Cybersecurity Role in AI-Powered Digital Marketing

Vasyl Buhas[1], Ihor Ponomarenko[2], Natalia Buhas[1], and Hennadii Hulak[3]

[1] *Kyiv National University of Technologies and Design, 2 Mala Shyianovska str., Kyiv, 01011, Ukraine*
[2] *State University of Trade and Economics, 19 Kyoto str., Kyiv, 02156, Ukraine*
[3] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

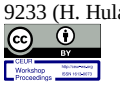
Abstract

Digitalization of human activity leads to a change in the types of economic activity and everyday behavior patterns of most consumers in the world. The development of innovative information technologies leads to the introduction to the market of qualitatively new products that are integrated into the Internet and are in high demand among modern users. The presence of a highly competitive environment encourages companies to identify ways of optimal development with the involvement of advanced approaches that will ensure high positions in the functioning market and form an economically justified demand for brand products from users. Achieving the presented tasks involves the use of modern marketing strategies in the digital environment. Thanks to the optimization of various digital marketing tools, it is possible to ensure long-term communications with the target audience and achieve a high level of loyalty among different groups of users. The use of modern web analytics tools allows generating information about various phenomena on the company's web resources. The development of server technologies makes it possible to accumulate large sets of heterogeneous data and process them thanks to the use of machine learning algorithms. The evolution of data processing methods, thanks to the use of various mathematical methods and models, has led to the widespread use of artificial intelligence in modern conditions. The effectiveness of artificial intelligence is explained by the ability to learn from large amounts of information and adapt the results of modeling to the changing influence of internal and external environmental factors. The above advantages led to the integration of artificial intelligence algorithms in digital marketing, which made it possible to ensure a qualitatively new level of digital tools implementation in the process of interaction with the target audience. Digital marketing communications led to the accumulation of various information about the company's activities and personal data of users, which involves the construction of a secure data storage system against the criminal actions of third parties. The approaches implemented in modern cybersecurity systems make it possible to reliably protect the information of all participants involved in marketing processes in the digital environment. The combination of digital marketing tools, artificial intelligence algorithms, and modern cybersecurity technologies allows to achieve a multiplicative effect in increasing the economic results of companies' activities.

Keywords

Artificial intelligence, communications, cybersecurity, data, digital marketing, optimization, target audience.

DECaT'2024: Digital Economy Concepts and Technologies, April 4, 2024, Kyiv, Ukraine
EMAIL: buhas.vv@knutd.edu.ua (V. Buhas); i.v.ponomarenko.stat@gmail.com (I. Ponomarenko); ncbugas@ukr.net (N. Buhas); h.hulak@kubg.edu.ua (H. Hulak)
ORCID: 0000-0001-8317-3350 (V. Buhas); 0000-0003-3532-8332 (I. Ponomarenko); 0000-0003-2457-1505 (N. Buhas); 0000-0001-9131-9233 (H. Hulak)



1. Introduction

In the modern world, the concept of big data, which is connected with the digitalization of global and national economic systems, has gained significant distribution [1]. Thanks to powerful servers and specialized software, companies have the opportunity to accumulate information about various processes within structural divisions. An important source of data is the Internet, since a large number of operations, including interaction with users, are carried out by companies on the global network. Information acts as a valuable resource that must be analyzed using modern machine learning algorithms and effective management decisions are formed based on the results obtained. Google Analytics 4 and other web analytics tools allow companies to accumulate large amounts of information based on a customized system of metrics, and the list of indicators may change due to changes in the internal and external environment of the company. Scientific and technical progress and increased competition stimulate the active development of digital marketing tools that allow to accumulation of new data and use the results of modeling based on large volumes of information for further qualitative improvement of strategies for interaction with the target audience. Opportunities to accumulate large volumes of heterogeneous information in the process of implementing marketing strategies in the digital environment provide companies with significant prospects for further development, along with this a complex of threats arises regarding the illegal use of data by third parties. The use of information by criminals to commit fraudulent activities can cause losses to the company and its customers, as well as lead to a deterioration of the image of the respective brand. To minimize the risks of illegal possession of information by criminals, the company must implement an effective data protection system. At the current stage of development, there is a large number of specialized cybersecurity systems that allow companies to resist threats of theft of personal data and information related to commercial secrets [2]. Cybersecurity technologies involve the use of a large number of algorithms, among which the following must first be noted: authentication and authorization, cryptographic protocols, threat detection methods, hash functions, digital signature, encryption, etc. When implementing information protection systems, it is expected to find the optimal ratio between the cost of digital security technologies and the obtained economic effect [3]. Excessive spending of monetary resources on the creation of a company's cybersecurity system may not correspond to the value of the data that the company owns, which will contribute to significant economic losses [4]. Integrating artificial intelligence into a company's digital marketing strategy allows companies to identify hidden relationships in the data and use the results to improve the company's performance. Along with this, it is possible to connect artificial intelligence with the company's cybersecurity system, which will make it possible to bring the data protection system to a qualitatively new level [5].

