ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.056.5 **doi: 10.32620/reks.2024.2.15**

Milana BOLATBEK, Gulshat BAISPAY*,
Shynar MUSSIRALIYEVA, Assel USMANOVA

Al-Farabi Kazakh National University, Almaty, Kazakhstan

A FRAMEWORK FOR DETECTING AND MITIGATING OF CYBER CRIMINAL ACTIVITIES USING UNIVERSITY NETWORKS IN KAZAKHSTAN

Abstract. *The increasing number of information security incidents in higher education underscores the urgent need for robust cybersecurity measures. This paper proposes a comprehensive framework designed to analyze the illegal use of internet resources in university networks in Kazakhstan. The* ***subject of this*** *article is the detection and mitigation of cybercriminal activities using university networks in Kazakhstan. The* ***goal*** *is to develop a comprehensive framework that integrates multiple educational organizations to enhance collaborative security efforts by monitoring network activity and categorizing texts using machine learning techniques. The* ***tasks*** *to be solved are: to formalize the procedure of integrating multiple educational organizations into a collaborative cybersecurity framework; developing a log analysis tool tailored for monitoring network activities within university networks; creating a novel dictionary of extremist terms in the Kazakh language for text categorization; to implement advanced machine learning models for network traffic classification. The* ***methods*** *used are: log analysis tools for real-time monitoring and anomaly detection in network activities, Natural language processing (NLP) techniques to develop a specialized dictionary of extremist terms in Kazakh, Machine learning models to classify network traffic and detect potential cyber threats, and collaborative architecture design to integrate network security efforts across multiple institutions. The following* ***results*** *were obtained: a comprehensive log analysis tool was developed and implemented, providing real-time monitoring of network activities in university networks; a dictionary of extremist terms in Kazakh was created, facilitating the categorization and analysis of texts related to potential security threats; advanced machine learning models were successfully applied to classify network traffic, enhancing the detection and mitigation of cyber threats; and an experimental architecture integrating multiple educational organizations was established, fostering collaborative efforts in cybersecurity.* ***Conclusions.*** *The scientific novelty of the results obtained is as follows: 1) a robust framework for collaborative cybersecurity in educational institutions was developed, leveraging log analysis and machine learning techniques; 2) the creation of a specialized dictionary of extremist terms in Kazakh significantly improved the accuracy of text categorization related to cybersecurity; 3) the application of advanced machine learning models to network traffic classification provided a methodological approach to effectively managing and securing network infrastructure effectively; 4) the experimental architecture demonstrated the potential for enhanced security through collaboration among educational organizations, offering strategic recommendations for improving information security in academic environments. The outcomes of this research contribute to the broader cybersecurity field by providing a structured approach to detecting and mitigating cyber threats in educational contexts. The proposed framework has potential applications extending to global security frameworks, aiming to foster a safer internet usage environment and reduce the risks associated with cyber threats and unauthorized data access.*

Keywords: *cybersecurity; higher education; network traffic classification; machine learning; Kazakhstan; internet security; log analysis; extremism detection.*

Introduction

Information security-related incidents in higher education are increasing. Unfortunately, few life-threatening games and applications claimed to be entertainment mediums by purpose turn out to be different. One such game is called Blue Whale (also transcribed as Siniy Kit) [1]. Siniy Kit is a game distributed through social networking sites like VK, in Russian-speaking world. In Siniy Kit a person writes a call, adding corresponding hashtags, and then game coordinators look for potential participant tags and offer them a game. It has been estimated that because of this game, many deaths occurred; to be precise more than 130 people who played the game were found dead.

Over the past ten years, terrorist groups have shifted their focus to the online realm. Currently, there are as many as 10,000 extremist websites [2]. Anti-Islam terrorist Anders Breivik used the Internet to learn about radical groups and, in July 2011, carried out bombings and shootings in Norway [3]. Another instance involves Zachary Chesser, a former high school student in north-

ern Virginia [4]. When he turned 18, Chesser began expressing support for Islamist terrorist organizations online, watching sermons by Anwar al-Awlaki, and corresponding via email with the cleric about potentially joining the Al-Shabaab militant group. Regrettably, in recent years, individuals from Kazakhstan have also joined extremist groups [5]. Therefore, there is an urgent need to implement automated monitoring of internet resources to detect extremist text messages.

In Kazakhstan, the recognition of extremist content is governed by several legislative acts. The primary legislation includes the Law on Counteracting Extremist Activities (2005), which outlines definitions, prevention measures, and penalties related to extremist content [6].

Additionally, the Criminal Code of the Republic of Kazakhstan includes specific articles (e.g., Article 174) that criminalize incitement of social, national, clan, racial, or religious discord [7].

The Law on Mass Media (1999) also played a role, regulating the dissemination of information and providing guidelines for media outlets to prevent the spread of extremist content. These laws collectively establish criteria for identifying and taking action against extremist materials. In our analysis, we ensured that the detection algorithms were aligned with these legal standards, thereby enhancing the system's relevance and compliance with national regulations [8].

Motivation. The increasing number of information security incidents in higher education underscores the urgent need for robust cybersecurity measures. Universities are often targeted due to their vast network of resources and valuable data, making it essential to develop effective frameworks to safeguard such institutions.

State of the Art. Current cybersecurity measures in university networks often lack integration and collaboration, leading to isolated and inefficient responses to threats. Existing solutions focus on individual network security, with limited emphasis on collaborative efforts and real-time monitoring across multiple institutions. This gap highlights the need for a comprehensive approach that leverages advanced technologies and collective resources.

