

УДК 336.71

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ВАЖНОЕ УСЛОВИЕ ЦИФРОВОЙ ЭКОНОМИКИ

Ж. К. Мусаева¹⁾, М. М. Шарипова²⁾

*¹⁾ Старший преподаватель кафедры менеджмента
Бухарского инженерно-технологического института, г. Бухара, Узбекистан*

*²⁾ Магистрантка кафедры менеджмента
Бухарский инженерно-технологического института, г. Бухара, Узбекистан*

В статье рассмотрены тенденции развития цифровой экономики, особенности цифровой трансформации и роли обеспечения информационной безопасности в различных сферах экономики Узбекистана. Также уделяется особое внимание решению проблем безопасности в киберпространстве страны.

Ключевые слова: цифровая экономика; электронный бизнес; цифровая трансформация; правовая база; мониторинг; инфраструктура; электронные услуги.

INFORMATION SECURITY IS AN IMPORTANT CONDITION FOR THE DIGITAL ECONOMY

J. K. Musaeva¹⁾, M. M. Sharipova²⁾

*¹⁾ Senior Lecturer of Management Department
of the Bukhara Engineering and Technology Institute, Bukhara, Uzbekistan*

*²⁾ Master's Student of Management Department
of the Bukhara Engineering and Technology Institute, Bukhara, Uzbekistan*

The article examines trends in the development of the digital economy, the features of digital transformation and the role of ensuring information security in various spheres of the economy of Uzbekistan. Also, special attention is paid to solving security problems in the country's cyberspace.

Keywords: digital economy; electronic business; digital transformation; legal framework; monitoring; infrastructure; electronic services.

Все системы в Узбекистане переводятся в цифровую форму. Главным фактором развития цифровой экономики является обеспечение информационной безопасности. Особенно в условиях карантинного режима, введенного из-за пандемии коронавируса, еще больше увеличился спрос на онлайн-товары и услуги, расширился спектр цифровых функций во всех сферах. Сегодня можно оплачивать товары и услуги, не выходя из дома, без проблем получать дистанционное обучение, пользоваться крупнейшими библиотеками мира и даже работать. Цифровые сервисы имеют ряд преимуществ перед традиционным типом, такие как оформление документов, отсутствие формальности, экономия времени. Например, если вы получаете государственные услуги в цифровой форме, вам будет предложена скидка в размере 10 процентов от установленной платы. Все это свидетельствует об активном переходе нашей страны к цифровой экономике [5].

В условиях карантина были зафиксированы случаи распространения вирусов, выводящих из строя программные системы в соответствии с рекомендациями по защите от болезни в глобальной сети. Финансовые мошенники, которые обманывают простых людей, обещая продавать и доставлять лекарства в Интернете, и просят заранее перевести

деньги на счет, использовали поддельные интернет магазины, веб-сайты, учетные записи в социальных сетях и адреса электронной почты. Это также подтверждает необходимость обеспечения информационной безопасности.

Концепции цифровой трансформации и информационной безопасности всегда идут бок о бок. Потому что наряду с оцифровкой всех систем и процессов важно обеспечить их технически безупречную работу и безопасность. Чем больше внимания уделяется развитию цифровой экономики в нашей стране, тем актуальнее обеспечение кибер безопасности. Узбекистан укрепляет свои позиции в мировом индексе кибер безопасности [1].

Информационная безопасность (кибербезопасность) – это концепция, которая служит для сортировки информации, являясь формой информационной безопасности. Это относится к техническим процессам и для обычного пользователя означает установку безопасных и надежных паролей в почте, социальных сетях, платежных системах, защиту вашего персонального компьютера и смартфона от вирусов. В более широком смысле информационная безопасность – это комплекс мер, направленных на защиту сетей, мобильных приложений и устройств, что означает сохранение конфиденциальности данных, защиту их целостности, полноценную работу того или иного сайта, приложения, программы [3].

