цифровых технологий компаниями, получившими поддержку в рамках федерального проекта «Цифровые технологии», процент», «Методикой расчета показателя «Количество PCT-заявок по «сквозным» цифровым технологиям, поданных организациями, получившими поддержку в рамках национального проекта «Цифровая экономика», «процент») // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=366350&demo=1 (дата обращения: 05.09.2022).

14. Об утверждении Плана противодействия коррупции ФАС России на 2021–2024 годы в нем Применение цифровых технологий в целях противодействия коррупции и разработка мер по противодействию новым формам проявления коррупции, связанным с использованием цифровых технологий»: Приказ ФАС от 30.09.2021 № 1054/21 // СПС «КонсультантПлюс». URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=414916&demo=1 (дата обращения: 04.09.2022).

15. Ожегов С. И. Толковый словарь русского языка. Москва, 1992.

16. Основные направления бюджетной, налоговой и таможенно-тарифной политики на 2019 год и на плановый период 2020 и 2021 годов (утв. Минфином России) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=308390#0GS 2ZGT0K5lxrJ9q (дата обращения: 05.09.2022).

17. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н. А. Голованова, А. А. Гравина, О. А. Зайцев и др. Москва: ИЗиСП, КОНТРАКТ, 2019. 212 с.

18. Чермянинов Д. В. Информационные и цифровые технологии в таможенном регулировании: суть и соотношение понятий // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2018. Т. 4, № 4. С. 133–145.

Н. Ф. Гуломова,
доктор экономических наук, PhD,
директор Индийско-Узбекского центра информационных технологий,
Ташкентский университет информационных технологий
имени Мухаммада аль-Хорезми

ПРОБЛЕМЫ, ВОЗНИКАЮЩИЕ В ПРОЦЕССЕ ПЕРЕХОДА К ЦИФРОВОЙ ЭКОНОМИКЕ В УЗБЕКИСТАНЕ: РОСТ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

Аннотация. Экспоненциальный рост взаимосвязей в Интернете привел к значительному росту угроз кибербезопасности. Совершенствование правового регулирования, а также разработка более инновационных и эффективных механизмов защиты от киберпреступлений считается необходимой потребностью в кибербезопасности. В данной статье рассмотрены проблемы кибератак, возникающие в процессе перехода к цифровой экономике, и меры по обеспечению кибербезопасности в Узбекистане.

Ключевые слова: киберпреступление, кибербезопасность, цифровая экономика, проблемы, кибератаки, правовые механизмы

PROBLEMS ARISING IN THE PROCESS OF TRANSITION TO THE DIGITAL ECONOMY IN UZBEKISTAN: THE RISE OF CYBERSECURITY THREATS

Abstract. The exponential growth of interconnections on the Internet has led to a significant increase in cybersecurity threats. Improving legal regulation, as well as developing more innovative and effective mechanisms for protecting against cybercrime, is considered a necessary need for cybersecurity. This article discusses the problems of cyber-attacks that arise in the process of transition to a digital economy and measures to ensure cyber security in Uzbekistan.

Keywords: Cybercrime, Cybersecurity, Digital economy, Problems, Cyberattacks, Legal mechanisms

Киберпреступность становится все более организованной, о чем свидетельствует рост числа инцидентов. В 2021 г. среднее количество кибератак и утечек данных увеличилось на 15,1 % по сравнению с предыдущим годом [1]. В эпоху глобализации безналичная оплата становится реальностью. Однако цифровая экономика, состоящая из взаимосвязанных электронных кошельков, социальных сетей и мобильного банкинга, создала условия для процветания киберпреступности в Узбекистане. Киберпреступления выступают как угроза развитию цифровой экономики. Для кражи денег с электронных кошельков людей появилась новая технология, в которой хакеры и мошенники используют фишинг. вымогательство (кибервымогательство) путем угрозы завладения и раскрытия личной информации; запугивание с применением насилия, оскорбления в социальных сетях (кибербуллинг) и т. п. Кроме того, все более серьезными становятся риски, связанные с повреждением и потерей информации из-за вирусных заражений каналов связи и баз данных. Банковский и финансовый секторы становятся все более привлекательными для злоумышленников. После недавних атак на финансовые учреждения и массового переноса услуг онлайн-банкинга в эпоху карантина все больше экспертов сходятся во мнении, что киберугрозы становятся ключом к финансовой стабильности банков и финансовых служб.

