Криворотова Влада Андреевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, vlada.krivorotova@mail.ru

Туровинина Мария Сергеевна

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, turovinina.mariya@mail.ru

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Аннотация. Статья посвящена исследованию влияния цифровизации на экономическую безопасность хозяйствующего субъекта. Цифровизация, как деятельность по распространению и использованию цифровых технологий, является основным направлением экономики 21 века и становится двигателем хозяйствующих субъектов, так как позволяет им продвинуться на новый уровень эффективности деятельности. Цифровые технологии помогают исследовать самые частые угрозы, которые возникают в хозяйствующем субъекте, что увеличивает вероятность предвидения внутренних и внешних угроз. Однако, использование цифровых технологий неоднозначно влияет на корпоративную безопасность, что требует разработки новых направлений обеспечения экономической безопасности хозяйствующего субъекта. В статье представлены самые распространенные угрозы, связанные с цифровизацией хозяйствующего субъекта.

Ключевые слова: экономическая безопасность, цифровизация, угрозы, обеспечение экономической безопасности.

Krivorotova Vlada Andreyevna

Student of the specialty "Economic security" of the Tyumen state University, Tyumen, vlada.krivorotova@mail.ru

Turovinina Maria Sergeevna

Student of the specialty "Economic security" of the Tyumen state University, Tyumen, turovinina.mariya@mail.ru

THE IMPACT OF DIGITALIZATION ON THE ECONOMIC SECURITY OF AN ECONOMIC ENTITY

Abstract. The article is devoted to the study of the impact of digitalization on the economic security of an economic entity. Digitalization, as an activity for the dissemination and use of digital technologies, is the main direction of the economy of the 21st century and becomes the engine of economic entities, as it allows them to move to a new level of efficiency. Digital technologies help to investigate the most frequent threats that occur in an economic entity, which increases the likelihood of anticipating internal and external threats. However, the use of digital technologies has an ambiguous effect on corporate security, which requires the development of new directions for ensuring the economic security of an economic entity. The article presents the most common threats associated with the digitalization of an economic entity.

Keywords: economic security, digitalization, threats, ensuring economic security.

На протяжении нескольких лет термин «цифровизация» используется учеными и практиками, несмотря на отсутствие законодательно закрепленного понятия данному термину. В большинстве своем под определением «цифровизация» подразумевается деятельность, благодаря которой распространяются и используются цифровые технологии, а также продукты и услуги с ними связанные. Цифровизация, это, скорее, подход к использованию цифровых ресурсов для преобразования работы организации или процесс перехода на новые модели бизнес-процессов, основанные на цифровых технологиях. Сами же цифровые технологии направлены на сбор, обработку и поиск информации в электронном виде, с бумажным носителем или без, что и объясняет применения к ним понятия информационные технологии. Цифровые технологии стали повседневной частью жизни физических и юридических лиц, а значит неразрывно связаны с экономикой.

Цифровизация бизнеса позволяет увеличить эффективность деятельности хозяйствующего субъекта: организовать оперативную работу, усилить мощность оборудования, сократить расходы. Так, основные производственные фонды всех промышленных предприятий – оборудования, подвержены поломкам, которые, в свою очередь, требуют определенных затрат и времени, и денег. Для того, чтобы повысить оперативность работы производственного оборудования, компания «Сименс» (Siemens) разработала виртуальный тренировочный модуль для своего программного обеспечениям Comos. Так, при помощи очков виртуальной реальности инструкции по ремонту оборудования (порядок замены отдельных деталей) проецируется в режиме реального времени прямо на конкретное производственное оборудование. Сотрудник получает подсказку – порядок замены тех или иных деталей. При помощи 3D-модели и очков дополненной реальности «модуль помогает персоналу справляться с экстренными ситуациями в режиме виртуальной симуляции. В этом виртуальном мире операторы учатся взаимодействовать с оборудованием

при помощи цифровой презентации, изменять параметры оборудования и отображать операционные показатели и инструкции по ремонту» [1]. Таким образом, сотрудник, обучившийся на виртуальном тренировочном модуле, в реальной ситуации поломки оборудования, будет готов принять своевременные решения по ремонту, тем самым сократив время простоя оборудования. И это всего лишь один пример того, как развитие и распространение цифровых технологий в организациях увеличивает результативность деятельности, а экономия текущих затратах на ремонт увеличивает прибыль организации и позволяет ей подняться на более высокий уровень. Цифровизация бизнеса открывает возможности для расширения производства тем, что возрастающая прибыльность и финансовая устойчивость привлекает новых инвесторов, которые, в свою очередь, могут предложить покорять «новые вершины» и расширить промышленность хозяйствующего субъекта.

