6. Он умеет объяснять сложные вещи простыми словами.
7. Его имя ассоциируется с надежностью и качеством.
8. Он становится «лицом профессии» и проводником бизнеса.

Таим образом, цифровизация не уничтожает профессию бухгалтера, а наоборот – открывает перед ней новые горизонты. Именно человек остается тем, кто способен разобраться в сложных ситуациях, увидеть риски и предложить решения.

Бухгалтер будущего – это не просто специалист по цифрам, а **бренд**, символ доверия и профессионализма. Его ценность заключается в умении сочетать экономические знания, цифровую грамотность и стратегическое мышление. Такой бухгалтер становится партнером бизнеса, проводником в мире финансов и гарантом финансовой устойчивости.

Список использованных источников

1. Бабченко. Т. Н. Цифровизация бухгалтерского учета: современные тенденции и перспективы развития / Т. Н. Бабченко // Экономика и бизнес. – 2023. – № 4. – С. 112–118.

2. Герасимова, Е. Б. Трансформация профессии бухгалтера в условиях цифровой экономики / Е. Б. Герасимова // Международный бухгалтерский учет. – 2022. – № 15. – С. 25–34.

УДК 004.056

ИНСТИТУЦИОНАЛЬНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ

М. Г. Плохоцкая
Е. С. Грузневич, к. э. н.. доцент
Витебский государственный технологический университет, г Витебск, Республика Беларусь

Аннотация. *В статье проводится комплексный анализ институциональной системы обеспечения кибербезопасности предприятий в Республике Беларусь. Особое внимание уделяется структуре государственного управления в сфере информационной безопасности, действующей нормативно-правовой базе, а также реализуемым государственным программам и стратегическим инициативам, направленным на укрепление киберустойчивости экономики. Рассматриваются ключевые институты, механизмы координации и правовые инструменты, формирующие основу защиты корпоративной информационной инфраструктуры в условиях нарастающих цифровых вызовов.*

Ключевые слова: *защита данных, кибербезопасность, информационная безопасность, информационное общество, информатизация.*

INSTITUTIONAL SYSTEM FOR ENSURING CYBERSECURITY OF ENTERPRISES IN THE REPUBLIC OF BELARUS

M. G. Plakhotskaya
K. S. Hruznevich, PhD in Economics, Associate Professor
Vitebsk State Technological University, Vitebsk, Republic of Belarus

Abstract. *The article provides a comprehensive analysis of the institutional system for ensuring the cybersecurity of enterprises in the Republic of Belarus. Special attention is paid to the structure of public administration in the field of information security, the current legal framework, as well as the implemented state programs and strategic initiatives aimed at strengthening the cyber resilience of the economy. The article examines the key institutions, coordination mechanisms, and*

legal tools that form the basis for protecting corporate information infrastructure in the face of growing digital challenges.

Keywords: *data protection, cybersecurity, information security, information society, informatization.*

В условиях стремительной цифровизации экономики и общества кибербезопасность становится стратегическим приоритетом как для государств, так и для отдельных предприятий. Для Республики Беларусь, активно реализующей программу цифрового развития, обеспечение защиты информационной инфраструктуры приобретает особое значение. Современные предприятия все больше зависят от цифровых технологий: от автоматизированных производственных процессов до взаимодействия с государственными органами и клиентами через электронные сервисы.

Согласно данным, представленным в обзоре ООН по электронному правительству 2024 года, Республика Беларусь характеризуется высоким уровнем развития цифрового правительства (77-е место в мире – это свидетельствует о серьезных достижениях в цифровизации государственных услуг и инфраструктуры) [1]. В то же время исследование Global Cybersecurity Index 2024 показывает, что уровень кибербезопасности в стране оценивается как «устанавливающийся» (Tier 3), демонстрируя высокие показатели в области юридического регулирования и международного сотрудничества, но при этом имея значительные пробелы в технических мерах, организационных стратегиях и развитии потенциала в сфере кибербезопасности [2].

Этот дисбаланс между уровнем цифрового развития и уровнем защищенности цифровых систем создает риски: чем выше степень цифровизации, тем выше потенциальные последствия кибератак – от финансовых потерь до нарушения критически важных государственных и производственных процессов. Особенно уязвимыми оказываются малые и средние предприятия, которые зачастую не обладают ни ресурсами, ни компетенциями для обеспечения адекватной защиты.

В этих условиях институциональная система обеспечения кибербезопасности предприятий становится не просто вспомогательным, а стратегически необходимым элементом национальной политики в области цифровой устойчивости.

Целью данного исследования является анализ институциональной системы обеспечения кибербезопасности предприятий в Республике Беларусь, включая нормативно-правовую базу, организационную структуру, ключевые государственные программы и механизмы взаимодействия между органами власти и бизнес-сообществом.

Исследование основано на анализе нормативно-правовых актов Республики Беларусь, регулирующих вопросы кибербезопасности и защиты информации. В частности, использованы: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [3]; Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» [4]; Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» [5]; а также Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы [6].

Методологическую основу составили методы системного анализа, сравнительно-правового анализа, документального анализа и обобщения. Дополнительно использовались данные из научных публикаций, а также официальной статистики.

