УДК *004.056.5:331.108(476)*

КАДРОВЫЙ ПОТЕНЦИАЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

М.Д. Юров, В.В. Чижик
Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается кадровый потенциал в сфере информационной безопасности Республики Беларусь в контексте формирования национальной системы обеспечения кибербезопасности. Проанализированы нормативно-правовые акты 2023–2025 гг., определяющие создание центров кибербезопасности и минимальную потребность в специалистах для их функционирования. Оценены возможности системы высшего образования по подготовке кадров в области информационной безопасности. Сопоставлены потребности и выпуск специалистов, что позволило определить степень обеспеченности отрасли квалифицированными кадрами и выявить существующие проблемы.

Ключевые слова: информационная безопасность; кибербезопасность; кадровый потенциал; подготовка специалистов; центры кибербезопасности; нормативно-правовые акты; кадровая потребность; критически важные объекты информатизации; национальная система кибербезопасности; система высшего образования.

HUMAN RESOURCE POTENTIAL IN THE FIELD OF INFORMATION SECURITY IN THE REPUBLIC OF BELARUS

M. Yurau, V. Chizhik
Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", Minsk, Republic of Belarus

Abstract. The article examines the human resource potential in the field of information security in the Republic of Belarus within the framework of the development of the national cybersecurity system. The analysis covers regulatory acts adopted in 2023–2025 that define the establishment of cybersecurity centers and the minimum staffing requirements for their operation. The study assesses the capacity of the higher education system to train information security specialists. Compared the estimated personnel demand with the number of graduates, evaluated the sector's staffing sufficiency and identify existing issues.

Keywords: information security; cybersecurity; human resources; specialist training; cybersecurity centers; regulatory framework; staffing needs; critical information infrastructure; national cybersecurity system; higher education system.

Введение

Цифровая трансформация экономики и системы государственного управления Республики Беларусь обусловливает необходимость комплексного переосмысления подходов к обеспечению информационной безопасности как неотъемлемой составляющей национальной безопасности. В условиях расширения цифровой инфраструктуры, роста объемов обрабатываемых данных и усложнения киберугроз возрастает значимость формирования институциональных механизмов защиты информационного пространства государства.

Принятие Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности», а также последующих нормативных правовых актов, регламентирующих порядок его реализации, сформировало нормативно-правовую основу для построения национальной системы обеспечения кибербезопасности. Одним из ключевых структурных элементов данной системы выступают центры обеспечения кибербезопасности и реагирования на киберинциденты, создаваемые на объектах информационной инфраструктуры государственных органов и иных организаций (далее — центры кибербезопасности). Их деятельность направлена на мониторинг, предупреждение, выявление и нейтрализацию киберугроз, что обеспечивает повышение устойчивости национального цифрового пространства [1].

Основная часть

Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» установил, что 27 владельцев критически важных объектов информатизации, а также уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты, обеспечивают создание центров кибербезопасности [1].

Постановление Совета Министров Республики Беларусь от 23 февраля 2024 г. № 120 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» определило перечень из 124 государственных органов и иных организаций, которые создают центры кибербезопасности и (или) приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры [1].

Постановление Совета Министров Республики Беларусь от 28 марта 2025 г. № 185 «Об изменении постановлений Совета Министров Республики Беларусь от 12 декабря 2023 г. № 879 и от 23 февраля 2024 г. № 120» определило перечень из 202 государственных органов и иных организаций, которые создают центры кибербезопасности и (или)

приобретают услуги по обеспечению кибербезопасности у организаций, создавших такие центры [1].

Поскольку в общедоступных источниках есть только перечень из 33 аттестованных центров кибербезопасности, а информация по количеству неаттестованных центров кибербезопасности, как и по количеству сотрудников в них отсутствует, то предположим, что все организации в установленный срок создали центры кибербезопасности с минимальной численностью для прохождения аттестации, равной 11 штатным единицам, включая руководителя [2, 3]. На основании всего вышеперечисленного можно рассчитать минимальную кадровую потребность всех центров кибербезопасности за 2023-2025 гг., но без учета сотрудников Национального центра обеспечения кибербезопасности и реагирования на киберинциденты.

Таким образом, после проведения всех расчетов, получаем, что в 2023 году для обеспечения работы 27 центров кибербезопасности минимально требовалось 297 сотрудников, в 2024 году требовалось минимум 1364 сотрудника в 124 центра кибербезопасности, а в 2025 году требовалось минимум 2222 сотрудника для 202 центров кибербезопасности.

