Для укрепления институциональной базы МСП правительство также ставит задачей конкретно на 2022 г. изменить подходы к определению субъектного состава сектора МСП: уточнить критерии отнесения к субъектам МСП «с учетом передового международного опыта». Для этого в текущем году будет разработан проект об изменении Закона от 01.07.2010 № 148-З «О поддержке малого и среднего предпринимательства».

Как известно, главным критерием отнесения к субъектам МСП в соответствии со ст. 3 данного Закона является численность работников. Вместе с тем в зарубежных странах применяются такие критерии, как размер годового оборота (дохода), стоимость активов, объем складочного капитала и другое.

В 2022 г. также должен быть не только разработан, но и введен индекс административной нагрузки на бизнес – как и ранее, путем внесения изменений в правовые акты, которые регулируют вопросы ведения предпринимательской деятельности в стране. Примечательно, что в последующем эта нагрузка на бизнес должна планомерно снижаться.

Еще одной задачей, которая обозначена в государственной программе, является стимулирование деловой инициативы, обучение навыкам предпринимательства и его популяризация.

Для выполнения этой задачи конкретно в 2022 г. будут разработаны интенсивные обучающие программы о налогообложении в Беларуси для субъектов МСП. Заказчиком мероприятия выступает Академия управления при Президенте.

Таким образом, в Республике Беларусь существует ряд проблем и барьеров развития предпринимательства, но, с другой стороны, некоторые важные шаги, необходимые для стимулирования развития и создания благоприятных условий, уже сделаны. Главное на этом пути – достаточная реализация установленных мер и мероприятий, а также дальнейшее развитие деловой инициативы и содействие предпринимательству.

Литература

1. Предпринимательство / Официальный сайт Министерства экономики Республики Беларусь. – Режим доступа: http://www.economy.gov.by/dadvfiles/002047_558173_dir4okt2012.pdf. Дата доступа: 06.03.2022
2. Программа социально-экономического развития Республики Беларусь на 2021–2025 годы. – Режим доступа: https://pravo.by/upload/docs/op/P32100292_1628024400.pdf. Дата доступа: 04.03.2022
3. О развитии предпринимательства. Декрет № 7 от 23 ноября 2017 г. – Режим доступа: https://president.gov.by/ru/documents/dekret-7-ot-23-nojabrja-2017-g-17533 Дата доступа: 01.03.2022

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ: ЭКОНОМИЧЕСКИЕ И СОЦИАЛЬНЫЕ АСПЕКТЫ

Д. А. Шпанькова

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель В. В. Клейман

Развитие современной экономики, основанной на использовании новейших цифровых технологий, создании новых материалов, анализе больших массивов данных, разработке новых систем управления, приводит к изменению принципов конкурентных отношений. Конкурентная борьба происходит не только за передел существую-

щих рынков, но и больше за формирование новых рынков товаров, услуг, технологий на базе новых цифровых платформ. В таких условиях цифровая экономика изменяет понимание и сущность экономической безопасности государства, бизнеса, частных лиц, порождает новые угрозы и риски для участников экономических процессов и связей.

Рост цифровой экономики вызывает определенные риски, связанные, в первую очередь, с интернет-угрозами. Стремительный рост количества киберпреступлений в совокупности с утечкой информации наносят значительный ущерб, что приводит к необходимости инвестирования в информационную безопасность. Имеет место отвлечение финансовых ресурсов из основной деятельности производителя [1].

Цифровая трансформация бизнес-процессов и технологий увеличивает расходы на информационную безопасность и инфраструктуру.

Значительные потери бизнеса последних лет связаны с распространением программ вымогателей, проникающих в компьютер и шифрующих важную информацию, чтобы впоследствии требовать выкуп за ее восстановление. Согласно данным компании «Лаборатория Касперского», в 2016 г. каждая пятая компания в мире столкнулась как минимум с одним аналогичным инцидентом. При этом около 70 % жертв таких программ полностью или частично потеряли свои корпоративные данные, у 20 % жертв на попытки восстановления доступа к данным ушло несколько недель. Более 30 % атакованных компаний заплатили выкуп, однако при этом каждый пятый плательщик так и не смог восстановить свои данные после оплаты. К примеру, жертвами самой громкой атаки вируса под названием WannaCry в 2017 г. стали более 300 тыс. пользователей компьютеров в 150 странах мира [2].

В соответствии с результатами исследования, специализирующегося на компьютерной и сетевой безопасности британского ресурса Comparitech, Беларусь вошла в число стран с наиболее серьезными проблемами в вопросах кибербезопасности. В десятке стран с худшими показателями кибербезопасности Беларусь заняла 8-е место. Экспертами отмечена крайне высокая вероятность заражения вредоносным ПО смартфонов и компьютеров белорусских пользователей – 9,33 % вероятности и 31,1 %, соответственно. При этом соседи нашей страны, за исключением Украины (у нее десятое место), оказались на лучших позициях. Латвия оказалась на 31-м месте, Россия на 38, а Польша – на 40. Наиболее безопасной в этом плане страной была признана Япония. Рейтинг составлялся посредством оценки нескольких ключевых критериев, среди которых были: подсчет процента зараженных вредоносным ПО смартфонов, компьютеров; количество атак, направленных на хищение денежных средств с банковских счетов пользователей; вероятность атак с целью принуждения пользователей к загрузке вредоносного ПО, атак со стороны криптомайнеров, а также оценка наличия необходимой законодательной базы [3].