2. Related Works

Information protection systems are constantly being improved in connection with the use of new technologies by criminals to acquire private data. The presence of high demand for effective cybersecurity systems prompts scientists in different countries of the world to conduct comprehensive research to identify more effective approaches to the preservation of various user groups' data. The high technology of modern cybersecurity is based on scientific achievements in the field of information technology and data protection at various levels of processing and storage. Innovations in related fields are integrated into protection systems, which allows the identification of new directions of cybersecurity development and optimization of information flow processes at various levels of company functioning.

The work [6] reveals the essence of cybersecurity and the main directions of its implementation by companies in modern conditions. Based on the surveys, the author established the main strategies and characteristic differences that influenced the choice of the appropriate data protection system in each of the studied companies. It has been established that the preventive approach is used by the majority of companies when

building cybersecurity systems, and the second most popular is the protection methodology using preventive actions.

The work [7] is devoted to the combination of cybersecurity and artificial intelligence. The study revealed the features of generative artificial intelligence integration in the construction of effective cybersecurity systems. The authors present strategies for using artificial intelligence in the construction of defensive and offensive information protection strategies in modern conditions. The potential risks that may arise in connection with the use of ChatGPT by attackers in the process of implementing complex strategies for acquiring business information and personal data of interested persons have been identified.

The Internet acts as an important source of data for the company, and effective management decisions are formed based on the methods of intellectual information analysis. In this aspect, it is important to pay attention to the following article [8], which examines the features of the intellectual analysis application in cybersecurity. Thanks to the application of modern methods of researching large information arrays, effective systems for auditing and detecting intrusions into databases are being developed.

Features of the use of cybersecurity approaches in digital marketing are presented in the work [9]. The authors proved the effectiveness of implementing digital marketing strategies as an innovative direction of economic activity and the importance of ensuring the inviolability of generated data for fraudulent activities. Scientific research allows companies to conclude the importance of integrating modern cybersecurity technologies in the process of combating cybercrime. Research is planned to identify future data theft threats and develop preventive measures.

The work [10] reveals the features of providing private data in the Metauniverse. Scientists have proven the importance of a comprehensive analysis of immersion technologies, artificial intelligence, and blockchain, which are used for the effective functioning of the Metaverse. The use of effective systems for the protection of private information acts as an important prerequisite for increasing the level of customer loyalty to companies in the digital universe.

3. The Aim

The creation of an effective system for protecting the company's information at various levels is one of the important strategic tasks in today's conditions. Communications with users, partners, and competitors in the digital environment led to the formation of large volumes of specific information that can be used to optimize the company's strategy in the long term. The existence of threats of illegal acquisition of company information leads to the need to create an effective cybersecurity system that meets today's requirements and can quickly adapt to challenges and threats in future periods. Thanks to a comprehensive analysis of existing areas of information protection, it is possible to identify approaches that can be rationally used by the specifics of a particular company's activities and strategic goals, taking into account the cost of cybersecurity technologies and the economic efficiency of the implemented measures. A significant increase in the popularity of machine learning algorithms and artificial intelligence use involves conducting comprehensive research on the vectors of information protection technology development and obtaining a multiplier effect due to the joint use of these approaches. Identification of new methods of data processing and technologies for involving various objects in information exchange allows for improving cybersecurity systems. Thanks to the use of scientifically based approaches, the probability of developing more effective information protection systems that will minimize the risks of acquiring and using data for criminal purposes increases significantly. Among the applied directions, it is advisable to pay attention to digital marketing, because in the process of interaction with users, companies get access to a large amount of personal data on legal grounds. Ensuring ethical norms in marketing and maintaining a positive image of companies involves the application of advanced concepts in the field of cybersecurity. It is appropriate to evaluate the role of artificial intelligence in the implementation of marketing strategies as an important element of ensuring the integrity of the information space and countering cyber threats. Modeling various approaches to the construction of information protection systems allows to identification of

optimal solutions and the building of a real functioning system of countermeasures against the illegal acquisition of business information and personal data [11, 12].

4. Models and Methods

In the 21st century, cybersecurity systems have undergone significant transformations due to the intensive introduction of innovative information technologies. The growing demand for data protection systems in the digital environment encourages the continuous introduction of advanced algorithms for processing large amounts of information. Fig. 1 presents the main cybersecurity algorithms that are used in modern conditions in the construction of effective systems for countering illegal acquisition of private information.