Следует отметить, что в большинстве случаев «цифровая трансформация бизнеса, как правило, дает положительные результаты не сразу, а в долгосрочной перспективе, так как первоначальные инвестиции в технологические и связанные с ним изменения представляют собой колоссальные затраты, которые будут окупаться продолжительный период времени» [2]. При этом, цифровизация бизнеса не только некоторое благо, но и требование внешней среды, некий ускоритель, поднимающий компанию на новый уровень. Для предприятий, внедряющих новые технологии, главным приоритетом является поднятие своего имиджа, и клиентской базы. Увеличение территориальных возможностей через предоставление онлайн-предложений сопутствуют росту клиентской базы.

Цифровизация также влияет на конкурентоспособность предприятий и их маркетинговую составляющую. В современном мире уже почти каждый потребитель ждет мобильности от хозяйствующего субъекта. Это стало особенно актуально в период пандемии, когда все торговые точки и учреждения, были закрыты из-за введения режима самоизоляции. Быть клиентоориентированным и подстраиваться под цифровой прогресс в ногу с потребителем бизнесу помогают цифровые интернет-технологии. Именно возможность принимать заказы или предоставлять услуги через корпоративный интернет-сайт, помогла многим малым предприятиям избежать банкротства в период пандемии.

Цифровые технологии положительно влияют не только на финансовую, но и кадровую безопасность. Во-первых, замена сотрудников цифровыми технологиями, сама по себе решает задачу кадровой безопасности. Во-вторых, подбор кадров упрощен наличием информационных систем. Например, «программа КС Полибейс «Кадровое агентство», представляющая собой сетевой программный комплекс, является комплексной автоматизацией кадровых агентств и кадровых служб» [3], где любой работодатель может

найти для себя «проверенного» сотрудника. Однако, стоит отметить и отрицательное влияние цифрового прогресса на кадровую сферу – грядущий кадровый дефицит (так как нужны новые «цифровые» специалисты), нехватка квалифицированных специалистов (образование не успевает за запросами цифрового общества) и безработица (граждан, чьи профессии заменили цифровыми технологиями).

Передовые технологии несут за собой не только положительные качества, но и некоторые угрозы экономической безопасности хозяйствующего субъекта. Так, «цифровая трансформация бизнес-процессов увеличила расходы на информационную безопасность 48% опрошенных российских компаний» [4]. Из-за прогрессивности и распространения цифровизации в обществе увеличивается показатель преступности в данной сфере. Согласно статистическим данным, «в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4 % - это почти каждое 20 преступление. Если в 2017 году зарегистрировано 1 883 таких преступления (+ 7,7 %), то за первое полугодие 2018 г. – 1 233 (+ 3,4 %). Наибольшее их количество выявлялось в 2017 году в Удмуртской Республике (194), Республике Коми (132), Омской (75), Владимирской (66), Кировской (64), Волгоградской областях (60), городе Москва (60), Краснодарском крае (51). Раскрываемость данных преступлений составила 41,3 %» [5]. В связи с этим возникает вопрос о том, из-за чего чаще всего возникают угрозы безопасности бизнеса.

Распространенной угрозой информационной безопасности является утечка персональных данных организации. В большинстве случаях, виновниками являются сами сотрудники компании и только в малой степени виновато руководство, из-за невнимательности и халатного отношения к исполнению своих обязанностей. Не редко угрозу утечки информации создают законопослушные сотрудники, которые не думают о хищении важных данных компании. Пренебрежительное отношение к работе законопослушных сотрудников приводит к ущербу из-за неосознанной передачи секретной информации злоумышленникам. Нельзя исключать и возможность того, что сотрудник из-за любопытства откроет фишинговое письмо и внесет вирус на сервер компании, от такого никакая организация не защищена.

Одной из главных угроз экономической безопасности бизнеса считается сотрудники администрации компании, т.к. именно они являются самым действенным и незаметным орудием утечки информации организации. Подобное допускается в силу человеческого фактора – главы корпораций вверяют сотрудникам, которые долгое время работают к компании, полный доступ к конфиденциальным данным. Таковыми инсайдерами являются менеджеры, управляющие, которые занимаю высокие посты и пользуются своим

преимуществом, устанавливая различные программы и приложения и, тем самым, отсылая секретные материалы заинтересованным лицам со стороны, даже об этом не подозревая.