В Республике Беларусь проводится серьезная работа, направленная на обеспечение кибер- и информационной безопасности. В частности, разработан комплекс нормативных правовых документов, представляющий собой фундаментальную основу для создания эффективной системы защиты информационных ресурсов, а также прав и интересов граждан, общества и государства: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [3], Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» [5], а также Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» [4].

Приведем основное содержание названных НПА в таблице 1.

Таблица 1 – Нормативно-правовое регулирование кибербезопасности в Республике Беларусь

Наименование	Основное содержание
Закон Республики Беларусь от 10 ноября 2008 г. № 455-З 2 «Об информации, информатизации и защите информации»	Определяется фундаментальным правовым актом в сфере информационной безопасности. Он закрепляет основные понятия (информация, информационные ресурсы, системы и сети, защита информации), определяет права и обязанности субъектов информационных отношений, а также устанавливает общие принципы обеспечения информационной безопасности. Особое значение имеет положение о том, что государственные информационные системы не могут эксплуатироваться без реализации мер позащите информации, а системы, обрабатывающие информацию с ограниченным доступом, обязаны использовать аттестованные средства защиты. Тем самым закон вводит обязательность проведения аттестации систем защиты информации и закладывает правовую основу для последующего регулирования в области кибербезопасности
Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности»	Этот документ знаменует переход от разрозненных подходов к созданию единой, централизованной национальной системы обеспечения кибербезопасности. В нем четко определены элементы системы (Оперативно-аналитический центр, Национальный центр кибербезопасности, центры кибербезопасности организаций), а также их задачи: обнаружение и предотвращение кибератак, анализ киберинцидентов, оценка уровня защищенности объектов инфраструктуры. Особенно важно, что Указ закрепляет за ОАЦ при Президенте РБ функции координации всей системы, включая право выносить обязательные предписания. Это делает ОАЦ ключевым управляющим органом в сфере кибербезопасности и придает системе четкость и иерархичность
Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»	Документ ориентирован на усиление технической и криптографической защиты информации в государственных органах, организациях и на критически важных объектах информатизации. Он регулирует порядок создания и аттестации систем защиты информации, а также вводит обязательное лицензирование деятельности по технической и криптографической защите. Указ определяет, что ответственность за организацию защиты информации несут руководители организаций, а контроль за ее реализацией осуществляет Оперативно-аналитический центр. Таким образом, документ формирует организационно-правовой механизм обеспечения безопасности на уровне отдельных предприятий и закладывает основу для последующего развития института кибербезопасности

Примечание – Источник: составлено автором на основе [3, 4, 5].

Названные документы устанавливают общие рамки и требования, тогда как программы по кибербезопасности включают конкретные меры, стратегии и инициативы для их реализации на практике. Ключевой является Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы. Она представляет собой стратегический документ, определяющий приоритеты цифровой трансформации страны. В рамках подпрограммы «Информационная безопасность и цифровое доверие» программа формулирует конкретные меры по обеспечению кибербезопасности как неотъемлемого условия устойчивого цифрового развития. Среди ключевых направлений – разработка и внедрение отечественных программно-аппаратных средств защиты, создание условий для надежной идентификации пользователей, формирование «цифрового доверия» при оказании электронных услуг.

Кроме того, в Беларуси сформирована централизованная и многоуровневая институциональная система обеспечения кибербезопасности, закрепленная различными НПА.

Координация государственной политики в этой сфере возложена на Министерство связи и информатизации. Оперативное управление и мониторинг киберугроз осуществляются через национальную систему обеспечения кибербезопасности. Представим элементы национальной системы кибербезопасности на рисунке 1.

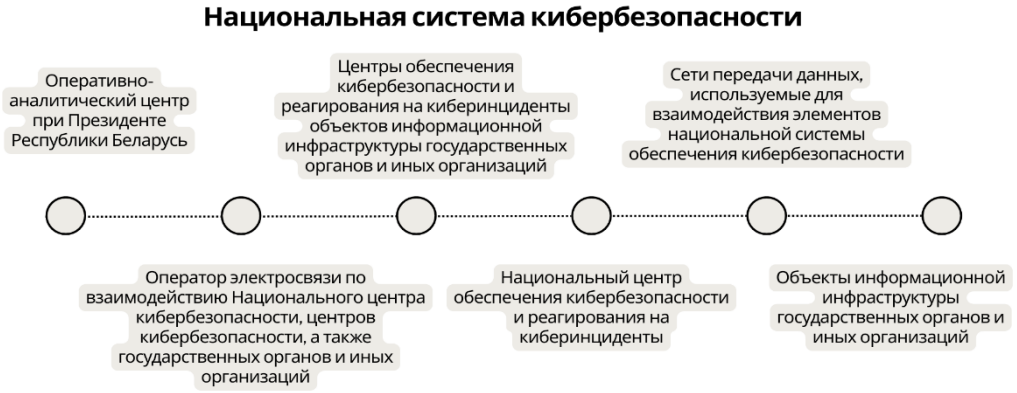

Рисунок 1 – Национальная система кибербезопасности

Ядром национальной системы обеспечения кибербезопасности Республики Беларусь выступает Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ), наделенный функциями центрального координирующего и регулирующего органа. Именно ОАЦ определяет требования к защите объектов информационной инфраструктуры, устанавливает состав технических параметров киберинцидентов, вырабатывает методические рекомендации по противодействию кибератакам и имеет право выносить обязательные для исполнения предписания [5].