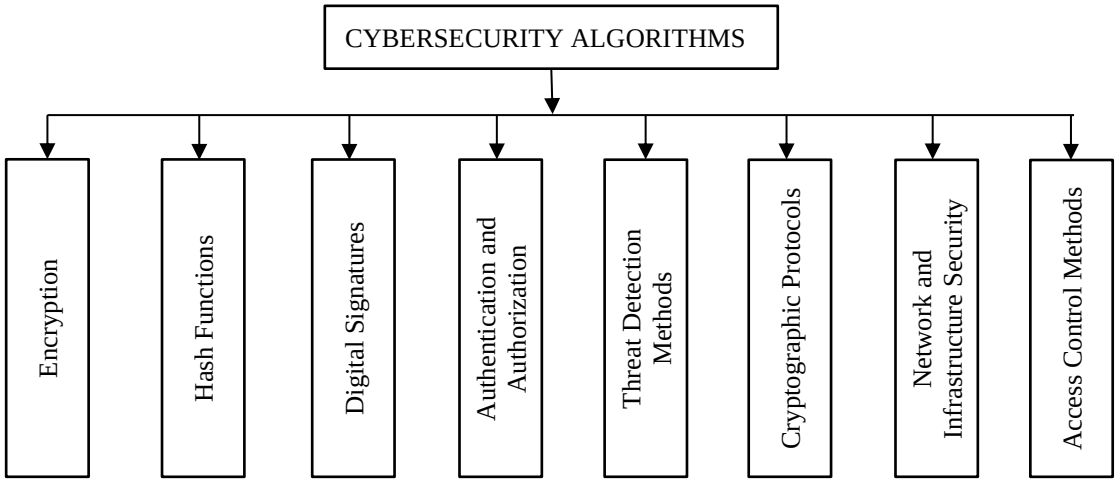


Figure 1: Basic cybersecurity algorithms [13, 14]

The effectiveness of cybersecurity algorithms explains their active use in the implementation of marketing strategies in the digital environment. The features of the main algorithms are disclosed below and the features of their use in digital marketing are given.

1. Encryption plays an important role in the company's data protection system, as it allows transforming information into an unreadable form for outsiders. The presence of special keys for decryption allows access to primary data only to authorized persons. The main types of transformation of information into an unreadable form are symmetric and asymmetric encryption [15].

Symmetric encryption involves the use of a single key for data encryption and decryption. The risk of the presented approach is the need to provide access to the key to at least two people, which leads to an increase in the probability of third parties taking possession of the decryption tool. Among the symmetric encryption algorithms, the most widely used include Advanced Encryption Standard (AES); Blowfish; Camellia; Data Encryption Standard (DES); International Data Encryption Algorithm (IDEA); Serpent; and Twofish.

Asymmetric encryption involves the use of public and private keys. The public key is used only to transform data into an unreadable form. The private key allows decryption of the transformed information by persons using the specified tool. This approach minimizes the risks of cybercriminals taking possession of the private key and using the obtained data to commit criminal acts. Asymmetric encryption algorithms include Diffie-Hellman Key Exchange, Digital Signature Algorithm (DSA), ElGamal, Elliptic Curve Cryptography (ECC), Lattice-Based Cryptography, Post-Quantum Cryptography (PQC), Rivest-Shamir-Adleman (RSA).

The use of modern cybersecurity approaches to data encryption in digital marketing allows companies to ensure the confidentiality of business information and personal data of users, the integrity of the company's information system, and helps to achieve a high level of trust among all participants. Payment tools, customer bank details and transactions integrated into marketing systems remain inaccessible to outsiders thanks to encryption. Encrypting e-mails minimizes the risk of personal data being accessed for fraudulent activities. Content

plays an important role in the implementation of marketing strategies in the digital environment, which in certain cases must be protected from unauthorized copying and distribution.

2. Hash functions allow to transformation of large amounts of information into short hash values with a specified length. The development of information technologies leads to the appearance of vulnerabilities in existing hash functions and the development of new, more secure hash functions that allow for a high level of big data protection. At the moment, the following hash functions are among the most popular: Message Digest Algorithm 5 (MD5), RACE Integrity Primitives Evaluation Message Digest (RIPEMD), Secure Hash Algorithm 1 (SHA-1), Secure Hash Algorithm 256-bit (SHA-256), Secure Hash Algorithm 3 (SHA-3), Whirlpool. The main areas of hash functions used in cybersecurity systems are:

- Data integrity check. Thanks to the use of hash functions, it is possible to identify the facts of data transformation in the process of transmission. The end consumer of the data has the opportunity to determine the hash value of the received data and conduct a comparative analysis with the sent hash.
- Password protection. The use of hash functions allows to storage of passwords in a secure form since the external system only contains a cache of a specific password. When the user enters a password, the hash for the specified combination of access characters is compared with the stored authentication cache. When implementing this approach, attackers do not have the opportunity to access the real password, and it is almost impossible to use a hash to generate an access code with correct characters.
- Protection of digital signatures. Digitization processes have led to the intensification of digital signatures used as an effective tool for certifying the authenticity of documents and messages. Using hash functions makes it possible to verify signed content by determining the hash for a specific document and comparing it using a public key to a template digital signature.
- Protection on servers. In the process of recording private information and keys on specialized servers, it is advisable to use hash functions for protection. In the case of illegal access to the servers, attackers will only be able to get hold of the hash values of the passwords, which have no value without decryption [16].
- Cryptographic protocols. This group of approaches involves the use of pseudo-random numbers and a system of additional parameters that allow generation hash functions with a high level of protection. Thanks to the use of cryptographic protocols, it is possible to implement highly effective cybersecurity systems for various participants in the economic environment.

The use of hash functions in digital marketing makes it possible to achieve a high level of information protection, including data integrity, inviolability of personal information, etc. The data obtained through the use of web analytics tools can be depersonalized by hashing methods. Information transformation makes it impossible to leak personal data and use it for fraudulent activities. Hash functions allow access to photo and video materials only to certain categories of consumers who have received the appropriate permissions.

3. Digital Signatures. The presented group of algorithms makes it possible to identify the originality of documents and establish cases of information replacement by intruders. The main algorithms include Digital Signature Algorithm (DSA), Edwards-curve Digital Signature Algorithm (EdDSA), Elliptic Curve Digital Signature Algorithm (ECDSA), Hash-based Message Authentication Code (HMAC), Multifactor Digital Signature Algorithms, Rivest-Shamir-Adleman (RSA).

The companies' implementation of complex marketing strategies in the digital environment includes the involvement of innovative technologies, among which machine learning algorithms, artificial intelligence, and cybersecurity are of great importance [17]. Fig. 2 shows the directions for using digital signatures in digital marketing as an effective cybersecurity tool for companies.

To interact with certain categories of users, it is advisable to use email marketing, which involves sending themed emails with text messages and specialized content. The use of

digital signatures allows for the transparency of communications between companies and users, making it impossible for cybercriminals to falsify official e-mails of respective brands during transmission.

The growth of Internet users in the conditions of digitalization stimulates the active development of various types of advertising. Thanks to the use of artificial intelligence, Internet advertising is shown to the target audience, which increases the efficiency of interaction between companies and users and allows for optimization of the conversion rate. There are many players in the online advertising market, which allows cybercriminals to create fake advertising messages to gain access to users' confidential information. Thanks to digital signatures, it is possible to authenticate advertising messages and identify criminal content. The use of digital signatures in Internet advertising allows to ensure the trust of advertising networks and other market participants.

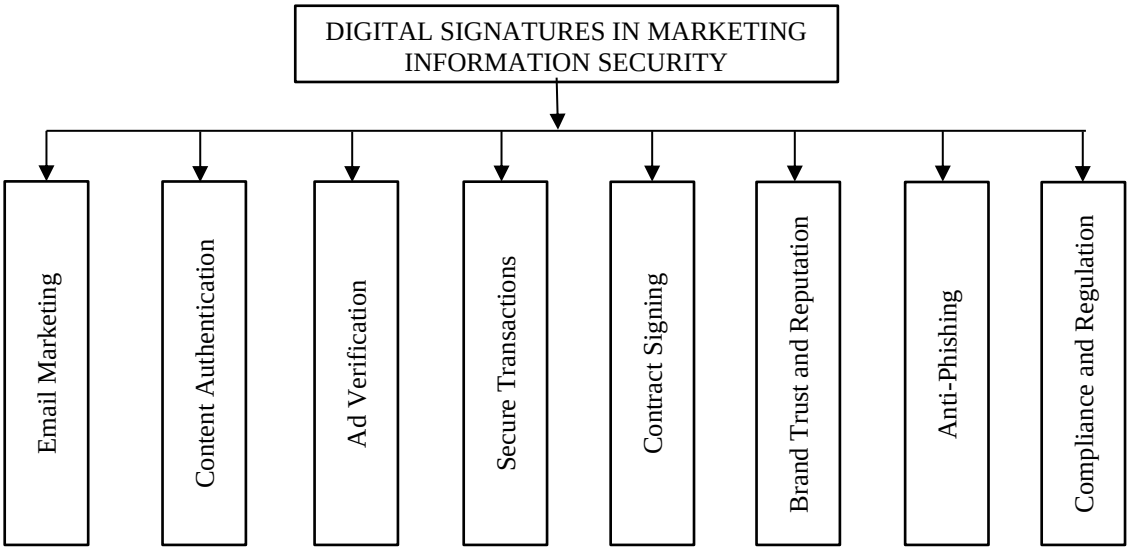


Figure 2: Using digital signatures in digital marketing [18]