По мере развития информационных технологий возрастает и уязвимость киберпространства и его базовой инфраструктуры для широкого спектра рисков, связанных как с физическими, так и с киберугрозами и опасностями. Использование данных уязвимостей позволит злоумышленнику получить удаленный доступ к информационной системе или веб-сайту, а также к файлам и информации, что в свою очередь может привести к утечке персональных данных 2 026 824 граждан Республики Узбекистан. Так, согласно данным 2019 г., в информационных системах и на веб-сайтах национального сегмента сети Интернет выявлено 268 инцидентов, 816 уязвимостей и около 132 000 угроз кибербезопасности [2]. В Узбекистане за 2020 г. было выявлено более 27 000 000 событий вредоносной и подозрительной сетевой активности, исходящей из адресного пространства сегмента сети Интернет, которые в свою очередь представляют угрозу безопасному

и стабильному функционированию информационных систем и ресурсов. В стране только в 2020 г. было выявлено почти 8 млн инцидентов информационной безопасности, часть из которых имели критический уровень. Для минимизации рисков в ближайшие 3–5 лет цифровые технологии должны стать предметом национального и наднационального регулирования в Узбекистане; в то же время должны быть введены защитные меры для продвижения отечественных услуг на международный рынок.

Скорость интернет-соединения в Узбекистане остается относительно низкой, имеет плохое качество связи и происходят частые отключения [3]. Сбои в программном обеспечении, кибератаки, аварии, отключение электричества могут парализовать работу государственных органов, социальных бюджетных учреждений, отдельных предприятий, нанося им значительный экономический ущерб. Так, в качестве примера можно привести блэкаут, произошедший в январе 2022 г. в Узбекистане. Крупная авария, которая началась в энергосистеме Узбекистана, оставила жителей страны без света и охватила три страны Центральной Азии. По данным Минэнерго, возобновление подачи электричества по всему Узбекистану заняло около 53 часов [4].

Правовой основой, регулирующей сферу развития и цифровизации информационно-коммуникационных технологий, являются законы Республики Узбекистан «О связи», «О телекоммуникациях», «О государственных закупках», «Электронная коммерция», «Об электронных цифровых подписях» и «Об электронном документообороте» [5]. Большинство этих правовых документов приняты в период с 2000 по 2005 г., касающихся развития цифровой экономики, не учитывают тенденции развития в сфере ИКТ. Цифровая экономика изучается в областях гражданского права, интеллектуального права, налогового права, кибербезопасности.

На сегодняшний день в соответствии с современными тенденциями, вызовами и угрозами в области информационных технологий, популяризации киберпреступлений в связи с развитием глобальной сети Интернет законодательство Узбекистана вышло на новый уровень своего развития. В целях регулирования отношений в области персональных данных и их защиты 2 июля 2019 г. был принят Закон Республики Узбекистан «О персональных данных».

Кибербезопасность в Узбекистане регулируется Законом «О кибербезопасности», подписанным Президентом Республики Узбекистана от 15 апреля 2022 г. Закон состоит из 8 глав и 40 статей. На практике основная часть киберпреступлений, а именно 90 % экономических преступлений в киберпространстве связаны с электронной коммерцией. Именно на электронной торговой площадке могут возникнуть всевозможные кибератаки. Электронная коммерция регулируется Законом Республики Узбекистан «Об электронной коммерции». Использование в качестве пространства информационных систем с учетом особенностей заключения договора в электронной коммерции (путем осуществления акцепта в виде электронного документа или электронного сообщения) является предпосылкой возможной потенциальной угрозы киберпреступности в данной сфере. Уголовным кодексом Республики Узбекистан предусмотрены такие компьютерные преступления, как грабеж с использованием компьютер-

