УДК 338.2

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ЭКОНОМИКИ ДАННЫХ

В. А. Остапенко

студент, Белорусский государственный университет, г. Минск, Беларусь, vlad.ostapenko.2003@gmail.com

Научный руководитель: **Г. Г. Головенчик**

кандидат экономических наук, доцент, Белорусский государственный университет, г. Минск, Беларусь, goloventchik@bsu.by

Статья рассматривает законодательные и практические аспекты информационной безопасности в Республике Беларусь. Автор анализирует достижения и вызовы, с которыми сталкивается страна в процессе обеспечения информационной безопасности и международное сотрудничество в этой сфере. Особое внимание уделяется необходимости развития кибербезопасности в рамках экономики данных, что представляет собой актуальное направление для дальнейших исследований и законодательных инициатив в Республике Беларусь и за её пределами.

Ключевые слова: информационная безопасность; персональные данные; законодательство; экономика данных; кибербезопасность.

ENSURING INFORMATION SECURITY WITHIN THE DATA ECONOMY

V. A. Ostapenko

student, Belarusian State University, Minsk, Belarus, vlad.ostapenko.2003@gmail.com

Supervisor: **G. G. Golovenchick**

PhD in economics, associate professor, Belarusian State University, Minsk, Belarus, goloventchik@bsu.by

The article examines in detail the legislative and practical aspects of information security in the Republic of Belarus. The author analyzes the achievements and challenges faced by the country in the process of ensuring information security and international cooperation in this area. Particular attention is paid to the need to develop cybersecurity within the framework of the data economy, which is an urgent area for further research and legislative initiatives in the Republic of Belarus and beyond.

Keywords: information security; personal data; legislation; data economy; cybersecurity.

В Республике Беларусь понятие информационной безопасности закреп-

лено на законодательном уровне в Концепции информационной безопасности Республики Беларусь [1]. **Информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Концепция охватывает различные аспекты информационной безопасности, включая защиту конфиденциальной информации, разработку механизмов реализации правовых норм, регулирующих отношения в информационной сфере, и подготовку концепции правового обеспечения информационной безопасности. В нем также подчеркивается важность обеспечения национальной безопасности, суверенитета и защиты персональных данных и информации о частной жизни, а также прав субъектов информационных отношений на создание, использование и эксплуатацию информационных систем и сетей, применение информационных технологий, формирование и использование информационных ресурсов.

Также особое отношение существует к персональным данным, закрепленное в законе «О защите персональных данных» от 7 мая 2021 г. Он регулирует отношения в сфере обработки персональных данных, основываясь на законодательстве о персональных данных и международных договорах Республики Беларусь. Закон устанавливает право субъекта персональных данных требовать прекращения обработки своих данных при отсутствии оснований для обработки, предусмотренных законом. Оператор обязан прекратить обработку данных по требованию субъекта. Закон также предусматривает прозрачность процесса обработки данных, согласие субъекта на обработку данных, и ограничение обработки данных конкретными законными целями [2].

За 2023 г. Национальным центром защиты персональных данных Республики Беларусь было удалено более 622 тысяч незаконно обрабатываемых записей персональных данных в результате рассмотрения 191 жалобы и проведения свыше 200 проверок, после чего были приняты меры по восстановлению нарушенных прав граждан и направлены материалы для привлечения к ответственности. Разработаны и опубликованы разъяснения и комментарии к законодательству о защите персональных данных, проведено обучение более 9,8 тыс. человек [3].

Тем не менее, несмотря на достаточно активную деятельность в рамках регулирования персональных данных и обеспечению информационной безопасности, в Республики Беларусь еще не проработана концепция экономики данных, которая характеризуется операциями с товарами и услугами, которые генерируют, хранят и обмениваются информацией, которая со временем обесценивается. Экономику данных можно интерпретировать двумя взаимосвязанными, но различными способами: как цифровую экономику, которая создает и фиксирует ценность самих данных, и как физическую экономику, в которой более эффективное использование

данных влияет на традиционные процессы и трансформирует их [4]. Основные уровни экономики данных отражены на рис. 1.