By knowing the analytics of network traffic, IT departments can benefit by organizing security measures. The security measures can vary from simple source and destination block to application signature scanning. There are several types of threats in the higher education sector, including vulnerability to open attacks, software vulnerabilities, information leakage, network breakdowns, insecure wireless networks, and misuse of information by students and staff. Various security measures can be implemented depending on the type of threat. As mentioned earlier, we propose a framework for analyzing illegal use of Internet. We developed an experimental setup architecture to integrate various higher education organizations. The log analysis tool was developed to monitor and filter user accessed network resources. Then, the IT department can limit access to websites or resources, including but not limited to extremist forums and weapons trade websites.

In addition, we developed a dictionary of extremist terms, which will be employed in the future to categorize texts into "extremist" and "neutral" categories using machine learning methods. The proposed work is unique in that there is no dictionary of this type in Kazakh language.

The objective of this paper is to develop a comprehensive framework that integrates multiple educational organizations to enhance collaborative security efforts. The proposed framework focuses on monitoring network activity, categorizing texts using machine learning techniques, and implementing advanced models for network traffic classification. The aim of this research is to examine the societal security challenges within the higher education sector and compile a list of extremist keywords in the Kazakh language to help identify texts with extremist tendencies. This study applies a quantitative approach using frequency analysis. The data were collected over a 20-day period with approximately 6000 workstations, and the event data contained between 7 and 8 million events.

This research addresses the following issues:

1) develop a log analysis tool designed to monitor university network activity;

2) create a new dictionary of extremist terms in the Kazakh language to categorize the text;

3) implement advanced machine learning models to classify network traffic.

The article was written according to the following structure. In Section 1, "Literature review and problem statement", the paper begins with an in-depth examination of the current research landscape related to cybercriminal activities within university networks. It will: analyze existing literature on the prevalence and types of cyber threats faced by universities, with a focus on the context of Kazakhstan, review studies on detection and mitigation techniques used globally and locally, summarize the findings regarding the effectiveness of various cybersecurity measures and the specific challenges posed by cybercriminals targeting academic institutions.

The methodology used in this study is outlined in Section 2: "Materials and Methods of Research". This section details the methodology employed in the study, including the following: data acquisition processes, covering the sources of network data from Kazakhstani universities; preprocessing steps to prepare the data for analysis, such as cleaning and normalization techniques; statistical analysis methods and machine learning algorithms used for detecting and classifying cyber threats;

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

techniques for visualization and interpretation of the results to ensure clarity and comprehensibility.

Section 3, "Results and Discussion", presents the core findings of the research, focusing on: the types and frequencies of cyber threats identified within the university networks; the performance of different detection algorithms and their accuracy rates; a detailed analysis of specific case studies in which cybercriminal activities were successfully identified and mitigated. We also discuss the broader implications of the findings, including: the strategic insights gained from the study to enhance cybersecurity in university networks, potential areas for further research and development to address emerging threats, the role of policymaking and institutional support in strengthening cybersecurity frameworks in higher education.

The paper ends with the Conclusions section, which summarizes the key findings of the study and their contributions to the cybersecurity field, highlighting the novel insights gained from the research, particularly in the context of Kazakhstani universities, and offering final thoughts on the future direction of research and practical implementations in cybersecurity for educational institutions.

Literature review and problem statement

Anonymous networks, created to protect users' personal data, have become important tools for increasing network security and ensuring anonymity. However, they are also used for hostile activities and generating suspicious traffic. In this regard, the detection of traffic in anonymous networks has become a necessity to protect against unpredictable adversaries on the Internet. Many methods to identify anonymous traffic are based on machine learning; however, such methods often require complex architectures and specialized data sets. Due to the robustness of anonymous network traffic analysis and the lack of publicly available datasets, such methods may demonstrate low efficiency and performance in detecting anonymous traffic [9].

Feature-engineering methods are used to extract pattern information and rank the importance of features in static traces of anonymous traffic. To effectively use these template attributes, we developed a reinforcement learning system that includes four main components: states, actions, rewards, and state transitions. A lightweight system designed to classify anonymous and non-anonymous network traffic uses two fine-tuned thresholds rather than traditional labels in a binary classification system. The proposed system can detect anonymous network traffic without the need for data labels. The experimental results demonstrate that the proposed system can determine anonymous traffic with an accuracy of more than 80% based on template information.

In today's world, controlled by the Internet, there are many calls every day caused by a huge number of users. Effective detection of such attacks is a growing research area, primarily through intrusion detection systems (IDS). IDS play a key role in monitoring network traffic to detect malicious activity such as Denial of Service, Probe, and Remote-to-Local and User-to-Root attacks. Our research focused on evaluating various autoencoders to improve network intrusion detection. The selection of an autoencoder for network intrusion detection was driven by several key criteria. Autoencoders are known for their strong feature learning capabilities, which are crucial for detecting anomalies in high-dimensional network traffic data. When the dataset lacked extensive labeled data, the unsupervised learning nature of autoencoders provided a significant advantage by identifying patterns and deviations without needing labeled examples. Furthermore, autoencoders are scalable, which makes them suitable for real-time intrusion detection in large-scale network environments. Their effectiveness has been demonstrated in previous studies, demonstrating high accuracy and low false-positive rates in detecting network intrusions. We also considered the practical aspect of resource efficiency because autoencoders can be implemented with reasonable computational power. Collectively, these factors made autoencoders the optimal choice for our network intrusion detection system.

The proposed method — a sparse deep denoising autoencoder — performs dimensionality reduction, which is used for the prediction and classification of names in datasets. When training the autoencoder on normal network data, we used error reconstruction as an anomaly indicator. We tested the proposed method on standard datasets such as KDDCup99, NSL-KDD, UNSW-NB15, and NMITIDS. It is noteworthy that the proposed sparse deep denoising autoencoder achieved an accuracy of more than 96% based exclusively on error reconstruction. The primary goal of this study is to improve the detection of intrusions, achieving higher detection accuracy than existing methods [10].

