Список использованных источников

1. Андреева, А.Н. Маркетинг роскоши: современные стратегии / А.Н. Андреева, Л.Н. Богомолова. – СПб.: Изд-во С.-Петербургского ун-та, 2008. – 336 с.
2. Березова, И.С. Анализ рынка товаров и услуг класса люкс в России / И.С. Березова, И.И. Тихомирова // Маркетинг и коммерциализация. – 2015. – №3. – С. 279-281.
3. Бодрийяр, Ж. Система вещей: [пер. с фр.] / Ж. Бодрийяр. – М.: Рудомино, 1995. – С. 47.
4. Веблен, Т. Теория праздного класса / Пер. с англ. — М.: Прогресс, 1984.
5. Зинчак, Е. В. Роскошь как объект исследования: разработка определения / Е.В. Зинчак // Управление экономическими системами. – 2013. – №12 (60).

Подготовлено в рамках исследований, выполняемых в СНИЛ «Поиск» УО БГЭУ

УДК 338.242.4

И.В. Мальгина
Академия управления при Президенте Республики Беларусь,
Минск, Беларусь

КИБЕРБЕЗОПАСНОСТЬ БИЗНЕСА: ЗАРУБЕЖНЫЙ ОПЫТ

Аннотация. *Тезисы посвящены рассмотрению государственных программ поддержки кибербезопасности бизнеса. Особое место в обеспечении кибербезопасности отводится органам государственного управления и университетам.*

I.V. Malgina
Academy of Public Administration under the aegis of the President
of the Republic of Belarus
Minsk, Belarus

BUSINESS CYBER SECURITY: FOREIGN EXPERIENCE

Annotation*. Theses are devoted to the consideration of government programs to support business cybersecurity. A special place in ensuring cybersecurity is given to government agencies and universities.*

Кибербезопасность бизнеса в новых реалиях имеет большую актуальность. В зарубежных странах имеются различные программы, способствующие кибербезопасности бизнеса и других организаций.

Так, штат Калифорния (США) является одним из немногих штатов, который требует от всех государственных служащих прохождения ежегодного обучения по кибербезопасности. Инициатива CyberCalifornia была создана в целях «помочь дальнейшему позиционированию Калифорнии как лидера в области кибербезопасности, связанной с коммерцией и технологией Интернета вещей (IoT)» [1]. Инициатива предназначена для содействия исследованиям и инновациям в области кибербезопасности. в штате; информировать калифорнийские предприятия о потребностях и ресурсах в области кибербезопасности; и соединить надежную систему развития рабочей силы Калифорнии с потребностями работодателей штата. Университет Южной Калифорнии открыл Центр безопасности компьютерных систем, который занимается изучением технологий безопасности, обеспечивающих конфиденциальность, целостность, отказоустойчивость, конфиденциальность, обнаружение и реагирование на кибератаки, а также живучесть критически важной инфраструктуры.

Выделено несколько направлений по кибербезопасности для малого и среднего предпринимательства в целях защиты бизнеса, клиентов и данных от растущих угроз кибербезопасности [2, 3]. Данные направления включают такие как: обучение сотрудников принципам безопасности (требование надежных паролей, правила использования Интернета и др.); защиту информации, компьютеров и корпоративной сети от кибератак (наличие антивирусного программного обеспечения, сканирование компьютера после обновления программного обеспечения); обеспечение безопасности интернет-соединения (наличие брандмауэра); план действий для мобильных устройств (защита паролем, установка приложений безопасности); резервные копии бизнес-данных и информации (сохранение резервных копий, хранение копий вне офиса или в облаке); создание учетной записи для каждого сотрудника (предотвращение доступа неавторизованным лицам, надежные пароли, предоставление доступа ИТ-персоналу).

Деятельность органов государственного управления и различных университетов должна быть направлена на способствование обеспечению кибербезопасности бизнеса, что включает как создание программного обеспечения, так и обучение основам кибербезопасности. Создание специальных программ обучения на

различных уровнях образования, финансирование различных программ по кибербезопасности бизнеса.

Список использованных источников

1. Cybercalifornia [Электронный ресурс]. – Режим доступа: http://cybercalifornia.biz/ - Дата доступа: 05.11.2023.
2. Bada, M. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs) / M. Bada, J. R. C. Nurse // Information & Computer Security. – 2019. – Т. 27. – № 3. – P. 393-410.
3. Tam, T. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses / T. Tam, A. Rao, J. Hall // Computers & Security. – 2021. – Т. 109. – P. 102385.

УДК 331.101.52, 377.6

О.Г. Матвеева[1], Д.С. Русаков[2]

[1] Санкт-Петербургский институт экономики и управления

[2] Санкт-Петербургский государственный лесотехнический университет имени С.М. Кирова

Санкт-Петербург, Россия

К ВОПРОСУ О ПРОЦЕДУРЕ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА КАК ИНСТРУМЕНТУ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В РАМКАХ СТРУКТУРНОЙ ПЕРЕСТРОЙКИ ПОДГОТОВКИ КАДРОВ

Аннотация. *Процедура демонстрационного экзамена, один из инструментов, механизмов процедуры государственной итоговой аттестации. Эта процедура приобретает все большее значение в системе подготовки специалистов среднего звена. Данная работа затрагивает аспекты процесса внедрения процедуры демонстрационного экзамена в рамках государственной итоговой аттестации.*

O.G. Matveeva[1], D.S. Rusakov[2]

[1]St. Petersburg Institute of Economics and Management

[2]St. Petersburg State Forestry University

St. Petersburg, Russia

ON THE QUESTION OF THE PROCEDURE OF DEMONSTRATION EXAMINATION AS AN INSTRUMENT FOR STATE FINAL CERTIFICATION WITHIN THE FRAMEWORK