goods increases or, conversely, decreases by N times, the line on the graph moves parallel closer or further from the origin of coordinates.

Also, an increase in prices by 2 times will be equivalent to a decrease in the buyer's income by 2 times. For example, let's say your budget is $60. You are going to buy tulips and peonies. The price of peonies is 4 dollars, and tulips are 2 dollars. You can either spend the entire amount on peonies, and then you will get 15 of them [=$60/4]. Or you can spend the entire amount on tulips, then the bouquet will have 30 flowers. The number of tulips is represented along the horizontal X-axis, and the number of peonies is represented along the vertical Y-axis. We now have two points on the budget line (0;15) and (30;0).

An attainable combination is any combination of two products that can be purchased using a given income. All items on or below the budget line are achievable. An unattainable combination is any combination of two products that cannot be purchased using a given income. All items above the budget line are unattainable [2].

LITERATURE

1. Electronic educational and methodological complex for the academic discipline "Fundamentals of Economics", 2002.

2. Baranovsky, S. I. Microeconomics: educational method. manual for university students studying economics. specialist. / S. I. Baranovsky. - Minsk: BSTU, 2007. – p.88

УДК 004.056

Student V.V. Ugorenko

Scientific supervisor, V.Y. Dokurno (Department of ICC&TT (Intercultural Communication and Technical Translation, BSTU)

CYBERSECURITY 2024-2025: TRENDS AND FORECASTS

In our digital age, cybersecurity has become a vital aspect of daily life. I chose this topic for my report due to its critical importance. Each year, cyber threats escalate, posing risks to organizations and individuals alike. My aim is to highlight current cybersecurity issues and challenges, providing practical tips to safeguard data and systems. I believe that raising awareness of online threats and prevention methods is crucial for digital security, and I am committed to sharing this knowledge with others.

In light of this, let's take a look at some of the most significant trends in cybersecurity that are expected in 2024:

1. Generative artificial intelligence and email security

AI technology is causing problems for organizations. Bad actors use it for sneakier phishing scams, sometimes pretending to be important peo-

ple. Experts warn that using AI with social media makes scams seem real, raising concerns about AI causing more damage in the future.

2. Password-free access practices

Biometric login methods like fingerprints or face scans are expected to replace regular passwords soon, making it harder for hackers to break into accounts. This shift should improve security against cyber threats.

3. Closer cooperation between cybersecurity managers, company directors and public organizations

Leaders will collaborate to improve security by optimizing budgets, prioritizing risks, and integrating IT with physical security. Involving stakeholders will be crucial to address internal threats effectively.

4. Advanced identity checks

Security experts predict increased collaboration among leaders to invest wisely in security and address urgent risks. They emphasize the importance of integrating digital and physical security to tackle internal threats effectively.

5. Wider adoption of proactive security tools and technologies

Invest in proactive tools to strengthen resilience and identify vulnerabilities early. Explore technologies like vulnerability management, attack surface control, and application security, along with effective penetration testing.

6. Additional rules for devices in the organization

More IoT regulations expected due to security concerns. Governments and regulators to impose stricter guidelines. Companies must follow cybersecurity rules, but handling new regulations uncertain, as many find it challenging.

7. The struggle of third-party manufacturers for security

Smaller companies with weaker security are easy targets for hackers, posing a threat to everyone. There's no simple fix for companies concerned about their partners' security.

8. Suppliers can influence cyber insurance policy

Cyber insurance may start evaluating suppliers' security. Unreliable suppliers could mean no insurance payment for ransomware attacks. Some worry about insurance companies having too much influence on how companies handle cyberattacks.

Conclusion

In 2024, cybersecurity will face new challenges as attackers use AI and other advanced tactics. But there's also hope with biometric security and proactive threat detection. To stay safe, companies need to keep up with these trends and quickly use the latest security tools. Being flexible and adaptable will be key to keeping data and finances safe in the long run.\