Encrypted traffic is a key element in ensuring data security and privacy. It plays an important role in network protection by preventing attackers from intercepting confidential information that they may otherwise access without authorization. However, its effectiveness is largely dependent on the accurate application of classification methods that distinguish between legitimate user activities and malicious attempts within the network boundaries.

Encrypted network traffic is becoming increasingly common in modern communication systems, which presents challenges to effective network management and security. To address this issue, machine learning models have been employed to classify encrypted traffic; how-

ever, their success has been limited due to the lack of visibility into packet contents and the inability to inspect packet contents directly.

To overcome this problem, more effective research has been conducted on developing machine learning models to classify encrypted data without the need for direct content analysis. This study considers packet length, timestamps, and Transport Layer Security (TLS) information, as well as encrypted payload data, as input features for classification tasks instead of analyzing unencrypted packet contents, which is currently impossible due to technological constraints.

The evaluation process will focus on analyzing different model architectures and feature selection methods that yield better results than existing approaches. In this paper, we propose three methods to identify encrypted traffic and classify various applications, such as web browsing, VOIP, file transfer, and video streaming.

The first two methods involve two stages: the first stage employs either a neural network or bidirectional LSTM, and the second stage employs various classification techniques, namely Random Forest, Support Vector Machine, linear regression, and K-nearest neighbor. The final result is obtained using an ensemble voting technique. In the third method, network packets are grouped by source IP, destination IP, and session time before being fed into three different combinations of LSTM networks, either coupled with 1D or 2D convolutional layers or without them. As with the first two methods, the final result is obtained via ensemble voting.

An extensive comparison of the three approaches demonstrated that the first method achieved the highest accuracy. In terms of time complexity, the second and third methods outperformed the first. The accuracy values obtained by the proposed methods were 96.8%, 95.2%, and 96.5%, respectively [11].

Web attacks often target web applications because they are accessible over a network and frequently involve vulnerabilities. The success of an Intrusion Detection System (IDS) in detecting web attacks depends on an effective traffic classification system. Previous studies have employed machine learning methods to create efficient IDSs using various datasets for different types of attacks. This paper uses the IDS dataset from the Canadian Institute for Cybersecurity (CIC-IDS2017) to assess web attacks. It is important to note that this dataset contains 80 attributes of recent assaults, as reported in the 2016 McAfee report.

In this study, three machine learning algorithms were evaluated: Random Forests (RF), K-Nearest Neighbor (KNN), and Naive Bayes (NB). The primary goal of this study is to propose an effective machine learning algorithm for an IDS web attack model. The evaluation compares the performance of these three algorithms (RF, KNN, and NB) based on their accuracy and precision in detecting anomalous traffic.

The results demonstrate that the proposed RF outperformed both NB and KNN in terms of average accuracy achieved during the training phase. During the testing phase, the KNN algorithm outperformed the other algorithms, achieving an average accuracy of 99.4916%. However, RF and KNN algorithms achieved 100% average precision and recall compared to the other algorithms. RF and KNN algorithms were ultimately identified as the most effective for detecting web attacks using an IDS [12].

Social media provides modern individuals with a digital platform to express their ideas and mobilize communities—a power also utilized by extremists. Given the societal risks associated with the use of unvetted content moderation algorithms for detecting Extremism, Radicalization, and Hate speech (ERH), responsible software engineers must consider who, what, when, where, and why such models are necessary to protect user safety and freedom of expression. Therefore, we propose and explore the unique research field of ERH context mining to unify disparate studies.

This study evaluates the entire design process, from sociotechnical definition building and data collection strategies to the technical design of algorithms and their performance. Our systematic literature review (SLR) covering the period from 2015 to 2021, which includes 51 studies, presents the first cross-examination of textual, network, and visual approaches to detecting extremist affiliations, hateful content, and radicalization towards groups and movements. We identify consensus-driven definitions of ERH and propose solutions to existing ideological and geographic biases, particularly due to the lack of research in Oceania and Australasia. Our hybrid investigation of Natural Language Processing, Community Detection, and visual-text models demonstrated the superior performance of transformer-based textual algorithms [13].

The Australian Higher Education and Research Sector (HERS) must adopt digital resilience strategies to effectively address cybersecurity challenges and manage major crises. In this study, we developed a digital resilience framework to mitigate these cybersecurity issues. Our findings highlight a range of key factors for crisis management, such as implementing cybersecurity awareness programs, providing cybersecurity support, redefining roles and responsibilities, using risk management tools, partnering with external security organizations, introducing new policies, reconfiguring technologies, adopting new technologies, and evaluating current changes to address these issues. These key factors will help achieve digital resilience and significantly reduce cybersecurity problems in HERS, not only during the current crisis but also in the future. This research offers valuable theoretical and practical recommendations that

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

can be applied beyond the context of the recent crisis [14].

The UK National Cyber Security Centre (NCSC) recently identified higher education as a sector of concern. In 2021, the NCSC reported that universities and higher education institutions were exponentially targeted by cybercriminals. Existing challenges were amplified or became more obvious during the pandemic when universities struggled to continue their operations through hybrid and remote learning, which heavily relied on digital infrastructure and services. Despite the sector's value and vulnerabilities, higher education has received relatively little attention from the cybersecurity research community.

Over the course of two years, we have conducted numerous interventions and engagements with the UK higher education sector. Through interviews with cybersecurity practitioners working in the sector, as well as roundtables and questionnaires, we performed qualitative and quantitative analyses of threat intelligence sharing, which we used as a proxy for measuring and analyzing collaboration. In a unique approach to studying collaboration in cybersecurity, we utilized social network analysis.