Today's users, especially members of Generation Z and Alpha, are interested in learning new content regularly. To meet the existing demand, companies must post relevant photos, videos, audio, and text information on social media, which helps to retain the target audience. The creation of a complete and secure information environment for the company involves the provision of content authentication. Users have the opportunity to ensure their security in the digital environment by checking the presence of a digital signature on relevant content associated with a specific company. This approach is important because content generation in today's environment is becoming more accessible thanks to the use of artificial intelligence. Among the latest developments, it is advisable to pay attention to the image generation service based on the text description, into which Dall-E 3 and ChatGPT are integrated. The combination of Dall-E 3 and ChatGPT allows to creation of images containing the interaction of several complex visualized objects. Accordingly, attackers can create fake content that mimics the corporate style of certain brands.

Among the problems of modern digital marketing, when building an effective information protection system, it is necessary to pay attention to the phishing of web resources. Attackers impersonate legitimate participants in the exchange of personal data and illegally use passwords to access financial and personal information. Fig. 3 shows the main phishing methods.

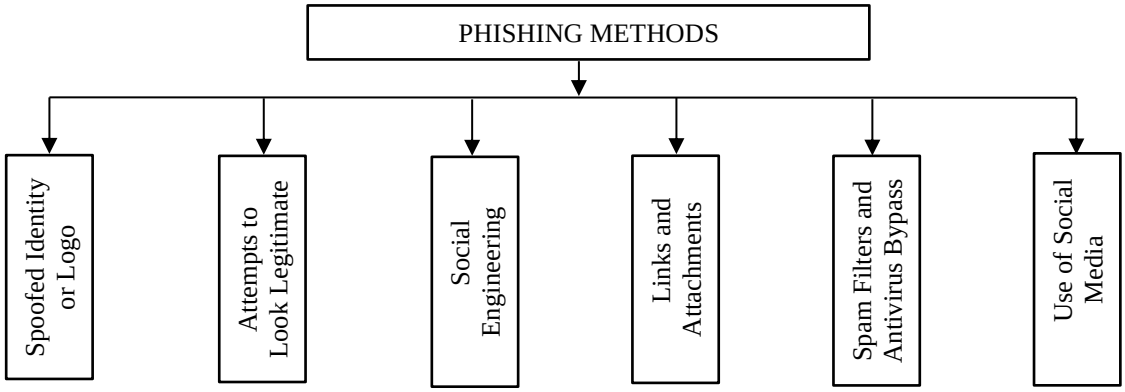


Figure 3: Methods of phishing [19]

4. Authentication and Authorization. In the digital environment, authentication systems based on machine learning algorithms, which replace outdated methods based on entering passwords and other symbolic information, are becoming more widespread. Currently, the following algorithms are used: Biometric Authentication; Certificate-Based Authentication; Kerberos; OAuth and OpenID Connect; Multi-Factor Authentication (MFA); Password-Based Authentication; Passwordless Authentication; Public Key Infrastructure (PKI); Single Sign-On (SSO); Smart Cards and PKCS#11; Token-Based Authentication. Artificial intelligence allows customers to use a person's face, voice, etc. as an identifier. The accuracy of machine learning algorithms and the uniqueness of the physiological characteristics of each user prevent unauthorized access to private information by outsiders.

The popularity of social networks among a large number of users forces companies to create complex strategies for interaction with the target audience in these media. By socio-economic, demographic, and psychological characteristics, different groups of users permanently use appropriate social networks for communications. To ensure the protection of accounts and personal data, social media users can use two-step authentication (Fig. 4). The presented approach involves the use of several digital channels for confirming the owner of an account on social media.

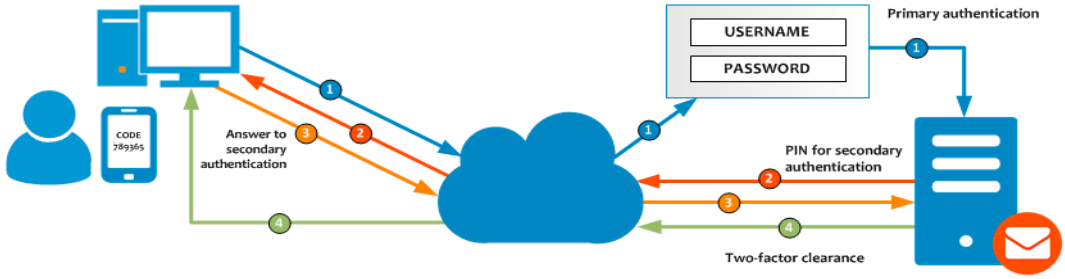


Figure 4: Two-step authentication [20]

The next stage is authorization, which represents the process of determining the level of authenticated persons' access to certain information. The different level of access rights to functionality and information is justified by a complex of factors, including the options of a certain digital product. For digital marketing tools, authentication is a very important feature, as it allows companies to create products with special rates that reveal a clearly defined set of capabilities to subscribers.

