**Готовность российских компаний к киберугрозам**

Дорогие коллеги!

Рады представить Вам исследование готовности российских компаний к киберугрозам, подготовленное ООО "Высшая Школа образования" для целей исследования готовности крупных российских компаний к киберугрозам.

Данные

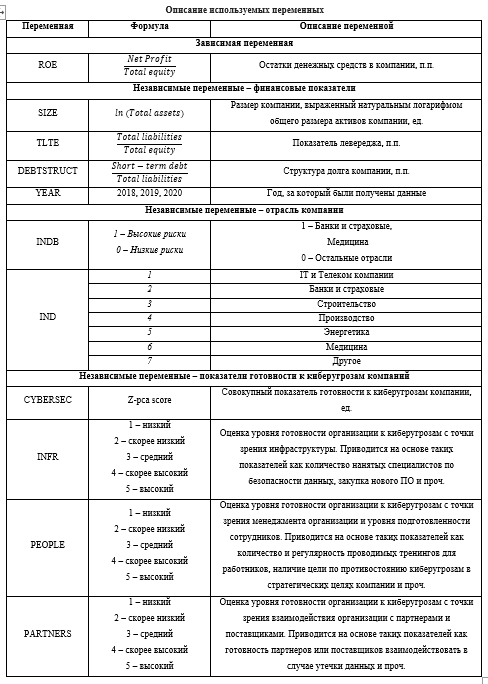
Данные представлены в виде 1146 наблюдений за 3 года с 2018 по 2020 гг. для 382 российских компаний из отраслей IT-Telecom, финансов (банки, страховые компании), строительства, производства, энергетики, медицины и других. Данные представлены в панельном виде и подразумевают панельный анализ.

Показатель совокупной способности противодействия киберугрозам (CYBERSEC) изначально собран из данных промежуточного, более широкого опросника, а потом агрегированы по пунктам (Z-pca score), предложенным ниже:

1. Показатель INFR. Организация обладает достаточным уровнем IT-инфраструктуры для противостояния киберугрозам (Осуществлялись ли инвестиции в проекты, направленные на предотвращение киберугроз, нанято достаточно IT-профессионалов, используется обновленное ПО и тд) (от 1 до 5).
2. Показатель PEOPLE Менеджмент организации уделяет достаточное внимание вопросам кибербезопасности (Данная цель включена в приоритетные стратегические цели компании, внедряются и обновляются практики по обеспечению кибербезопасности и тд).Сотрудники организации обладают достаточным уровнем компетенции в вопросах кибербезопасности (регулярно проводятся тренинги, тренинги по вопросам кибер-безопасности доступны для сотрудников и тд) (от 1 до 5)
3. Показатель PARTNERS. Партнеры и поставщики организации будут сотрудничать с организацией в целях предотвращения и/или ликвидации инцидентов, связанных с киберугрозой (например, утечкой данных) (от 1 до 5)

С остальной информацией по исследованию можно ознакомиться в файле расшифровке переменных.

Ссылка на ресурс: <https://www.kaggle.com/datasets/stanislavkurovskiy/cybersecurity-russia2018-2020>

****