This paper presents our study and findings on the state of cybersecurity in UK universities. This study also provides some recommendations for future steps that we argue are necessary for the higher education sector to continue supporting the UK's national interests. Key findings include the positive inclination of university cybersecurity professionals towards collaboration and the factors that impede such inclination. These factors include management and insurance constraints, concems about individual and institutional reputational damage, a lack of trusted relationships, and the absence of effective mechanisms or channels for sectoral collaboration.

The network itself was found to be highly fragmented, with very few active potential connections. None of the organizations we expected to facilitate collaboration within the network play a significant role, and some universities currently act as key information bridges. For these reasons, any changes that might be initiated by sectoral bodies such as Jisc, UCISA, or government organizations like the NCSC would need to pass through these information brokers [15].

Cybersecurity threats are growing exponentially, placing a significant burden on organizations. Higher Education Institutions (HEIs) are particularly vulnerable, and cybersecurity issues are drawing increasing attention. However, existing cybersecurity research has limited value for HEI leaders and policymakers because it is usually technology-focused. Publications showcasing best practices often lack a systemic perspective on cybersecurity in HEIs. Thus, this study aims to fill this gap in the literature and develop institutional cybersecurity strategies for HEI leaders and policymakers from a systemic perspective.

Here, we first review how the cybersecurity landscape has evolved over the past few decades, and we highlight the latest trends and projections for the coming decade. By analyzing these historical developments and changes, we underscore the importance of strengthening HEI cybersecurity capacities. To explore why HEIs face severe challenges in combating ever-escalating cyberattacks, we propose a systemic approach to ensure cybersecurity in HEIs and emphasize the need to reassess prioritized areas.

By conducting an extensive literature review and desk research on methods that could address cybersecurity vulnerabilities in the next decade, we synthesize our findings into a set of institutional strategies designed to better prepare HEIs to tackle cybersecurity threats in the future [16]. These strategies include the following:

1. Strengthening Institutional Governance for Cybersecurity.
2. Revisiting Cybersecurity Key Performance Indicators (KPIs).
3. Clarifying Cybersecurity Policies, Guidelines, and Mechanisms.
4. Training and Cybersecurity Awareness Campaigns to Promote a Cybersecurity Culture.
5. Responding to AI-Based Cyber Threats and Using AI to Enhance Cybersecurity.
6. New and sophisticated security measures are introduced.
7. Attention to Mobile Device Use and Implementing Encryption as a Daily Practice.
8. Risk Management.

In the current landscape, cybersecurity is increasingly critical for higher education institutions, which are facing a growing number of cyber threats that can result in significant financial and reputational harm [17]. The average cost of these breaches was $3.65 million, including expenses related to incident response, legal fees, and penalties. Denial of service (DoS) and ransomware attacks can disrupt educational operations and data access, leading to operational standstills until ransoms are paid or data are restored. Apart from the financial repercussions, these breaches also damage the institution's reputation, undermining trust among students, parents, alumni, donors, and partners.

The integration of digital technologies, data networks, and smart devices is revolutionizing university campuses, creating interconnected environments that require heightened security measures to address physical violence and cyber threats. In response, institutions are investing in automation technologies to enhance campus security. This includes migrating network infrastructure to more secure providers and implementing systems for improved student tracking to enable real-time alerts for

potential physical dangers and more effective emergency responses [18].

Cybersecurity efforts also involve protecting student data and campus network infrastructure. Universities encounter unique cybersecurity challenges, such as decentralized IT structures, diverse user base, and the delicate balance between openness and security. The variety of users and entry points, including students, faculty, staff, and third-party contractors, complicates the task of monitoring and controlling access to sensitive data and systems. Balancing the academic environment's need for openness with the imperative for security is crucial but challenging, especially in avoiding constraints on academic freedom and collaboration [19].

Research conducted at the University of Twente [20] underscores the significance of proactively anticipating and addressing network attacks, such as distributed denial-of-service (DDoS) attacks, botnets, spam, and the exploitation of critical network services like the Domain Name System (DNS) [21]. These studies underscore the value of establishing scalable, sustainable data lakes and leveraging big data methodologies to scrutinize the attack landscape, identify potential threats, comprehend the implementation and uptake of security measures, and formulate future network designs.

An article in the Sensors journal explores phishing attacks as an initial stage for infiltrating systems for remote sabotage, delineating various phishing tactics, such as mass phishing, spear phishing, executive phishing, and clone phishing. This study highlights the threat posed by false data injection attacks (FDIA) [22] in critical infrastructures, highlighting vulnerabilities in unencrypted protocols and the importance of shielding networks from such attacks.

Furthermore, a study in the Symmetry journal emphasizes the role of AI in detecting, analyzing, and mitigating malware, including the utilization of dynamic deep learning techniques in conjunction with heuristic methods to categorize and detect modern malware families. This underscores the importance of adjusting and enhancing malware detection techniques to keep pace with the evolution of threats and attacks [23].

In summary, these studies emphasize the necessity of taking a holistic approach to university networks' safeguarding. This includes employing advanced technologies and methodologies to detect, analyze, and prevent cyber threats. Progress in artificial intelligence and machine learning, along with enhancements in cryptography and data security practices, are increasingly crucial in combating cybercrime and guaranteeing the security of critical infrastructures and data.

Most popular network traffic analysis tools either do not have a graphical interface or were originally developed to solve other problems and only partially satisfy these requirements [24, 25]. The most popular tool in the second group was the Wireshark tool. The main means of presenting a network trace in it is to parse packets in the form of a list, while only a selected packet displays the full stack of protocols and the values of the fields in the headers of these protocols. A packet, as a list element, is represented by a string comprising the values of a fixed set of fields allocated in the network layer protocol header (IP address), as well as the fields of the highest-level protocol header that can be parsed. Note that fixed representations of packages can be problematic in many cases [26].