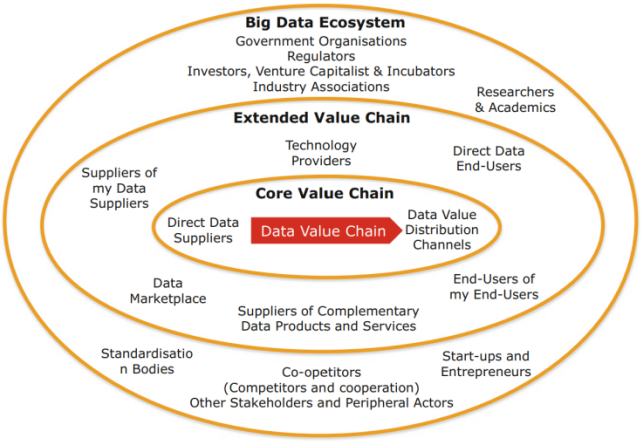

Рис. 1. Микро-, мезо- и макроуровни экосистемы больших данных.
Источник: [4]

В рамках такой экономики важно создание цифровой и институциональной инфраструктуры, которая будет соответствовать современным принципам кибербезопасности. Создание такой инфраструктуры будет эффективно не только в рамках Республики Беларусь, но и Евразийского экономического союза.

Экономика данных в рамках ЕС активно развивается: уже выработана методология оценки объемов рынка данных, доли в экономике, отраслях, отмечены основные движущие силы со стороны data-driven компаний. В 2023 г. экономика данных в ЕС-27 оценивалась в 544 миллиарда евро, что свидетельствует о значительном росте на 9,3% по сравнению с 2022 годом (рис. 2). Ожидается, что к 2030 г. он достигнет почти 955 миллиардов евро (доля в ВВП – 5,8%) в соответствии с базовым сценарием [5].

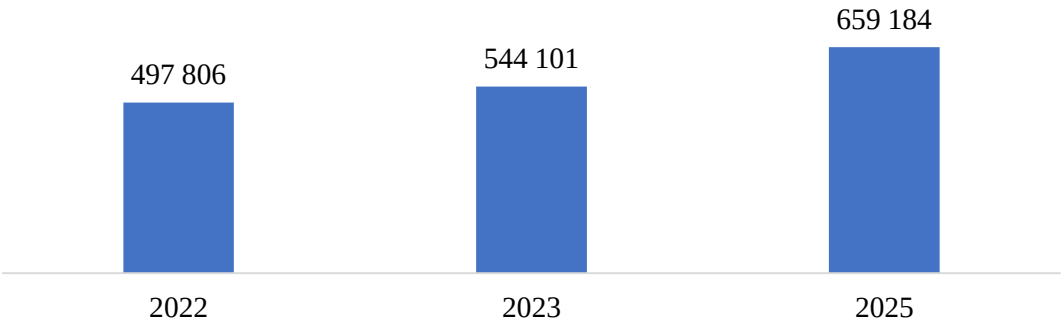

Рис. 2. Стоимостные размеры экономики данных ЕС с 2023 по 2025 годы.
Источник: [5]

Говоря про законодательные инициативы, то ЕС преуспело в этом направлении, закрепив важные аспекты кибербезопасности в своих правовых

документах. В рамках Общего регламента по защите данных (далее – GDPR), в ЕС было наложено несколько крупных штрафов. Это включает в себя огромные штрафы, наложенные на Amazon (746 миллионов евро), Facebook (265 миллионов евро) и ее дочернюю компанию WhatsApp (225 миллионов евро), а также Google (90 миллионов евро) [6].

Инициативы Европейского союза в области кибербезопасности, подкрепленные программой «Цифровая Европа» (Digital Europe), направлены на стандартизацию высокого уровня кибербезопасности во всех государствах-членах, признавая растущую важность онлайн-сервисов и экономических возможностей в сфере кибербезопасности. Закон о киберустойчивости (Cyber Resilience Act) вводит обязательные требования к безопасности цифровых продуктов и программного обеспечения, обеспечивая их сохранность на протяжении всего жизненного цикла и укрепляя доверие потребителей и бизнеса. Закон ЕС о кибербезопасности (EU Cybersecurity Act) укрепляет Агентство ЕС по кибербезопасности (ENISA) и устанавливает единую систему сертификации в области кибербезопасности, облегчая единый процесс сертификации, признанный во всем ЕС. Стратегия кибербезопасности ЕС (EU Cybersecurity Strategy) направлена на повышение устойчивости, оперативного потенциала и международного сотрудничества в борьбе с киберугрозами, подчеркивая необходимость надежных мер кибербезопасности для безопасного цифрового будущего. Создание Европейской сети и Центра компетенций в области кибербезопасности (European Cybersecurity Competence Network and Centre) объединяет усилия по созданию совместной экосистемы кибербезопасности, расширению исследований, инноваций и внедрению передовых технологий кибербезопасности. Эти стратегические меры отражают приверженность ЕС защите своей цифровой экономики от киберугроз с помощью нормативно-правовой базы, инноваций и международного сотрудничества [7].