5. Threat Detection Methods. The study of large data arrays involves the use of various mathematical models to identify anomalous cases that differ in distribution indicators from the characteristics of the general population [21]. To detect abnormal or criminal actions, modern cybersecurity systems can use various algorithms:

- Signature-Based Detection. The presented method is implemented by comparing signatures from the existing database and performing operations. The high efficiency of threat identification is due to the presence of various digital threat description templates in the databases,

but there are risks of inefficiency in the case of threats with new technical characteristics.

- Anomaly-Based Detection. Within a certain system, a baseline of normal behavior with statistically reliable levels of deviation is established. Deviations outside the limits are identified as potential threats to the information environment. This approach can be used for known and new types of threats. The complexity of configuring Anomaly-Based Detection can lead to false identification of threats.
- Heuristic Analysis. To identify threats, rules, and algorithms are used, which are adjusted to scientifically based standards of behavior normality, which include expert assessments, historical data, and existing information system security criteria. The flexibility of the presented approach allows for the adaptation of the threat identification system to specific needs.
- Machine Learning and AI. The development of mathematical algorithms for processing big data and the appearance on the market of powerful servers for processing information contributed to the growing popularity of machine learning and artificial intelligence. The presence of many machine learning algorithms makes it possible to identify the optimal approaches for creating effective cybersecurity systems based on the specifics of individual enterprises' activities. The effectiveness of machine learning and artificial intelligence used in the field of cybersecurity is manifested in the rapid response to adaptive and complex cyber threats [22].

In digital marketing, machine learning and artificial intelligence algorithms have gained significant popularity, as they allow companies to increase the level of interaction with the target audience and optimize economic results. Along with this, the use of machine learning and artificial intelligence in the cybersecurity system of digital marketing allows achieving a high level of information protection related to commercial secrets and containing the personal data of customers. Fig. 5 presents the machine learning algorithms used to ensure digital marketing information security.