In the applied field, this problem is also widely represented: there are many both commercial and freely distributed systems, the most important components of which are responsible for solving it [27, 28].

The range of the proposed solutions is quite wide - software, software-hardware, and complete hardware implementations are available. This is partly because the solution to this problem has a greater number of practical applications, among which are as follows:

– statistics collection systems.

– traffic management systems, for example, ensuring communication quality (QoS, QoE) and optimizing channel throughput (Wan Optimization);

– security systems: firewalls (NGFW), intrusion detection and prevention systems (IDS/IPS), and spam blocking systems.

– systems to apply policies to network traffic (PCEF, PCRF, NAC) [29]. Traffic classification is necessary in this context because the obtained results can be used in various applications that are important both for network administration and for end users [30].

From a provider's perspective, discerning protocols, applications, and application types based on network data flows can serve several purposes. These include monitoring network traffic (e.g., blocking specific protocols like BitTorrent), guaranteeing superior customer service by prioritizing high-priority streams and managing individual packet transmission speeds, setting service prices, strategizing resource deployment and utilization, enhancing provided services, and adjusting routing algorithms (e.g., altering data transmission priorities during periods of high network congestion).

Network Traffic Classification: Analysis and Applications [31]. This paper argues that the rapid adoption of advanced administrations and Internet of Things (IoT) innovation is leading to the expansion of a unique number of digital attacks, and that rule-based network intrusion detection systems (NIDS) are struggling to adapt. Accordingly, artificial intelligence (AI) is used as a second line of defense, and the philosophy is shown to be able to extract obscure patterns from network traffic and distinguish between all types of unsuspected new threats. Network traffic enforcement is a key device in digital de-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

fense to identify and thwart digital insider threats. Regulating network traffic is the first step in recognizing the various applications and conventions available in your organization. Also central to this article, organization outage recognition, which examines organization movement from a traffic representation perspective.

Detection of virtual private network traffic using machine learning [32], this paper presents computational models to address the current limitations in VPN traffic detection. A VPN usage detection model is developed using a multilayer perceptron neural network trained using flow statistics data found in the Transmission Control Protocol (TCP) header of captured network packets. Validation testing demonstrated that the proposed models can classify network traffic as either direct (originating from the user's own device) or indirect (using VPN's identity and location hiding capabilities) with high accuracy. Experiments conducted to classify OpenVPN usage demonstrated that the neural network could correctly identify VPN traffic with an overall accuracy of 93.71%. Further work on classifying Stunnel's OpenVPN usage demonstrated that the neural network was able to correctly identify VPN traffic with an overall accuracy of 97.82% when using 10-fold cross validation. This experiment also provided control over the 3 different validation methods and the different accuracy results obtained. These results demonstrate significant progress in detecting unauthorized user access, which suggests that further advances can be made in the future, particularly in business security applications where detecting VPN use is critical to an organization.

Classification of VPN network traffic flow using time related features on apache spark [33] This paper classifies VPN network traffic flow using time-dependent features in Apache Spark and artificial neural networks. Today's internet traffic is encrypted using VPN/non-VPN protocols. This situation precludes classical deep packet inspection approaches by analyzing packet payloads. MATLAB 2019b is used to conduct this study because the increasing demand for VPN networks has triggered the evolution of technology. The proposed method avoids unnecessary processing and the flooding found in standard VPN network traffic classification. The proposed system was trained on 80% of the dataset, and 20% was retained for testing and validation with 10-fold validation, as well as 50 training epochs. According to the authors, this study is the first to implement and use artificial neural networks and apache spark engine to perform VPN traffic flow classification. VPN classification accuracy of the ANN and Apache Spark Engine was 96.76%. The accuracy of non-VPN classification using the proposed method was 92.56%. This paper has demonstrated that the approach used by CIC-Darknet2020 for packet-level encrypted traffic classification cannot contain packet header information because it allows direct mapping of packets to a specific application with high accuracy. Considering only non-VPN traffic, 96.76% of all packets in the dataset were attributed to the application. The remaining packets can still be classified with high probability by making predictions based on the applications using the proposed flow.

Network traffic classification using convolutional neural networks and ant-lion optimization [34] demonstrated that deep learning methods have been widely studied for network traffic classification. Unfortunately, these models require a large amount of training data. Another challenge with most traffic classification methods is that the features must be extracted by an expert. In these methods, it is very tedious and time-consuming to find desired features, which leads to better classification. Therefore, a significant solution to this problem is to employ deep learning techniques that automatically extract features. This paper is an attempt to solve these problems using a combination of a convolutional neural network (CNN), an-lion meta-heuristic algorithm (ALO) and self-organizing map (SOM) to develop a traffic classification model. The proposed method could detect encrypted traffic and distinguish between VPN and non-VPN traffic. The model was evaluated on the "ISCX VPN-Non-VPN" dataset and achieved 98% accuracy.

The primary research topic in this paper is network traffic classification, which is solved using machine learning methods [35]. The data on the various problem statements and limitations that were achieved using earlier methods provide an idea of the reasons for using machine learning in this area. It is assumed that various machine learning algorithms can be used to solve problems, and their advantages and disadvantages. This study explores the selection of features for classification and the problem of obtaining data that are necessary for learning, which are the main trade-offs in this issue. The most frequently used datasets and their characteristics are described. This section concludes the review, addressing the following issues: model training and comparison, user data protection, and traffic variability.

