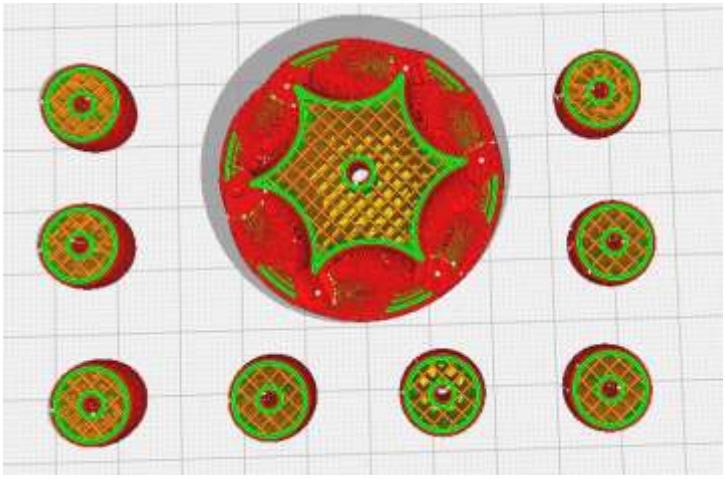

Fig. 3. 3D model of the Mecanum wheel layers

The FDM printing technology is very attractive for the automotive industry as well, building both prototypes and working models. Depending on the size and needs, you can change the filling of the model inside, as well as the strength of the walls, the height of the layer, etc. Thus, we can control the characteristics of our wheel by changing these parameters. By changing the type of plastic, we change the properties of the structure.

References:

1. US Patent No. US3876255A. Wheels for a stable self-propelled vehicle moving in any desired direction on the ground or other base URL: https://patents.google.com/patent/US3876255A/en
2. Mazzanti, V., Malagutti, L., & Mollica, F. (2019). FDM 3D printing of polymers containing natural fillers: A review of their mechanical properties. Polymers, 11(7), 1094.
3. Sood, A. K., Ohdar, R. K., & Mahapatra, S. S. (2012). Experimental investigation and empirical modelling of FDM process for compressive strength improvement. Journal of Advanced Research, 3(1), 81-90.
4. The 3D model of the wheel. *the Thingiverse.* URL: https://www.thingiverse.com/thing:2758771

WAYS OF MITIGATION DATA BREACHES FOR GLOBAL ENTERPRISE COMPANIES

DMYTRO MORHUL, PhD student
OLEKSIY P. NARIEZHNII, Associate Professor, PhD, Scientific Adviser
IULIIA I. SHAMAIEVA, Associate Professor, PhD in Philology, Language Adviser
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

Data breaches are a serious threat to enterprise companies as they can result in loss of sensitive information, reputational damage, and financial losses [2], which explicates the topicality of our work.

There are some practices have been recommended by various industry experts, government agencies, and cybersecurity organizations such as the National Institute of Standards and Technology (NIST), the Center for Internet Security (CIS), and the International Organization for Standardization (ISO)

Here are some ways we have come up with that enterprise companies in the global world can mitigate the risk of data breaches:

1. Conduct regular security assessments as regular security assessments can help identify vulnerabilities in the system and prevent data breaches
2. Implement a strong password policy that can help prevent unauthorized access to sensitive information. This includes requiring complex passwords, regular password changes, and multi-factor authentication.
3. Encrypt sensitive data since encryption can help protect sensitive data in case of a breach. This includes encrypting data at rest and in transit.
4. Implement access controls that can help limit access to sensitive data to only authorized personnel. This includes role-based access controls, network segmentation, and user activity monitoring.
5. Conduct employee training and awareness programs. Employees can be a weak link in the security chain. Conducting such training and awareness programs help them recognize security threats and take appropriate action.
6. Implement a data backup and recovery plan. A data backup and recovery plan can help mitigate the damage caused by a data breach. This includes regularly backing up data, testing backups, and having a plan in place to recover data in case of a breach.
7. Stay up to date with security patches and updates, whose regular application can help prevent vulnerabilities from being exploited.

Overall, a comprehensive approach to cybersecurity is needed to mitigate the risk of data breaches. This includes a combination of technical controls, employee training and awareness programs, and regular security assessments.

According to Verizon's 2022 Data Breach Investigations Report (DBIR), which analyzed data from 83 countries and over 29,000 incidents, 83% of the breaches analyzed were financially motivated, and 10% were espionage-related. The report also found that the top industries affected by data breaches were healthcare, public administration, and financial services. Additionally, the report found that most breaches (61%) involved credentials and involved the use of stolen/compromised credentials [1].

To sum up, mitigation of data breaches is highly important for enterprises as a data breach can have severe consequences that can affect the company's reputation and operations. The loss of sensitive information can lead to legal liabilities, customer trust, and damage to brand reputation. It can also result in financial losses, such as fines and penalties, as well as costs associated with remediation, investigation, and notification of affected individuals. Therefore, effective mitigation of data breaches is crucial to protect the company's assets, reputation, and long-term viability.

References:

1. Verizon.com, 2022 Data Breach Investigations Report, Available at https://www.verizon.com/business/resources/reports/dbir/

2. Murugiah Souppaya, Karen Scarfone, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology, Available at https://www.nist.gov/publications/guide-enterprise-patch-management-planning-preventive-maintenance-technology

APPLICATION OF ARTIFICIAL INTELLIGENCE IN INDUSTRY

ARSENIY NORKOV, student
YURIY V. PAKHOMOV, Associate Professor, Scientific Adviser
RADUL G. MAKOVIEI, Senior Teacher, Language Adviser
O. M. Beketov National University of Urban Economy in Kharkiv

Artificial intelligence (AI) refers to computer systems that can perform problem-solving and make decision tasks normally associated with human intelligence. These can include:

- Recognizing images and speech
- Making decisions
- Translating languages
- Providing recommendations
- And more…

AI applications range from consumer-oriented solutions (such as chatbots) to highly complex industrial use cases, like predicting the need for manufacturing equipment maintenance.

Artificial intelligence studies ways that machines can process information and make decisions without human intervention. There is popular opinion that the goal of AI is to mimic the way that humans think, but this isn't necessarily the case. On other hand, humans are much more efficient at performing certain tasks, AI aren't perfect. The best kind of AI is the kind that can think and make decisions rationally and accurately.

Probably the best example of this is that humans are not well prepared to process data that appear within large datasets. However, an AI can easily sort through sensor data of a manufacturing machine and pick out outliers in the data that clearly indicate that the machine will require maintenance in the next several weeks. AI can do this in a shortest time that a human would spend analyzing the data.

Integration AI into manufacturing

First, you must first identify which technologies execute specific types of activities, as well as their strengths and limits, before engaging with an AI program. For instance, some examples of artificial intelligence in business are, Robotic process automation, Natural Language Processing (NLP) and rule-based