ной техники, растрата или взлом, кража путем несанкционированного доступа к компьютерной системе, незаконный сбор информации, ее разглашение или использование. В настоящее время в Узбекистане действует законодательство о преступлениях в области кибербезопасности, и государственные центры работают над регулированием этой сферы. UZ-CERT создана в целях обеспечения реализации постановления Президента Республики Узбекистан от 5 сентября 2005 г. № 167 «О дополнительных мерах по обеспечению компьютерной безопасности национальных информационно-коммуникационных систем» восстановление данных. Однако современная тенденция развития требует необходимости создания центров кибербезопасности на сетевой основе. Кроме того, необходимо дальнейшее изучение данной области с правовой точки зрения, разработка стандартов кибербезопасности для организаций, а также национальных программ кибербезопасности и стандартов показателей кибербезопасности. Благодаря последним реформам в области правового регулирования вопросов цифровизации Узбекистан улучшил свою позицию в Глобальном индексе кибербезопасности.

Индекс и рэнкинг кибербезопасности стран (Global Cybersecurity Index (GIC))

Страна	Индекс GIC	Рэнкинг на глобальном уровне	Рэнкинг среди стран СНГ	Правовые меры	Технические меры	Организационные меры	Развитие потенциала	Сотрудничество
Российская Федерация	98,06	5	1	20,00	19,08	8,98	20,00	20,00
Беларусь	50,57	89	5	10,36	9,50	8,31	7,88	14,51
Казахстан	93,15	31	2	20,00	19,54	18,46	15,15	20,00
Армения	50,47	90	6	12,87	13,86	4,87	7,85	11,02
Узбекистан	71,11	70	4	19,27	12,56	10,05	15,68	13,56
Киргизская Республика	49,64	92	7	13,43	7,85	14,37	1,87	12,11

Разработано автором на основе [6].

Узбекистан занял 70-е место, индекс Узбекистана составил 71,11 балла из максимальных 100. В частности, Узбекистан получил 19,27 балла в сегменте правовых мер, 10,05 балла – в сегменте организационных мер, 12,56 балла – в сегменте технических мер, 15,68 балла – в сегменте по развитию потенциала и 13,56 бал-

ла – в сегменте сотрудничества. За три года Узбекистан значительно улучшил свою позицию в рейтинге стран по уровню кибербезопасности, поднявшись с 92-го (2017 г.) на 70-е (2020 г.) место. Однако по показателям технических и организационных мер и партнерству в области кибербезопасности страна немного отстает, и необходимо улучшить данные показатели, направленные на обеспечение информационной безопасности.

В силу своей специфики лишь принятия и осуществления национальных законов недостаточно для решения современных проблем кибербезопасности. Транснациональный характер киберпреступлений требует эффективного решения проблемы кибербезопасности с налаживанием партнерских отношений между государственным и частным секторами, а также международного сотрудничества с созданием единой нормативной базы, которая должна выполнять роль ключевого компонента стратегий по обеспечению кибербезопасности.

Таким образом, в настоящее время в Узбекистане действуют законы о кибербезопасности, и государственные центры работают над регулированием этой сферы. Современная тенденция развития требует необходимости создания центров кибербезопасности на сетевой основе. Кроме того, необходимо дальнейшее изучение данной области с правовой точки зрения, разработка стандартов кибербезопасности для организаций, а также разработка национальных программ кибербезопасности и стандартов показателей кибербезопасности. По этой причине совершенствование норм Гражданского, Налогового кодексов и других нормативно-правовых документов Республики Узбекистан требует учета процессов цифровой экономики.

Список литературы

1. Chuck Brooks Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. 2022. URL: https://www.forbes.com/

2. Гафуров К. Роль диджитализации в образовании при подготовке юристов и политика Узбекистана в борьбе с киберпреступлениями // Журнал правовых исследований. 2020. № 10. С. 39–46.

3. Ookla: Internet speed in Uzbekistan is getting even worse Интернет-издание kun.uz от 22.11.2018. URL: https://m.kun.uz/en/news/2018/11/22/

4. Блэкаут 25 января начался с Узбекистана – межгосударственная комиссия // Spot. 16.03.2022. URL: https://www.spot.uz/ru/2022/03/16/blackout-start/

5. Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/

6. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-c