Traffic monitoring and analysis are performed for a few key reasons, including analyzing network resource usage, evaluating the effectiveness of network applications, adapting to quality of service (QoS) policies, complying with legal requirements for traffic registration, and developing realistic traffic models for scientific research [36]. Within the framework of this article, the task was to develop a methodology to evaluate the performance of various applications under high-speed Internet conditions. To achieve this goal, several issues were investigated, primarily traffic classification methods that efficiently process large amounts of data in real time while relying on limited processor and memory resources. In addition, methods for evaluating the quality of service

(QoS) of applications in real time based on the data received from the traffic classifier were also investigated. This study focused on the problems of traffic classification and analysis, limiting itself to studying the relationship between traffic classification and QoS assessment, and it offers a universal algorithm for this task. This paper considers well-known traffic classification methods, such as the use of port numbers, deep packet inspection (DPI), and statistical classification based on machine learning algorithms, and evaluates their effectiveness for specific scenarios. It was found that classification based on port numbers is losing relevance due to the dynamic use of ports by many applications. In contrast, DPI requires significant computing resources and is associated with privacy issues. At the same time, statistical classifiers based on machine learning have demonstrated their applicability.

Since the internal corporate networks of companies continue to increase in volume, network service managers must be aware of the various types of traffic that pass through their networks and be able to control such traffic. To solve problems that arise due to malfunctions more effectively, it is necessary to monitor and analyze traffic. This will allow you not to stop the operation of network services for long periods of time. Many tools can help administrators monitor and analyze network traffic. This section focuses on router-based and non-router monitoring methods (active or passive). This section describes the three most popular and frequently used monitoring tools that are used in router-based data networks (SNMP, RMON and Cisco Netflow) and provides information about two new monitoring methods that use a combination of passive and active monitoring methods (WREN and SCNM).

The development of networking, which is one of the most significant and important aspects of information technology, is becoming increasingly intensive [37]. This is because it offers a large amount of information, resources, and human experience. On the one hand, it contains a large amount of malicious content that can be obtained via misuse. Conversely, prolonged exposure to a computer or other network device can lead to health deterioration. The importance of monitoring and analyzing network traffic is increasing because corporate computing environments are increasingly network-oriented. Most of the traffic monitoring and analysis tools that are currently used are designed to measure the load on individual network segments. They also tend to have complex user interfaces. Here, you will learn about the creation of the program and its implementation using MS Windows, which is designed to manage the network and monitor user network activity. This program includes two parts: client and server. Click on the offer to select the most suitable option from all possible options. The client side application is an auxiliary application that turns on and off when the computer is started, as well as when it is turned off. The client side application does not have the right to stop when the computer is turned off and running. The server side is more complex. This application has a graphical interface that is responsible for receiving, managing, and updating data from a group of clients to provide the network owner with an up-to-date view. The effectiveness of the application was tested by using it in a corporate network.

Traffic classification is widely used in the fields of network security and network management [38]. To begin the research, it was typical to compare network traffic with various unencrypted applications. However, no research has been conducted on the classification of encrypted application network traffic, particularly underlying traffic. An attempt to solve this problem is to create an encrypted network traffic classification model that includes attention mechanisms and spatiotemporal characteristics. The proposed model initially uses the long-term short-term memory (LSTM) method to study continuous network flows and identify the features of the temporal correlation between these flows. Second, to extract high-order spatial features from the network stream, the convolutional neural network (CNN) method is used, after which the compression and excitation module (SE) is used to weigh and redistribute the high-order spatial features necessary to obtain the key spatial features of the network stream. Finally, due to the above three training stages, a fast classification of network flows can be achieved.

It demonstrates an outstanding generalization capability and can effectively adapt to diverse sets of network traffic data. In addition, the proposed model efficiently handles both encrypted and unencrypted traffic, achieving high-level accuracy. Experimental results demonstrate that the proposed model can successfully classify traffic originating from encrypted and unencrypted applications, which significantly increases the accuracy of identifying traffic originating from encrypted applications. In most cases, the classification accuracy exceeds 90%.

Cyber threats and data breaches are growing concerns in our interconnected digital world. Botnets pose serious threats because they can launch various cyberattacks such as DDoS attacks, spam emails, malware distribution, and data theft [39]. Identifying and categorizing botnets has become highly complex due to the massive volume of network traffic. This paper introduces a multilayer framework for detecting and classifying botnets using machine learning algorithms. The proposed framework includes three main parts: Feature Selection, Botnet Detection, and Botnet Classification. The Feature Selection layer reduces the dataset to six essential features, which improves the framework's accuracy and ef-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ficiency. The Botnet Detection layer identifies botnet activity by distinguishing legitimate and botnet packets. The Botnet Classification layer analyzes the filtered botnet packets to classify them into different types of botnets. This framework uses the SHAP (ShapleyAdditive Explanations) technique to describe the model's decision-making process. The effectiveness of the proposed model was evaluated using the NCC-2 and CTU-13 datasets, and a 10-fold cross-validation technique was applied for validation. The results demonstrate an average accuracy of 99.98% in botnet detection and 99.30% in classifying botnet families, which indicates high performance. The comparative analysis demonstrates the superiority of the proposed model over existing methods in terms of accuracy, precision, recall, and F1-Score.

The proliferation of smart devices generates vast amounts of data, which raises concerns about personal information, including health and financial data [40]. These data flow through networks and are exposed to network traffic, which can be either normal or malicious, introduced by hackers to disrupt the network. Although firewalls and traditional intrusion detection systems can identify attacks based on known patterns, they often fail to detect advanced or unknown threats. To address this gap, intelligent techniques are crucial. This study examines the machine learning techniques proposed recently to detect different types of unknown attacks. This study focuses on classifying anomalous behavior in network traffic using the CIC-IDS-2017 dataset, which contains data about attacks. It uses machine learning algorithms as Gaussian Naïve Bayes, Logistic Regression, Decision Tree, Random Forest, AdaBoost, and other ensemble models to classify threats.