В рамках обеспечения информационной безопасности специалисты Фонда капитального развития ООН (далее – UNCDF) выделяют несколько основных направлений противодействия киберугрозам: международное сотрудничество, национальные инициативы, улучшение уголовного законодательства и расширение возможностей правоохранительных органов, сотрудничество с частным сектором, освещение проблемы кибербезопасности посредством СМИ и образования [8].

Стратегии национальных правительств должны обеспечивать структурированный подход к защите национальной инфраструктуры и повышению устойчивости к кибератакам посредством создания автономных агентств по кибербезопасности и национальных групп реагирования на инциденты компьютерной безопасности (далее – CSIRTs).

Предприятия частного сектора все чаще внедряют надежные процедуры и методы обеспечения безопасности, руководствуясь национальными и международными системами управления кибер-рисками. Создание внутренних

CSIRTs в компаниях еще больше повышает их способность управлять инцидентами в области кибербезопасности и реагировать на них, подчеркивая важную роль частного сектора в поддержании кибербезопасности.

Обучение сотрудников по вопросам безопасности и инициативы по просвещению потребителей являются жизненно важными компонентами комплексной стратегии кибербезопасности, направленной на формирование культуры безопасности и внедрение передового опыта среди пользователей [8].

Регулирование в сфере информационной безопасности и защиты персональных данных в Республике Беларусь демонстрирует значительный прогресс, однако развитие концепции экономики данных остается важным направлением для дальнейшего укрепления кибербезопасности. Национальные усилия по обеспечению безопасности в информационной сфере активно дополняются международным сотрудничеством и внедрением современных технологических решений. Создание цифровой и институциональной инфраструктуры, соответствующей современным требованиям кибербезопасности, станет ключом к эффективной защите в эпоху цифровизации экономики не только на национальном уровне, но и в рамках международного сообщества.

Библиографические ссылки

1. Постановление Совета безопасности Республики Беларусь 18 марта 2019 г. № 1 "О Концепции информационной безопасности Республики Беларусь" // Национальный правовой Интернет-портал Республики Беларусь. URL: https://pravo.by/ document/?guid=3871&p0=P219s0001 (дата обращения: 11.03.2024).

2. Закон Республики Беларусь 7 мая 2021 г. № 99-З "О защите персональных данных" // Национальный правовой Интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=12551&p0=H12100099&p1=1&p5=0 (дата обращения: 11.03.2024).

3. Национальный центр защиты персональных данных Республики Беларусь [Электронный ресурс]. URL: https://cpd.by/o-centre/otchety-o-dejatelnosti/ (дата обращения: 05.04.2024).

4. *Jose´ Marı´a Cavanillas, Edward Curry.* New Horizons for a Data-Driven Economy A Roadmap for Usage and Exploitation of Big Data in Europe // SpringerLink.

5. *Glennon M., La Croce L.* DATA Market Study 2021–2023 / Lisbon Council: C. Moise, D. Osimo. Luxembourg / Gasperich : [s.n.], 2023. Deliverable D2.7 First Report on Facts and Figures. Version 2.0. Data Policy and Innovation, EUFO 1/265, L–2557. Contract ref. LC-01568518.

6. How much does GDPR compliance cost in 2023 [Electronic resource]. URL: https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020 (date of access: 06.04.2024).

7. Cybersecurity policies [Electronic resource] // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (date of access: 05.04.2024).

8. The role of cybersecurity and data security in the digital economy [Electronic resource] // UNCDF. URL: https://policyaccelerator.uncdf.org/all/brief-cybersecurity-digital-economy (date of access: 05.04.2024).