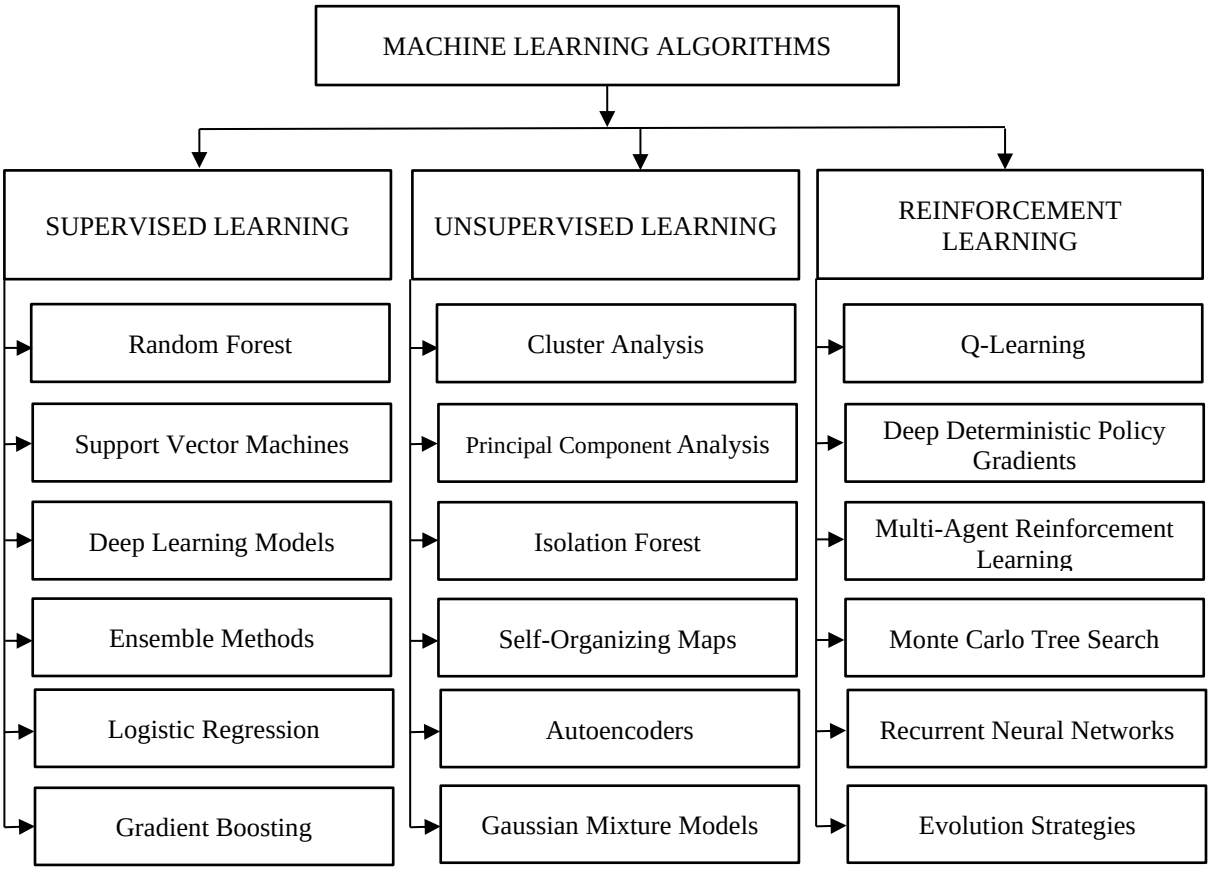


Figure 5: Machine learning algorithms in digital marketing cybersecurity [23, 24]

The presence of many machine learning algorithms allows us to test and create various systems for protecting the information environment of digital marketing. The main directions of using mathematical algorithms in this field are phishing detection, malware detection, intrusion detection, user and entity behavior analytics, ad fraud detection, sentiment analysis, anomaly detection, dimensionality reduction, network traffic analysis, content recommendation, behavior analysis, content clustering and tagging, botnet detection, dynamic network security, optimizing cybersecurity incident response strategies, user access control, optimizing ad placement strategies in digital marketing, recognize and respond to evolving attack patterns, etc.

6. Cryptographic Protocols. The presented technology is used to protect information transmitted over the Internet. Establishing secure interaction between systems in the digital environment is carried out through the use of special key exchange protocols. Modern cryptographic protocols include Hypertext Transfer Protocol Secure (HTTPS), Internet Protocol Security (IPsec), Open Authorization (OAuth), Pretty Good Privacy (PGP), Secure Sockets Layer/Transport Layer Security (SSL/TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME).

The use of cryptographic protocols in digital marketing makes it possible to achieve a high level of data confidentiality and authentication. The presented technology is used during interaction between users and web resources when receiving information during the implementation of advertising campaigns on the Internet [25].

7. Network and Infrastructure Security. This group includes algorithms used to identify and counter attacks in networks. The main algorithms are Firewall Algorithms, Honeypot and Deception Technology Algorithms, Intrusion Detection and Prevention Algorithms (IDPS), Intrusion Detection System (IDS) Signature-Based Algorithms, Virtual Private Network (VPN) Encryption Algorithms, etc. [26].

8. Access Control Methods. The presented methods enable different groups of users to access different information by the established rights. Modern algorithms include Adaptive Access Control, Attribute-Based Encryption (ABE), Biometric Access Control, Blockchain-Based Access Control, Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Single Sign-On (SSO), Time-of-Access Control, etc.

5. Further Research

The presented study reveals the specifics of implementing effective cybersecurity systems to protect information that is used to ensure the functioning of digital marketing strategies of various companies. Digitization processes contribute to the intensification of legal and illegal technologies development for processing large arrays of heterogeneous information. The integration of artificial intelligence into cybersecurity systems makes it possible to optimize the processes of combating illegal acquisition of information for fraudulent and criminal actions. Strengthening the interaction between companies and users in the digital environment through the use of advanced marketing tools involves the integration of advanced cybersecurity approaches based on artificial intelligence algorithms. Further scientific research involves determining the optimal methods of processing large amounts of marketing information using machine learning methods to ensure the protection of existing information. It is appropriate to pay attention to the features of the protection of visual content of companies, as artificial intelligence services for image creation are gaining popularity in the market, for example, a product with integrated Dall-E and ChatGPT.

6. Conclusion

Information protection is one of the priority tasks in all types of economic activity. Building an effective cyber protection system allows companies to ensure the inviolability of business data and personal information of users. Observance of trade secrets allows companies to gain advantages over competitors in the market, and reliable storage of customer information ensures a high level of mutual trust and a loyal attitude of the target audience. The emergence of new machine learning algorithms used by artificial intelligence stimulates the further development of cybersecurity systems. Artificial intelligence masters the elements of

creativity and can quickly respond to changes in internal and external environmental factors, which will contribute to increasing the effectiveness of the protection of information systems used by companies in the process of implementing marketing strategies in the digital environment.

References

[1] D. Virovets, et al., Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 182–190.

[2] V. Buhas, et al., Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188, no. 2 (2021) 273–281.