В Беларуси 18 марта 2019 г. постановлением № 1 утверждена Концепция информационной безопасности Республики Беларусь.

В качестве перспективного механизма обеспечения кибербезопасности предусматривается создание единой системы мониторинга белорусского сегмента интернета, которая объединит в себе национальный центр и сеть ведомственных (отраслевых) центров выявления и противодействия угрозам и инцидентам информационной безопасности (SOC – Security Operation Center).

Одновременно предполагается формирование облачной платформы для предоставления государственному сектору и бизнес-сообществу комплексных сервисов информационной безопасности с целью автоматизированного учета киберинциден-

тов и оперативного обмена информацией о них между уполномоченными государственными органами, операторами электросвязи и командами быстрого реагирования на компьютерные инциденты (CERT/CSIRT).

Главной задачей центров выявления и противодействия угрозам и инцидентам информационной безопасности будет постоянный мониторинг информационных систем и ресурсов, выявление и пресечение кибервоздействий. В настоящий момент работа по созданию одного из таких центров проводится РУП «НЦЭУ», которое в перспективе может стать базисом «национального SOC». Основу ведомственных (отраслевых) центров составят уже созданные в стране информационные системы, функционирующие в РУП «Белтелеком», FinCERT Национального банка и другие.

Ожидается, что в результате работы этих центров будет выявляться значительное количество технической информации, содержащей ключевые признаки вредоносного воздействия на информационные системы и ресурсы. В перспективе на основе накапливаемых данных возможно перейти к созданию функционирующего в онлайн-режиме Национального реестра (службы) оценки репутации IP-адресов и DNS-имен, предоставляющего поставщикам интернет-услуг сведения о признаках и источниках кибервоздействий [4]. Основу кибербезопасности составляют три процесса, представленные на рис. 1.

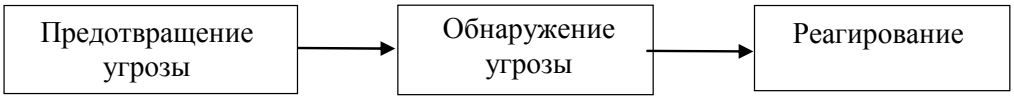

Рис. 1. Процессы кибербезопасности

Направление развития информационных технологий неразрывно связано с образованием граждан, развитием человеческих ресурсов.

Можно выделить еще один вид риска – риск снижения профессионального мастерства. На стадии внедрения цифровой экономики окажется «невыгодно» быть профессионалом в своей области деятельности, так как старые профессии будут отмирать и в течение активной трудовой жизни человек будет вынужден несколько раз сменить профессию.

Помимо очевидных выгод, цифровая экономика несет с собой и очевидные вызовы и угрозы, которые напрямую связаны с ее особенностями и характеристиками. Так, например, расширение спектра и индивидуализация цифровых услуг ведут к тому, что контроль в области цифровых сервисов снижается, а возможности для мошенничества увеличиваются. Значительно повышаются риски утечек информации, что требует повышения уровня защиты, выделения дополнительных инвестиций в информационную безопасность.

Цифровая экономика также открывает новые возможности для коррупционеров, которые могут пользоваться материальными благами анонимно, не раскрывая своей личности, используя логины, пароли, ники и коды. Выявить коррупционера и наказать его представляется возможным только в том случае, если удастся организовать постоянное и непрерывное наблюдение за его действиями и идентификацией совершенных им расходов с его личностью.

Таким образом, цифровая экономика на первой стадии внедрения и освоения больше порождает проблемы, чем их решает. Однако уклониться от этого не удастся и более того, мы не сможем уклониться, иначе интеллектуальный и технический прогресс не позволит двигаться вперед. Значит, надо предвидеть риски, к ним следует готовиться, минимизировать и по возможности избегать.

Литература

1. Горулев, Д. А. Экономическая безопасность в условиях цифровой экономики / Д. А. Горулев / Технико-технологические проблемы сервиса. – 2018. – № 1 (43). – С. 77–84.
2. Риски цифровой экономики // Экономика в деталях. – Режим доступа: https://popecon.ru. – Дата доступа: 20.04.2022.
3. Беларусь вошла в десятку наиболее проблемных в сфере кибербезопасности стран мира // Финансовый директор. – Режим доступа: https://findirector.by/news/belarus-voshla-vdesyatku-naibolee-problemnykh-v-sfere-kiberbezopasnosti-stran-mira-/. – Дата доступа: 01.04.2022.
4. Облако, репутация IP-адресов и киберриски. Концепция информбезопасности Беларуси с технической стороны // Онлайнер. – Режим доступа: https://tech.onliner.by/2019/03/13/koncepciya. – Дата доступа: 25.04.2022.