УДК 004.056

ЗНАЧЕНИЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

А. О. Лущай

Учреждение образования «Брестский государственный технический университет», Республика Беларусь

Научный руководитель А. К. Крамаренко

Рассмотрены ключевые аспекты значения подготовки специалистов в области кибербезопасности для промышленных предприятий. Отмечены основные угрозы, особенности защиты операционных технологий и дефицит кадров. Приведены данные по ситуации в Беларуси и даны рекомендации по развитию профильного образования.

Ключевые слова: кибербезопасность, промышленность, информационная безопасность, подготовка кадров.

THE IMPORTANCE OF TRAINING CYBERSECURITY SPECIALISTS FOR INDUSTRIAL ENTERPRISES

A. O. Lushchai

Brest State Technical University, Republic of Belarus

Scientific supervisor A. K. Kramarenko

The article examines key aspects of the importance of training specialists in the field of cybersecurity for industrial enterprises. It considers the main threats, features of protecting operational technologies and personnel shortages. It provides data on the situation in Belarus and gives recommendations for the development of specialized education.

Keywords: cybersecurity, industry, information security, personnel training.

Цифровизация промышленного сектора открывает новые горизонты для повышения эффективности, автоматизации и дистанционного управления производственными процессами. Однако одновременно с этим усиливается и киберугроза: промышленные предприятия становятся одной из главных целей кибератак. Учитывая важность бесперебойной работы производственных систем, обеспечение информационной безопасности (ИБ) становится приоритетной задачей. В этом контексте возрастает значимость подготовки квалифицированных специалистов по кибербезопасности, обладающих знаниями как в ИТ-сфере, так и в области промышленных процессов.

Цель данной работы – проанализировать значение подготовки таких специалистов и обозначить ключевые направления ее совершенствования.

Промышленные предприятия используют специальные автоматизированные системы, которые управляют оборудованием, процессами и производственными линиями. Эти технологии отличаются от обычных офисных компьютеров и требуют особого подхода к защите. На первом месте стоит не защита данных, а стабильная и безопасная работа оборудования. Оборудование работает годами и редко обновляется, что усложняет установку современных защитных решений. Любые изменения в системе безопасности нужно внедрять так, чтобы не нарушить производство

и не создать рисков для персонала. Поэтому специалисты в этой сфере должны не только разбираться в кибербезопасности, но и хорошо понимать, как устроены производственные процессы.

Современные угрозы становятся все более изощренными. К числу наиболее опасных относятся внедрение вредоносного ПО, способного нарушить работу оборудования, атаки на сетевые протоколы управления, кража данных о производственных процессах и технологиях, действия внутренних злоумышленников на предприятии. Последствия киберинцидентов в промышленности могут быть не только экономическими, но и физическими: аварии, пожары, угрозы для жизни персонала. Стоит сделать акцент на актуальности данной проблемы для нашей страны. В 2023 г. Беларусь вошла в топ-3 стран СНГ по количеству кибератак – на ее долю пришлось 7 % всех инцидентов. Особенно часто атакуются госсектор, промышленность и финансы. Всего за год зафиксировано около 20 000 киберпреступлений, что составляет 21 % всех преступлений в стране. По данным Kaspersky ICS CERT, вредоносные объекты были обнаружены на 40,1 % промышленных систем (АСУ), что превышает мировой средний уровень. На фоне этого ощущается нехватка специалистов по кибербезопасности.

В последние годы Беларусь сталкивается с нарастающей волной киберугроз, что особенно актуально для промышленных предприятий. Согласно данным компании Positive Technologies, в 2023–2024 гг. Беларусь заняла третье место среди стран СНГ по количеству кибератак, на ее долю пришлось 7 % всех зафиксированных инцидентов. Особенно уязвимыми оказались государственные учреждения (22 % атак), промышленный сектор (14 %) и финансовые организации (11 %). В целом, за 2023 г. в стране было совершено около 20 тыс. киберпреступлений, что составляет 21 % от общего числа преступлений в Беларуси. Промышленные предприятия Беларуси также находятся в зоне повышенного риска. По данным Kaspersky ICS CERT, во второй половине 2023 г. вредоносные объекты были заблокированы на 40,1 % компьютеров автоматизированных систем управления (АСУ) в стране. Это выше среднего мирового показателя, что свидетельствует о высокой уязвимости промышленных систем. Таким образом, для эффективной защиты промышленных предприятий Беларуси необходимо не только техническое укрепление инфраструктуры, но и системная подготовка специалистов, обладающих знаниями как в области информационных технологий, так и в специфике промышленных процессов. Это требует обновления образовательных программ, развития практических навыков и создания условий для непрерывного профессионального роста в сфере кибербезопасности.

Подготовленные специалисты по ИБ выполняют широкий спектр задач. Выявляют уязвимости и анализируют риски, проектируют и внедряют защитные решения с учетом специфики промышленного оборудования, осуществляют постоянный мониторинг состояния систем безопасности. На них лежит ответственность за реагирование на инциденты и восстановление после атак, обучение персонала безопасному обращению с ИТ средой. Особо важно, чтобы такие специалисты обладали междисциплинарными знаниями – сочетали техническую подготовку с пониманием производственной логики.

Во многих странах, включая Беларусь, остро ощущается нехватка квалифицированных специалистов, способных эффективно работать на пересечении информационных технологий и производственных процессов. Современные угрозы требуют от сотрудников не только знаний в области ИТ и кибербезопасности, но и глубокого понимания особенностей функционирования промышленных объектов, их технологических циклов, а также возможных последствий вмешательства в них. Однако

действующие учебные программы зачастую не учитывают эту специфику: в них недостаточно внимания уделяется реальным сценариям угроз в промышленной среде, особенностям операционных технологий, а также практическим навыкам работы с реальным оборудованием.