Непосредственное обнаружение киберинцидентов и реагирование на них реализуются через Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты. Этот центр координирует деятельность специализированных центров кибербезопасности, который обеспечивают мониторинг, оценку уязвимостей, расследование инцидентов и оперативное устранение последствий атак на уровне конкретных организаций [5].

Вся система функционирует на основе защищенного информационного взаимодействия: обмен данными между ОАЦ, Национальным центром, ведомственными центрами кибербезопасности и другими участниками осуществляется по специализированным сетям передачи данных [5].

Помимо центрального блока, в обеспечении кибербезопасности участвуют и другие государственные структуры. Министерство внутренних дел отвечает за противодействие киберпреступност. Комитет государственной безопасности обеспечивает контрразведывательное сопровождение и защиту сведений, составляющих государственную тайну [5]. Такой распределенный, но централизованно управляемый подход позволяет охватить все ключевые аспекты кибербезопасности – от проактивной защиты до уголовно-правового и контрразведывательного реагирования.

Таким образом, в Республике Беларусь сформирована централизованная институциональная система обеспечения кибербезопасности предприятий, основанная на современной нормативно-правовой базе и стратегических государственных программах. Успешное функционирование системы зависит от эффективного взаимодействия Оперативно-аналитического центра, национального и ведомственных центров кибербезопасности, а также от дальнейшего развития кадрового потенциала и внедрения практических мер защиты на уровне предприятий.

Список использованных источников

1. United Nations. UN E-Government Survey 2024 //United Nations Department of Economic and Social Affairs. – New York, 2024. – С. 324.

2. International Telecommunication Union. Global Cybersecurity Index-2024 // 5th Edition. – Geneva : ITU, 2024. – С. 124.

3. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З // Нац. правовой Интернет-портал Респ. Беларусь. – URL: https://pravo.by/document/?guid=3871&p0=h10800455 (дата обращения: 07.12.2025).

4. О некоторых мерах по совершенствованию защиты информации : Указ Президента Респ. Беларусь от 16 апр. 2013 г. № 196 // Нац. правовой Интернет-портал Респ. Беларусь. – URL: https://pravo.by/document/?guid=12551&p0=P31300196. (дата обращения: 06.12.2025).

5. О кибербезопасности : Указ Президента Респ. Беларусь от 14 февр. 2023 г. № 40 // Официальный интернет-портал Президента Респ. Беларусь. – URL: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g. (дата обращения: 07.12.2025.

6. О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы : постановление Совета Министров Респ. Беларусь от 2 февр. 2021 г. № 66 // Нац. правовой Интернет-портал Респ. Беларусь. – URL: https://pravo.by/ document/-?guid=3871&p0=C22100066 (дата обращения: 08.12.2025).

УДК 37.013.42:330

ПРОФОРИЕНТАЦИЯ ШКОЛЬНИКОВ НА ЭКОНОМИЧЕСКИЕ СПЕЦИАЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ГЕЙМИФИЦИРОВАННЫХ ОБРАЗОВАТЕЛЬНЫХ ПЛАТФОРМ

Е. А. Иношевская
Е. С. Грузневич, к. э. н., доцент
Витебский государственный технологический университет, г. Витебск, Республика Беларусь

Аннотация. *В статье рассматриваются инновационные подходы к профориентации школьников на экономические специальности с использованием геймифицированных образовательных платформ. Обосновывается актуальность темы в условиях цифровизации и роста интереса молодежи к экономике. Особое внимание уделяется теоретическим основам геймификации, ее влиянию на мотивацию и вовлеченность учащихся, а также практическим моделям игровых симуляций, позволяющих формировать прикладные компетенции. Приводится сравнительный анализ традиционных и инновационных методов профориентации, подтверждающий эффективность игровых технологий в образовательной среде.*

Ключевые слова: *профориентация, геймификация, экономика, образовательные платформы, мотивация.*

CAREER GUIDANCE OF SCHOOL STUDENTS IN ECONOMIC SPECIALTIES THROUGH GAMIFIED EDUCATIONAL PLATFORMS

E. A. Inoshevskaya
K. S. Hruznevich, PhD in Economics, Associate Professor
Vitebsk State Technological University Vitebsk, Belarus

Abstract. *The article examines innovative approaches to career guidance for school students in economic specialties through gamified educational platforms. The relevance of the topic is justified in the context of digitalization and the growing interest of young people in economics. Theoretical foundations of gamification and its impact on students' motivation and engagement are discussed. Practical models of gamified simulations are presented, demonstrating their role in developing applied competencies. A comparative analysis of traditional and innovative career guidance methods highlights the effectiveness of gamification in the educational environment.*

Keywords: *career guidance, gamification, economics, educational platforms, motivation.*