The Internet of Things (IoT) has been extensively used in various fields like smart homes, healthcare, and industry [41]. However, the rapid growth of Internet of Things (IoT) devices has made them attractive targets for cyberattacks. To protect IoT systems, it is critical to accurately classify IoT traffic accurately for effective intrusion detection. Traditional methods struggle to extract and capture complex spatial relationships and topological information from IoT traffic data. To address this issue, a Multi-Scale Convolutional Feature Fusion Network with a Convolutional Block Attention Module (MCF-CBAM) for precise IoT traffic classification was introduced. The proposed method includes three significant innovations: the extraction of multi-scale spatial features from traffic data, which reduces network complexity, the enhanced focus of the attention module on critical features, and the cross-scaled connections, which improve feature reuse and generalization. In the experimental results, the proposed method was evaluated on three datasets: N-BaIoT, KDDCUP99, and UNSW-NB15, using three different models MCF, MCF-SE, and MCF-CBAM. The performance was evaluated using Accuracy, Precision, Recall, and F1-score metrics that gave scores of 0.999 and above.

As DoS and DDoS attacks become increasingly common, there is a growing need for effective defense mechanisms [42]. Network-based intrusion detection and prevention systems are commonly used to identify such anomalies in computer networks. Although these systems can detect known attacks, they still struggle to adapt to the evolving nature of DoS/DDoS anomalies. Machine learning (ML) algorithms offer solutions by effectively handling concept drift and changing cyber threat data patterns over time. This paper introduces a new algorithm called Anomaly2Sign that automatically generates rules for Suricata using a Decision Tree (DT)-based process. The DT is trained on anomalous and legitimate traffic, which allows it to select anomalous features mapped into the rule structure. In addition, the DT hyperparameters are adjusted at runtime to create a minimal rules that can detect many anomalous packets. The proposed algorithm achieves classification metrics ranging from 99.7% to 99.9% using the BOUN-DoS and BUET-DDoS datasets, outperforming other ML classifiers such as Logistic Regression, Support Vector Machine, and Multi-Layer Perceptron.

Machine learning-based network intrusion detection for large and imbalanced data using oversampling, stacking feature embedding, and feature extraction [43] Cybersecurity has become a major global concern, with Intrusion Detection Systems (IDS) playing a crucial role in safeguarding interconnected networks by identifying malicious actors and activities. Machine Learning (ML) algorithms, particularly in behavior analysis within IDS, demonstrate promise in detecting dynamic cyber threats and identifying anomalies and malicious behavior in networks. However, handling increasing data volumes poses challenges when training ML models. To address this issue, this paper introduces a new ML-based network intrusion detection model that uses Random Oversampling (RO) to address data imbalance and Stacking Feature Embedding based on clustering results, along with Principal Component Analysis (PCA) to reduce the dimensionality. The proposed model is specifically designed for large, imbalanced datasets.

The performance of the proposed model was evaluated on three benchmark datasets: UNSW-NB15, CIC-IDS-2017, and CIC-IDS-2018. On the UNSW-NB15 dataset, the experimental results demonstrate that the Random Forest and Extra Tree models achieve accuracy rates of 99.59% and 99.95%, respectively. Additionally, on the CIC-IDS-2017 dataset, the Decision Tree, Random Forest, and Extra Tree models achieved 99.99% accuracy, whereas the Decision Tree and Random Forest models achieved 99.94% accuracy on CIC-IDS-2018. These results consistently outperform current state-of-the-art

methods, which indicates significant progress in network intrusion detection [44].

The increasing demand for communication networks that support a wide array of services necessitates effective methods for analyzing, monitoring, evaluating, and design networks. The analysis encounters ongoing challenges such as incomplete and expanding user requirements, and uncertainties regarding networked system development. To satisfy user needs and ensure reliability and availability, system models that mirror actual network loads and offer reasonably accurate predictions of system performance within a practical timeframe. Traffic analysis plays a crucial role in understanding network requirements and capabilities.

In recent years, numerous traffic models have been proposed to comprehend and analyze traffic characteristics in networks. However, no single traffic model can fully reflect the traffic characteristics of all network types under all circumstances. Consequently, studying traffic patterns to understand their characteristics and identify the most suitable traffic pattern for a specific environment has become an essential and rewarding endeavor. Effective traffic modeling is also fundamental for precise capacity planning [45].

Materials and research methods

Case study. The university IT department provided access to research work, and data were collected in the traffic log format containing between 7 and 8 million events to automatically determine the categories of Internet usage by students. A custom solution was developed for processed traffic log analysis. Due to the absence of the analyzer and the graphical interface, a custom application was developed using the standard Linux Apache MySQL (LAMP) development stack. Due to budget limitations and the lack of applications for analyzing real-time traffic, a custom solution was developed for analyzing processed traffic. The processed data was analyzed using quantitative methods based on the frequency of events occurring.

With a sufficient budget, the hardware installation should include an Intel Xeon E5-2620 v4 processor, 64 GB of DDR4 RAM, and a 1 TB solid-state drive for data storage. An NVIDIA Tesla V100 GPU can be used to handle the computing load, thereby facilitating the training of deep learning models. Ubuntu 20.04 LTS was used as the operating system, and Python 3.8 was the main programming language. Libraries such as TensorFlow, Karas, and Scikit-learn were used for model development, and Pandas and NumPy were used for data processing and analysis.

The firewall vendor was from the leaders of the Gartner's Magic Quadrant [46]. The data was automatically categorized into 24 categories during the analysis. In Fig. 1 the first 13 categories are presented (small data was truncated and not visible in this chart).