Тем не менее в последние годы наметилась положительная динамика. В ряде белорусских и зарубежных вузов появляются специализированные образовательные программы, ориентированные именно на подготовку специалистов по промышленной кибербезопасности. Создаются центры компетенций, где студенты получают доступ к лабораторным стендам, имитирующим работу реальных производственных систем. Развиваются программы корпоративного обучения: крупные промышленные компании начинают инвестировать в подготовку собственных ИБ-специалистов, адаптируя обучение под нужды конкретных отраслей.

Также в образовательную практику внедряются учебные тренажеры, моделирующие работу автоматизированных систем управления (например, SCADA), что позволяет будущим специалистам безопасно отрабатывать действия в условиях киберинцидентов. Все более востребованными становятся сертификационные курсы международного уровня (такие как Certified ICS Security Professional, Global Industrial Cyber Security Professional и др.), которые обеспечивают признание компетенций не только на национальном, но и на глобальном уровне.

Таким образом, несмотря на сохраняющийся кадровый дефицит, предпринимаемые шаги свидетельствуют о понимании проблемы на государственном и отраслевом уровнях и формируют задел для устойчивого развития системы подготовки кадров в сфере промышленной кибербезопасности. Кибербезопасность становится критически важным элементом устойчивого функционирования промышленных предприятий. Сложность современных производственных процессов, использование автоматизированных систем и растущая цифровизация создают дополнительные уязвимости, которые могут быть использованы злоумышленниками для нанесения значительного экономического и репутационного ущерба. Особенно актуальна эта проблема для Беларуси, где наблюдается рост числа кибератак на промышленный сектор при остром дефиците квалифицированных специалистов.

Анализ показал, что защита промышленных объектов требует особого подхода, учитывающего как технические особенности оборудования, так и производственные реалии. Обеспечение кибербезопасности в этой сфере невозможно без профессионалов, обладающих как знаниями в ИТ и безопасности, так и пониманием специфики производственных процессов.

Подготовка таких специалистов должна быть приоритетной задачей для системы образования. Необходимы актуализация учебных программ, развитие практико-ориентированных курсов, внедрение междисциплинарного подхода, а также взаимодействие учебных заведений с промышленными предприятиями. Только в условиях тесного сотрудничества между государством, бизнесом и образовательными учреждениями можно сформировать устойчивую систему подготовки кадров в области промышленной кибербезопасности.

Таким образом, инвестирование в обучение и развитие специалистов – это не просто мера защиты, а стратегический вклад в экономическую безопасность страны и ее технологическое развитие.

Литература

1. Крамаренко, А. К. Интеграция программного обеспечения в бизнес: процесс, проблемы и перспективы / А. К. Крамаренко, В. Н. Русенко // Репозиторий БрГТУ. – URL: https://rep.bstu.by/handle/data/46440 (дата обращения: 14.04.2025).

2. Национальный статистический комитет Республики Беларусь. – URL: http://belstat.gov.by/ (дата обращения: 14.04.2025).
3. ПВТ-2024: новые резиденты и стабильность экспорта. – URL: https://ibmedia.by/news/pvt-2024-novye-rezidenty-i-stabilnost-eksporta/ (дата обращения: 14.04.2025).
4. Дополнительное образование]. – URL: https://president.gov.by/ru/belarus/social/education/additional (дата обращения: 14.04.2025).
5. Digital and AI Readiness Assessment presented in Belarus. – URL: https://www.undp.org/belarus/news/digital-and-ai-readiness-assessment-presented-belarus (дата обращения: 14.04.2025).

УДК 331.5

СОТРУДНИЧЕСТВО МЕЖДУ ВУЗАМИ И ПРОМЫШЛЕННОСТЬЮ КАК ИНСТРУМЕНТ МОДЕРНИЗАЦИИ НАЦИОНАЛЬНОЙ ЭКОНОМИКИ

В. В. Якименко

Учреждение образования «Брестский государственный технический университет», Республика Беларусь

Научный руководитель А. К. Крамаренко

Рассмотрен институциональный потенциал кооперации между высшими учебными заведениями и промышленными предприятиями как одного из ключевых инструментов модернизации экономики Республики Беларусь. Особое внимание уделено анализу рассогласования интересов сторон, а также практическим примерам успешного взаимодействия.

Ключевые слова: университетско-промышленное сотрудничество, институциональный анализ, инновационная экономика, трансфер технологий, дуальное образование, модернизация.

COOPERATION BETWEEN UNIVERSITIES AND INDUSTRY AS A MECHANISM FOR NATIONAL ECONOMIC MODERNIZATION

V. V. Yakimenko

Brest State Technical University, Republic of Belarus

Scientific supervisor A. K. Kramarenko

The article examines the institutional potential of cooperation between higher education institutions and industrial enterprises as one of the key tools for modernizing the economy of the Republic of Belarus. Particular attention is given to the analysis of misaligned interests between the parties, as well as to practical examples of successful collaboration.

Keywords: university-industry cooperation, institutional analysis, innovation-driven economy, technology transfer, dual education, modernization.

Проблема недостаточной кооперации между высшими учебными заведениями и промышленным сектором приобретает особую актуальность в условиях усиливающейся конкуренции за технологическое лидерство. Экономики постсоветского пространства, включая Республику Беларусь, находятся на этапе структурных изменений, требующих переосмысления роли науки и образования в производственном развитии. Сотрудничество между университетами и промышленностью в этом контексте представляет собой не только интеграцию образования, науки и производства,