Согласно анализу ГУП «Центр кибербезопасности», в 2019 году на сайтах национального сегмента сети Интернет было выявлено 268 инцидентов ИБ. Это означает, что количество правонарушений в цифровом мире снизилось на 44 % по сравнению с прошлым годом. Из них 222 приходились на не санкционированную загрузку контента, 45 на дефолт (хакерская атака, означающая, что страница веб-сайта была заменена другой, например, страницей с рекламой), а одна на долю секретной добычи (скрытая активность на крипто валютной платформе), 69 % инцидентов были обнаружены на сайтах провайдер-хостингов в Узбекистане, а оставшийся 31 % был связан с сайтами провайдер-хостингов зарубежных стран. Было проведено расследование 80 случаев и даны практические рекомендации по устранению выявленных уязвимостей, а оставшиеся 188 случаев были разрешены независимо владельцами веб-сайтов.

Проблемы безопасности в киберпространстве вызваны управлением контентом с ошибками безопасности в коде, работой с устаревшими версиями, простотой доступа к паролям, шаблонами, загруженными из небезопасных источников, управлением веб-сайтами на компьютерах, зараженных вирусами [4].

Мониторинг национального сегмента сети Интернет выявил более 130000 угроз кибербезопасности. Из них 106508 случаев касались хостов, которые стали участниками этих сетей. 13882 случая связаны с блокировкой IP-адресов из черного списка. 8457 случаев связаны с использованием TFTP (Trivial File Transfer Protocol) и портов, что может привести к загрузке постороннего контента из-за отсутствия механизмов аутентификации. 2114 случаев связаны с использованием слабого протокола RDP (Remote Desktop Protocol). 1042 случая связаны с отсутствием механизма аутентификации в программном обеспечении и системах управления базами данных, а также с SSL-сертификатами с просроченными или недействительными подписями.

Эти анализы еще раз подтверждают актуальность проблемы кибербезопасности, поскольку уязвимости программного обеспечения могут привести к тому, что злоумышленник нарушит права на информационную систему или веб-сайт, а также файлы и данные удаленно, личные данные граждан. Меры кибербезопасности предотвращают такие случаи.

Согласно Государственной программе реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан на 2017–2021 годы в «Год науки, просвещения и цифровой экономики», разработана Национальная стратегия кибербезопасности на 2020 год, и законопроект «О кибербезопасности» на 2023 год [1].

Юридическое усиление стандартов кибербезопасности – необходимая и уместная мера. Цифровой мир еще не смог четко определить свой статус юридически. В связи с этим появляются новые виды и формы угроз, которые необходимо отразить в законодательстве. Разработка национальной стратегии кибербезопасности будет регулировать деятельность по борьбе с преступностью в национальном киберпространстве. Ведь вред и опасность совершения преступлений в виртуальном мире не меньше, чем в реальном мире.

Также, согласно Национальной стратегии кибербезопасности на 2020–2023 годы, будет сформирована единая система кибербезопасности и правовая база в области защиты критической инфраструктуры от кибератак. В законе «О кибербезопасности» предполагается отразить защиту информационно-коммуникационных технологий от современных кибер атак, внедрение современных механизмов кибер безопасности на различных уровнях, определение прав и обязанностей государственных органов, предприятий и организаций, согласование их деятельности. Действительно, возникла необходимость унификации нормативно-правовых документов в этой сфере. В основе всех реформ, проводимых в нашей стране, лежит цель создания удобств для нашего народа. Акцент на кибербезопасности заложил основу для надежного и безопасного использования цифровых возможностей [3].

В целях подготовки кадров, владеющих современными технологиями программирования, в нашей стране реализуется проект «Миллион программистов». Главное условие этого проекта цифровая трансформация, как мера экономического развития, интеграции в мировое сообщество, комплексного развития всех секторов. В современном мире существует большой спрос на программистов, способных внедрить цифровую трансформацию, мобилизацию, искусственный интеллект. Поскольку инфраструктура, обеспечивающая цифровую экономику, даже большие инвестиции в сферу ИКТ, не оправдывают себя без программистов, которые могут эффективно использовать электронные возможности.

В настоящее время через образовательный портал uzbekcoders.uz проходят тренинги по проекту, направленному на запуск цифровой экономики и обучение одного миллиона программистов для обеспечения его эффективной работы. Видео уроки снабжены узбекскими субтитрами. Любой желающий может зарегистрироваться и посещать онлайн-классы. Занятия проходят бесплатно удаленно [2].