[3] S. Obushnyi, et al., Ensuring Data Security in the Peer-to-Peer Economic System of the DAO, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3187 (2021) 284–292.

[4] S. Obushnyi, et al., Autonomy of Economic Agents in Peer-to-Peer Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 125–133.

[5] M. Ansari, et al., The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. Int. J. Adv. Res. Comput. Commun. Eng. 11(9) (2022) 81–90. doi: 10.17148/ijarcce.2022.11912.

[6] D. Ghelani, Cybersecurity, Cyber Threats, Implications and Future Perspectives: A Review, Authorea Preprints (2022). doi: 10.22541/au.166385207.73483369/v1.

[7] M. Gupta, et al., From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy, IEEE Access 11 (2023). doi: 10.1109/ACCESS.2023.3300381.

[8] I. Salem, et al., Introduction to The Data Mining Techniques in Cybersecurity. Mesopotamian J. Cybersecur. 2022 (2022) 28–37. doi: 10.58496/MJCS/2022/004.

[9] S. Kumar, H. Pallathadka, L. Pallathadka, An Analysis of Cybersecurity Threats in Digital Marketing, J. Crit. Rev. 9(03) (2022) 85–94.

[10] M. Pooyandeh, K. Han, I. Sohn, Cybersecurity in the AI-Based Metaverse: A Survey, Appl. Sci. 12(24) (2022) 12993. doi: 10.3390/app122412993.

[11] R. Motoryn, et al., Evaluation of Regional Features of Electronic Commerce in Europe, Stat. J. IAOS 38(4) (2022) 1339–1347. doi: 10.3233/sji-220938.

[12] I. Gryshchenko, et al., Making Use of Competitive Advantages of a University Education Innovation Cluster in the Educational Services Market, European J. Sustainable Dev. 10(2) (2021) 336.

[13] C. Annamalai, Application of Factorial and Binomial Identities in Information, Cybersecurity and Machine Learning, Int. J. Adv. Netw. Appl. 14(1) (2022) 5258–5260. doi: 10.35444/ijana.2022.14103.

[14] M. Sewak, S. Sahay, H. Rathore, Deep Reinforcement Learning in the Advanced Cybersecurity Threat Detection and Protection, Inf. Syst. Front. 25(2) (2023) 589–611. doi: 10.1007/s10796-022-10333-x.

[15] R. Sharma, S. Dangi, P. Mishra, A Comprehensive Review on Encryption Based Open Source Cybersecurity Tools, 6th International Conference on Signal Processing, Computing and Control (ISPCC) (2021) 614–619. doi: 10.1109/ISPCC53510.2021.9609369.

[16] A. Ahmed, W. Ahmed, An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function Over Internet of Things, Sensors 19(17) (2019) 3663. doi: 10.3390/s19173663.

[17] A. Ahmed, O. Barukab, Unforgeable Digital Signature Integrated into Lightweight Encryption Based on Effective ECDH for Cybersecurity Mechanism in Internet of Things, Processes 10(12) (2022) 2631. doi: 10.3390/pr10122631.

[18] K. Rahman, Applications of Blockchain Technology for Digital Marketing: A

systematic Review, Blockchain Technol. Appl. Digi. Mark. (2021) 16–31. doi: 10.4018/978-1-7998-8081-3.ch002.
[19] E. Gualberto, et al., The Answer is in the Text: Multi-stage Methods for Phishing Detection Based on Feature Engineering, IEEE Access 8 (2020) 223529–223547. doi: 10.1109/ACCESS.2020.3043396.
[20] Zimbra Two-factor Authentication. URL: https://wiki.zimbra.com/wiki/Zimbra_Two-factor_authentication
[21] T. Chen, et al., System-Level Data Management for Endpoint Advanced Persistent Threat Detection: Issues, Challenges and Trends, Comput. Secur. 135 (2023) 103485. doi: 10.1016/j.cose.2023.103485.
[22] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.
[23] C. Kumar, T. Bharati, S. Prakash, Online Social Network Security: A comparative Review Using Machine Learning and Deep Learning, Neural Process. Lett. 53 (2021) 843–861. doi: 10.1007/s11063-020-10416-3.
[24] S. Pinto, P. Siano, M. Parente, Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection, Energ. 16(4) (2023) 1651. doi: 10.3390/en16041651.
[25] A. Aly, et al., Design of Symmetric-key Primitives for Advanced Cryptographic Protocols, IACR Trans. Symmetric Cryptol. 3 (2020) 1–45. doi: 10.13154/tosc.v2020.i3.1-45.
[26] T. AlMasri, M. Snober, A. Al-Haija, IDPS-SDN-ML: An Intrusion Detection and Prevention System Using Software-Defined Networks and Machine Learning, 1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS) (2022) 133–137. doi: 10.1109/APICS56469.2022.9918804.