Теперь, когда мы установили минимальную кадровую потребность за 2023-2025 гг., необходимо выяснить достаточно ли специалистов готовят в учреждениях образования. На основании всего вышеперечисленного можно рассчитать максимально возможное количество специалистов, которые готовит система высшего образования за 2023–2025 гг. Важно отметить, что в данных расчетах не учитываются образовательные программы магистратуры, аспирантуры и докторантуры, поскольку в общедоступных источниках нет информации о планах приема за 2023-2025 гг.

После проведения всех расчетов, получаем, что в 2023 году на специальности бакалавриата по информационной безопасности готовили 409 бакалавров, из которых 293 обучались на бюджетной форме обучения, а 116 обучались на платной форме обучения, в 2024 году готовили 497 бакалавров, из которых 333 обучались на бюджетной форме обучения, а 164 обучались на платной форме обучения, в 2025 году готовили 409 бакалавров, из которых 277 обучались на бюджетной форме обучения, а 132 обучались на платной форме обучения [4].

Стоит упомянуть, что для более достоверных расчетов необходимо учитывать дополнительные факторы: текучесть кадров в сфере информационной безопасности, уход выпускников в другие сферы, трудоустройство сотрудников с непрофильным образованием, рост числа центров кибербезопасности в будущем и т.д.

Заключение

Проведенный анализ показал, что формирование национальной системы обеспечения кибербезопасности в Республике Беларусь сопровождается стремительным ростом потребности в квалифицированных кадрах. Минимальная кадровая потребность центров кибербезопасности увеличилась с 297 человек в 2023 году до 2222 человек в 2025 году, что соответствует среднегодовому темпу роста более 140 %. В то же время возможности системы высшего образования остаются ограниченными: ежегодный выпуск бакалавров по направлениям, связанными с информационной безопасностью колеблется в пределах 409–497 человек и не демонстрирует устойчивой тенденции к росту.

Сопоставление спроса и предложения свидетельствует о формировании значительного дефицита кадров, который в 2024–2025 гг. достиг 867 и 1813 человек соответственно. Коэффициент обеспеченности отрасли специалистами снизился до критического уровня – 18 % в 2025 году. Прогноз на 2026 год показывает дальнейшее увеличение дефицита при сохранении текущих тенденций.

Таким образом, существующая система подготовки кадров не обеспечивает потребности национальной системы кибербезопасности, что создает риски для устойчивого функционирования критически важной информационной инфраструктуры и реализации государственной политики в области информационной безопасности.

Список использованных источников

1. Национальный правовой Интернет-портал Республики Беларусь : [сайт]. – Мн., 2003–2026. – https://pravo.by/ (дата обращения: 21.03.2026).

2. Перечень аттестованных центров кибербезопасности // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: https://www.oac.gov.by/cybersecurity-centers-list/activity/certified-cybersecurity-centers (дата обращения: 21.03.2026).

3. Рекомендации для создаваемых центров кибербезопасности // Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: https://www.oac.gov.by/activity/cybersecurity-centers-list/recommendations-for-cybersecurity-centers (дата обращения: 21.03.2026).

4. ИТ-абитуриент // Парк высоких технологий. – Мн., 2005–2026. – URL: https://park.by/education/graduate/ (дата обращения: 21.03.2026).

References

1. National Legal Internet Portal of the Republic of Belarus: [website]. – Minsk, 2003–2026. – https://pravo.by/ (date of access: 21.03.2026).

2. List of certified cybersecurity centers // Operations and Analysis Center under the President of the Republic of Belarus. – URL: https://www.oac.gov.by/cybersecurity-centers-list/activity/certified-cybersecurity-centers (date of access: 21.03.2026).

3. Recommendations for the creation of cybersecurity centers // Operations and Analysis Center under the President of the Republic of Belarus. – URL: https://www.oac.gov.by/activity/cybersecurity-centers-list/recommendations-for-cybersecurity-centers (date of access: 21.03.2026).

4. IT applicant // Hi-Tech Park. – Minsk, 2005–2026. – URL: https://park.by/education/graduate/ (date of access: 21.03.2026).

Сведения об авторах

Юров М.Д., студент экономического факультета специальности «Управление информационными ресурсами», Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», maksimyurauscience@gmail.com.

Чижик В.В., старший преподаватель кафедры информационных технологий, Учреждение образования Федерации профсоюзов Беларуси «Международный университет «МИТСО», nest101999@mail.ru.

Information about the authors

Yurau M., student of the Faculty of Economics specialty "Information resources management", Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", maksimyurauscience@gmail.com.

Chizhik V., Senior Lecturer at the Department of Information Technology, Higher Educational Establishment of the Federation of Trade Unions of Belarus "International University "MITSO", nest101999@mail.ru.