На первом этапе проекта была запущена рекламная кампания по ознакомлению общественности с проектом и продвижению уроков, которые помогут им приобрести цифровые навыки. На начальном этапе проекта «Миллион программистов» было охвачено более 62000 студентов, из них 5400 получили сертификаты. Проект включен в бесплатные сервисы образовательного портала ZIYONET, мобильного оператора UZMOBILE и интернет провайдеров UZONLINE. В рамках этого проекта в учебных центрах по цифровым технологиям вводится обучение навыкам программирования.

В рамках проекта будут обучены программисты по четырем направлениям. К ним относятся Android (в партнерстве с Google), Frontend и Full-stack программирование, а также анализ данных. Каждый из них состоит из начального 120-часового, то есть 12-недельного курса. Для начала занятий не требуется специальных знаний. В тренинге используются материалы Udacity, ведущей онлайн-платформы, ориентированной на ИТ-специальности. Учебный план платформы и содержание курсов были разработаны в сотрудничестве вместе с Google, Facebook, Amazon, Autodesk и другими ведущими компаниями. Все курсы направлены на формирование практических навыков работы с проектами, основанными на реальных наборах данных.

Молодёжь также интересуются современными профессиями. Им была предоставлена возможность посещать несколько курсов одновременно. График тренировок гибкий. На освоение первого этапа нужно всего две недели. Но даже несмотря на то, что

времени на подготовку уроков мало, их можно пройти за 3 месяца. Второй этап начинается после завершения первого, т. е. после сдачи тестов, оценивающих практические знания. Если участник также не успевает завершить его в течение 10–12 недель, он может освоить его в течение 3 месяцев. Таким образом, с первого дня регистрации на сайте дается в общей сложности 6 месяцев, чтобы полностью изучить содержание курса. Участникам вручены два типа сертификатов участника и выпускников.

Библиографические ссылки

1. Послание Президента Республики Узбекистан Шавката Мирзиёева Олий Мажлису от 29 декабря 2020 года.
2. Постановление Кабинета Министров «О дополнительных мерах по дальнейшему развитию и внедрению цифровой экономики в Республике Узбекистан» от 31 августа 2018 года.
3. Гулямов С. С. и др. Блокчейн-технологии в цифровой экономике. Т : Издательство «Иктисод молия», 2019. 396 с.
4. Lapidus L. V. Цифровая экономика: управление электронным бизнесом и электронной коммерцией. М. : ИНФРА-М, 2017. 281 с.
5. Мусаева Ж. К. Цифровая экономика как залог будущего развития – Цифровая экономика: новый этап в развитии нового Узбекистана новыми технологиями, платформами и бизнес-моделями Материалы Международной научно-практической конференции «Новый этап». Ташкент : Таджикот, 2020.

УДК 338.242

МОДЕЛЬ ТОВАРНОГО РЫНКА С ПАССИВНОЙ РЕАКЦИЕЙ ПОКУПАТЕЛЕЙ И ПРОДАВЦОВ НА ИЗМЕНЕНИЕ ЦЕН

Н. В. Новикова

*Старший преподаватель кафедры аналитической экономики и эконометрики
экономического факультета Белорусского государственного университета, г. Минск*

Мотивы поведения субъектов рыночных отношений – производителей и потребителей – могут основываться на информации о тенденции цен на товары или услуги, причем наличие такой информации способно существенно влиять на ход договорного процесса при достижении компромисса. В зависимости от реакции на такую информацию основных субъектов рыночных отношений продавцов и покупателей определяется либо устойчивость экономического равновесия, либо его неустойчивость. В данной работе показано, что пассивная реакция спроса и предложения приводит к неустойчивому развитию товарного рынка.

Ключевые слова: рынок; спрос; предложение; равновесие; стабильность.

MODEL OF A COMMODITY MARKET WITH A PASSIVE REACTION OF BUYERS AND SELLERS TO PRICE CHANGE

N. Novikova

*Senior Lecturer of Analytical Economics and Econometrics Department
at the Faculty of Economics of the Belarusian State University, Minsk*

The motives of behavior of the subjects of market relations – producers and consumers – can be based on information about the trend in prices for goods or services, and the availability of such information can significantly affect the course of the contractual process when a compromise is reached. Depending on the reaction to such information of the main subjects of market relations of