;

– критичность мышления – умение быстро и эффективно обдумывать поступающую информацию, соотносить правдоподобность источников, распознавать попытки манипуляции и социальной инженерии. Можно отметить, что данное качество особенно актуально, так как атаки, эксплуатирующие доверчивость и когнитивные искажения, являются наиболее эффективными, основным примером этого можно считать работы Митника и Хэднаги [10];

– внимание (концентрация, устойчивость, переключаемость) – способность длительное время уметь концентрироваться на однотипной и монотонной деятельности (например, мониторинг событий безопасности), а также быстро переключаться между задачами при возникновении инцидента ИБ. Стандарт NIST SP

800-63, описывающий процедуры аутентификации, косвенно предполагает высокий уровень внимательности при работе с учетными данными [3];

- рабочая память и скорость обработки информации – необходимы для оперативного принятия решений в условиях максимальной срочности, характерного для реагирования на инциденты ИБ.

Личностный блок (черты, близкие к конструктам «Большой пятерки»):

- добросовестность – организованность, дисциплинированность, следование определенным правилам и регламентам. Требования ФСТЭК России и ФСБ России к работе с государственной тайной косвенно склоняются именно к этому качеству, подобно и другим стандартам, регулирующим требования к защите информации;

- эмоциональная стабильность (противоположный полюс — нейротизм) – устойчивость к стрессу, способность сохранять спокойствие в критических ситуациях (инциденты ИБ, давление со стороны злоумышленников при социотехнических атаках). Методология оценки функциональных состояний, разработанная А.Б. Леоновой [8], предоставляет способы для диагностики этого параметра;

- интернальный локус контроля (ответственность) – склонность приписывать ответственность за результаты деятельности собственным действиям, а не внешним обстоятельствам;

- бдительность и умеренная подозрительность к обстоятельствам – данное качество не является патологической паранойей, а профессионально обусловленная настороженность, готовность к обнаружению подозрительных событий в поведении пользователей и систем.

Психофизиологический блок:

- стрессоустойчивость – способность организма выдерживать длительные когнитивные и эмоциональные нагрузки без особого снижения эффективности осуществляемой деятельности. Например, для операторов центров мониторинга (SOC) характерна высокая когнитивная нагрузка, что требует особого внимания к данному параметру;

- работоспособность в условиях тяжелого режима работы, недостаток сна и большое количество монотонной работы, все это также относится к посменной работы в режиме 24/7 центра мониторинга.

Мотивационно-ценностный блок:

- профессиональная этика и лояльность – соответствие моральным нормам ИБ-сообщества, осознание социальной ответственности. Работы Е.А. Климова по профессиональному самоопределению [11] позволяют определить концепцию этого компонента как интегральную характеристику личности специалиста;

- мотивация достижения в сочетании с соблюдением правил — баланс между инициативностью и строгим следованием установленным правилам и регламентам.

2. Распределение характеристик по ролевым категориям (на основе NICE Workforce Framework)

Анализ KSAs (Knowledge, Skills, and Abilities), приведенных в NICE Workforce Framework, показывает, что для разных ролей принцип значимости отдельно взятых характеристик существенно отличается. В таблице 1 представлены профили для трех обширных категорий.

Таблица 1 – Приоритетные психофизические характеристики для различных ролей в области ИБ

Категория ролей (NICE)	Примеры ролей	Ключевые когнитивные характеристики	Ключевые личностные черты
Анализ и расследование (AN)	Threat/Warning Analyst, Cyber Defense Analyst	Аналитическое мышление, индуктивное/дедуктивное мышление, рабочая память, способность к построению гипотез	Открытость опыту (любопытность), настойчивость, бдительность
Эксплуатация и поддержка (OM)	System Administrator, Database Administrator	Внимание к деталям, процедурная память, способность к многозадачности	Добросовестность, дисциплинированность, методичность
Надзор и управление (OV)	Executive Cyber Leader, Program Manager	Стратегическое мышление, вербальный интеллект, способность оценивать риски	Эмоциональная стабильность, интернальный локус контроля, развитые коммуникативные навыки

3. Сопоставление с профессиональными стандартами Российской Федерации

Сравнительный анализ с профессиональными стандартами Российской Федерации [4] выявил высокую степень соответствия с описанными выше характеристиками, однако с некоторой спецификой. В отечественных документах больший акцент делается на нормативно-правовой компетентности и, косвенно, на качествах, связанных с добросовестностью и ответственностью, обусловленными требованиями законодательства о государственной тайне. Кроме того, требования ФСБ России [5] предполагают углубленную проверку биографических данных и психологическое тестирование, направленное на выявление склонности к негативному поведению.