Еще один вид нарушителей безопасности, сопряженный с предыдущим – это сокращенный сотрудник. Этот тип работников, увольняясь, овладевает информацией, к которой имел доступ, и забирает с собой, используя данные не только для выгодных коммерческих сделок, но и для нанесения вреда компании. От предыдущего вида угроз, данный вид отличается тем, что информация «слита» намеренно.

Угроза информационной безопасности может исходить и от руководителя компании, желающего сэкономить на лицензионном программном обеспечении для компьютеров. Стоит помнить, что вредоносное нелицензионное программное обеспечение не дает гарантированной защиты от хакеров, которые желают похитить любыми способами сервисную информацию. Владелец такого программного обеспечения не будет получать обновлений и технической поддержки от производителя. Более того, к этой покупке прилагаются различного рода вирусы, которые могут причинить ущерб компьютерной безопасности организации.

Существует еще одна разновидность нарушителей информационной безопасности, которых обычно называют «кротами». Из самого названия очевидно, что подобные сотрудники, имея полный доступ, предумышленно похищают информацию и отдают конкурентам организации, как правило за денежное вознаграждение.

Информационные угрозы в условиях цифровизации становятся одним из наиболее опасных и трудновыявляемых. В этих условиях требуется создание и развитие на предприятиях специализированных подразделений по противостоянию угрозам исходящих от внешней и внутренней цифровой среды. Службам экономической безопасности не стоит опасаться внедрения цифровых технологий, но необходимо быть готовыми к последствиям их введения в финансово-хозяйственную деятельность. Всегда понятнее, когда используется в деятельности отечественное оборудование, так и с информационными технологиями – стоит развивать отечественный сектор данной отрасли. Следует поддерживать молодых специалистов, создавая условия для их плодотворной работы, тем самым не только инвестировать в новые технологии, создать благоприятную почву для предпринимательской активности, но и увеличивать приток новых сотрудников.

В заключение отметим, что цифровизация уже считается одним из главных двигателей экономики, так как позволяет увеличить эффективную работу хозяйствующего субъекта. Цифровые технологии положительно влияют на финансовую, технологическую и кадровую безопасность, создавая всевозможные «приложения», облегчающие задачу ведения бизнеса, но требуют престольного внимания к информационной безопасности. Несмотря на то, что

родоначальником угроз информационной безопасности называют человеческий фактор, обнаружить и доказать вину сотрудника, использовавшего цифровые технологии для передачи секретной информации злоумышленникам, непросто. Таким образом, цифровизация хозяйствующего субъекта стимулирует специалистов служб экономической безопасности к разработке мер предотвращения информационных рисков для обеспечения экономической безопасности бизнеса.

Библиографический список

1. Тарасов И. В. Технологии индустрии 4.0: влияние на повышение производительности промышленных компаний. 2018. С. 69-62. URL: https://cyberleninka.ru/article/n/tehnologii-industrii-4-0-vliyanie-na-povyshenie-proizvoditelnosti-promyshlennyh-kompaniy/viewer (дата обращения: 10.10.2020).

2. Гарифуллин Б. М., Зябриков В. В. Цифровая трансформация бизнеса: модели и алгоритмы. Москва. 2018. С. 1345-1358. URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-biznesa-modeli-i-algoritmy/viewer (дата обращения: 10.10.2020).

3. Мартынова М. Э., Камшилова С. Г. Цифровые технологии в управлении персоналом компании. Челябинск. 2019. С. 69-74. URL: https://cyberleninka.ru/article/n/tsifrovye-tehnologii-v-upravlenii-personalom-kompanii/viewer (дата обращения: 10.10.2020).

4. Коротеева М. А. Влияние цифровой экономики на финансовую безопасность. Барнаул. 2018. С. 56-61. URL: https://cyberleninka.ru/article/n/vliyanie-tsifrovoy-ekonomiki-na-finansovuyu-bezopasnost/viewer (дата обращения: 10.10.2020).

5. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Генеральная прокуратура Российской Федерации [https://genproc.gov.ru/]. Москва, 2018. URL: https://genproc.gov.ru/smi/news/genproc/news-1431104 (дата обращения: 10.10.2020).