

КИБЕРБЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКИХ ОРГАНИЗАЦИЙ: НЕОБХОДИМОСТЬ ВРЕМЕНИ

И. В. Мальгина

*кандидат экономических наук, доцент, доцент кафедры
государственной экономической политики, Академия управления
при Президенте Республики Беларусь, г. Минск, Республика Беларусь,
e-mail: irina_malgina@list.ru*

Статья посвящена рассмотрению роли кибербезопасности в развитии субъекта малого и среднего предпринимательства при формировании цифровой экономики. Современные процессы развития цифровой экономики требуют усиления кибербезопасности субъектов малого и среднего предпринимательства.

Ключевые слова: малое и среднее предпринимательство; цифровая экономика; кибербезопасность.

CYBER SECURITY OF BUSINESS ORGANIZATIONS: THE NEED OF TIME

I. V. Malgina

*PhD in economics, associate professor, associate professor
of the department of state economic policy, Academy of Public Administration
under the President of the Republic of Belarus, Minsk, Republic of Belarus,
e-mail: irina_malgina@list.ru*

The article is devoted to the consideration of the role of cybersecurity in the development of small and medium-sized businesses in the formation of the digital economy. Modern processes of development of the digital economy require strengthening the cybersecurity of small and medium-sized businesses.

Keywords: small and medium business; digital economy; cybersecurity.

Кибербезопасность – это самая важная безопасность, которую может иметь субъект малого и среднего предпринимательства (МСП) и она очень важна для любого бизнеса. Ни один субъект МСП не хочет стать жертвой кибератаки, поэтому роль кибербезопасности в организации чрезвычайно важна. При этом, кибербезопасность важна для всех предприятий и ее преимущества огромны не только для различных компаний, но и для их сотрудников. Так, только в 2017 г. канадские предприятия потратили 14 млрд долл. на кибербезопасность и по сути

каждая пятая канадская компания свидетельствовала, что пострадала от кибератаки [1]. Статистика показывает, что чем крупнее бизнес, тем больше он подвержен атаке [2]. Выяснилось, что компании со штатом 250 и более сотрудников более чем в два раза чаще становились объектами атак, чем компании со штатом от 10 до 49 сотрудников. И, конечно, чем крупнее компания, тем выше стоимость простоя, вызванного атакой. Учитывая, что среднее время простоя на компанию в 2017 г. оценивалось в 23 часа, денежная стоимость каждого часа простоя может быть разрушительной.

Важность кибербезопасности для бизнеса заключается не только в защите их информации, но и в информации их сотрудников и клиентов. Компании имеют много данных и информации о своих системах. Этот факт повышает важность безопасности, будь то безопасность данных, информационная безопасность или кибербезопасность в целом. Кража личных данных и утечка конфиденциальных документов стали серьезными проблемами, и во многих случаях их можно избежать.

Существует много последствий отсутствия кибербезопасности у субъекта МСП [2; 3].

Первая – экономическая, влечет за собой потерю финансовых средств в случае утечки конфиденциальных данных, что впоследствии может привести к еще большим последствиям. Это может быть интеллектуальная собственность, инсайдерская торговля или даже корпоративная информация, которая может вызвать всевозможные проблемы.

Вторая – репутационная, влечет за собой потерю доверия потребителей, клиентов и инвесторов в случае утечки их данных. Для возвращения доверия могут потребоваться годы, однако репутация субъекта МСП может сильно пострадать.

Третья – регулятивные расходы, влечет за собой возмещение ущерба сотрудникам субъекта МСП в случае утечки личной информации сотрудников субъекта МСП из организации и ее компрометации.

Обучение и информирование руководства и сотрудников субъекта МСП важно для любой компании. При этом, когда субъект МСП обучает всех своих сотрудников преимуществам кибербезопасности, сама компания в первую очередь меньше подвержена рискам кибербезопасности. Субъект МСП экономит деньги на потерях, связанных с кибербезопасностью, и серьезности инцидентов кибербезопасности, если предложит своим сотрудникам надлежащее обучение кибербезопасности. Еще одним преимуществом обучения сотрудников является экономия времени. Когда в субъекте МСП меньше угроз кибербезопасности, сотрудники тратят меньше времени на отслеживание проблемы, ее

исправление и, возможно, необходимость переделывать любую затронутую работу. Когда сотрудники должным образом обучены кибербезопасности, они развивают более позитивную корпоративную культуру в отношении кибербезопасности и информационной безопасности.

Библиографические ссылки

1. *Nobles C.* Botching human factors in cybersecurity in business organizations // HO-LISTICA – Journal of Business and Public Administration. 2018. Т. 9, № 3. P. 71–88.
2. *Moşteanu N. R.* Challenges for Organizational Structure and design as a result of digitalization and cybersecurity // The Business & Management Review. 2020. Т. 11, № 1. P. 278–286.
3. *Dawson M.* Applying a holistic cybersecurity framework for global IT organizations // Business Information Review. 2018. Т. 35, №. 2. P. 60–67.