Обсуждение

Полученная структура блока психофизических характеристик представляет собой совокупность требований, извлеченных из разных источников. Ее научная актуальность заключается в переходе от распространенных неоднозначных описаний к систематизированной модели, которая может быть в дальнейшем формализована в виде онтологии предметной области. Как отмечают Гаврилова Т.А. и Хорошевский В.Ф. [12], именно такая структура знаний является необходимым условием для построения эффективных баз знаний интеллектуальных систем.

Предложенный подход также позволяет решить проблему неоднозначной оценки: каждая характеристика должна быть проанализирована через психодиагностические методики (опросник 16PF Кеттелла, ММРІ, тест структуры интеллекта Амтхауэра, корректурная проба Бурдона и др.), что обеспечит объективность и точность результатов. Важно подчеркнуть, что использование данных методик в составе системы ИИ должно строго соответствовать требованиям Федерального закона № 152-ФЗ «О персональных данных», особенно в части обработки специальных категорий персональных данных [17].

Ограничением настоящего исследования является его преимущественно теоретико-аналитический характер. Апробация предложенной модели требует проведения тщательных исследований, направленных на установление связи между выделенными характеристиками и объективными показателями успешности профессиональной деятельности (отсутствие инцидентов ИБ из-за ошибки специалиста, скорость и качество решения профессиональных задач).

Заключение

В результате проведенного исследования определено и структурировано содержание блока психофизических характеристик специалиста в области ИБ. Блок включает следующую структуру (когнитивные способности, личностные черты, психофизиологические показатели, мотивационно-ценностные ориентации), а также вариативную часть, распределенную по ролевым категориям в соответствии с международными и профессиональными стандартами Российской Федерации.

Практическая значимость полученных результатов состоит в возможности их использования в качестве основы для:

- разработки онтологической модели предметной области «Психофизический портрет специалиста по ИБ»;
- проектирования базы знаний интеллектуальной системы поддержки принятия кадровых решений;
- создания методических рекомендаций по профессиональному психологическому отбору и оценке персонала в сфере ИБ.

Дальнейшие исследования будут направлены на упорядочение модели на языке представления онтологий (OWL) и ее интеграцию с существующими таксономиями компетенций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. – Wiley, 2018. – 320 p.
2. Mitnick K.D., Simon W.L. The Art of Deception: Controlling the Human Element of Security. – Wiley, 2002. – 368 p.
3. NIST Special Publication 800-181 Rev. 1. Workforce Framework for Cybersecurity (NICE Framework). – National Institute of Standards and Technology, 2020.
4. Профессиональный стандарт «Специалист по информационной безопасности» (утв. приказом Минтруда России от 15.09.2016 № 522н).

5. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений (утв. приказом ФСТЭК России от 11.04.2025 № 117).
6. Бодров В.А. Психология профессиональной пригодности: учеб. пособие для вузов. – М.: ПЕР СЭ, 2001. – 511 с.
7. Дружинин В.Н. Психология общих способностей: учебник для вузов. – 3-е изд. – М.: Юрайт, 2025. – 349 с.
8. Леонова А.Б. Психодиагностика функциональных состояний человека. – М.: Изд-во Моск. ун-та, 1984. – 200 с.
9. Человеческий фактор: в 6 т. Т. 1. Эргономика – комплексная научно-техническая дисциплина / под ред. Г. Салвенди. – М.: Мир, 1991. – 599 с.
10. Mitnick K.D., Vamosi R. The Art of Invisibility. – Little, Brown and Company, 2017. – 320 p.
11. Климов Е.А. Психология профессионального самоопределения: учеб. пособие. – 4-е изд. – М.: Академия, 2010. – 304 с.
12. Гаврилова Т.А., Хорошевский В.Ф. Базы знаний интеллектуальных систем. – СПб.: Питер, 2001. – 384 с.
13. Анастаси А., Урбина С. Психологическое тестирование. – 7-е изд. – СПб.: Питер, 2009. – 688 с.
14. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
15. Gruber T.R. Toward principles for the design of ontologies used for knowledge sharing // International Journal of Human-Computer Studies. – 1995. – Vol. 43, № 5-6. – P. 907–928.
16. Рассел С., Норвиг П. Искусственный интеллект: современный подход. – 2-е изд. – М.: Вильямс, 2006. – 1408 с.
17. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 08.08.2024).

© А. В. Галлямова, В. А. Белов, 2026