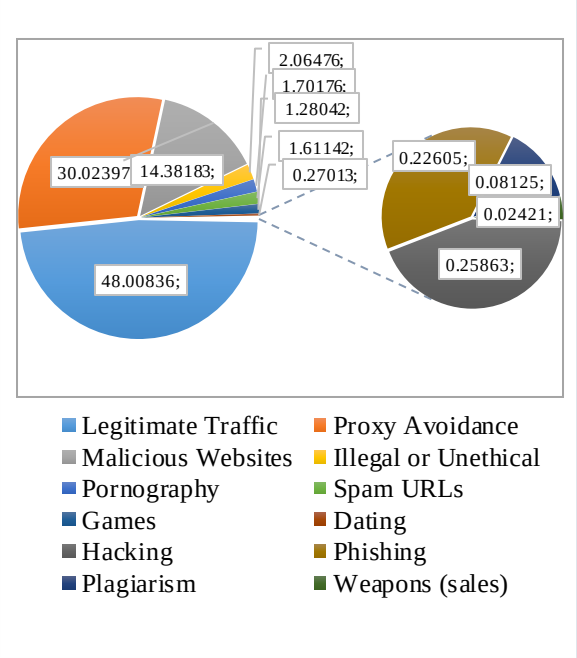

Fig. 1. Processed data from the raw logs

From this figure, we determined that users use the university network for unethical purposes together with ordinary sites, including pornography, weapons trade, and religious sites, which may include extremist content. The full list of categories is shown in Table 1.

From the frequency analysis, we observed that network traffic generated by higher education institutions passes proxy avoidance services to access malicious websites because proxies are widely used by students to access illicit web content. However, we cannot exactly infer whether users use malware and viruses to subvert security protocols to access specific resources.

One of the basic techniques to generate a blacklist database of websites is based on tools based on reports [47]. The primary concern is that the available blacklist databases is not complete for the Kazakhstan region, including but not limited to the top-level domain (TLD) .kz, ru and .com. Examples of TLDs are neither listed in the various blacklist databases nor categorized as such. Some that are freely accessible from higher education networks are given in Table 2.

As a solution to address these issues, a proof of concept was developed. The simple submission form adds suspicious URLs to the database for IT department review. Admin or authorized entity may also add new categories. The application features a Representational State Transfer (REST) API that has been implemented with consideration of future integration. In addition, web hooks are implemented in JSON format if considered to integrate with a third-party traffic filtering vendor. Any

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

object can access the resource/list, which contains the object and category of the URL (Fig. 2).

Table 1

Frequency of occurrence events by the category

Categories	Number of events	Percentage
Legitimate Traffic	3648635	48.00836
Proxy Avoidance	2281822	30.02397
Malicious Websites	1093019	14.38183
Illegal or Unethical	156922	2.06476
Pornography	129334	1.70176
Spam URLs	122468	1.61142
Games	97312	1.28042
Dating	20530	0.27013
Hacking	19656	0.25863
Phishing	17180	0.22605
Plagiarism	6175	0.08125
Weapons (sales)	1840	0.02421
Global Religion	1534	0.02018
Alternative Beliefs	1274	0.01676
Gambling	856	0.01126
Lingerie and Swimsuit	474	0.00624
Alcohol	227	0.00299
Nudity and Risque	164	0.00216
Other Adult Materials	150	0.00197
Advocacy Organizations	50	0.00066
Tobacco	18	0.00024
Drug Abuse	12	0.00016
Discrimination	4	0.00005
Explicit Violence	1	0.00001

Table 2

Tld examples

Category	Global Religion	Weapons (sales)
Domain names	umma.ru	guns.ru
	azbyka.ru	www.weaponplace.ru
	ummet.kz	www.dmazay.ru
	pobeda.ru	rusarmy.com

In Fig. 3 we propose an architecture for further scalability, and the integration is provided.

The database clusters consider implementing fault-tolerant MySQL or other RDBMS or NO RDBMS systems.

The development of the representational REST API [48] and messages from web-resources were downloaded [49].

In this research TF-IDF method was used to define the most frequently used words [50]. To identify words that are characteristic of a document, such as a forum message, one calculates the term frequency (TF) of a term (word or phrase) within the entire document and then multiplies it by the inverse document frequency (IDF). The product of TF and IDF is known as TF-IDF [51, 52].

Fig. 2. Sample of JSON response accessing the /list resource

The most straightforward approach is to use the raw count of a term in a document, which is the number of times a term appears in the document. Inverse document frequency (IDF) indicates the information content of a word and indicates whether the term is common or rare across all documents. The inverse fraction is calculated as the logarithmically scaled inverse fraction of documents containing the word, obtained by dividing the total number of documents by the number of documents containing the term and then taking the logarithm of that quotient (1) [53].

$$\mathrm{idf}(t, D) = \log \frac{|D|}{|\{d_i \in D | t \in d_i\}|}, \quad (1)$$

where |D| – total number of documents in the corpus.

$|\{d_i \in D | t \in d_i\}|$ – the number of documents where the term t appears.

Then TF-IDF is calculated as follows:

$$\mathrm{tf} - \mathrm{idf}(t, d, D) = \mathrm{tf}(t, d) * \mathrm{idf}(t, D). \quad (2)$$

The TF-IDF values of the keywords were calculated using (2).

After defining the keywords, their basic information was recorded in the SQLite Expert Personal 3.5.46.2466 database [54].

SQLite Expert Personal 3.5.46.2466 was selected to store basic keywords information due to its lightweight and embedded nature, which makes it easy to integrate into research applications without requiring a separate server process. It is widely compatible across platforms and programming languages, supports standard SQL queries, and provides adequate performance for managing keyword data efficiently. Additionally, SQLite

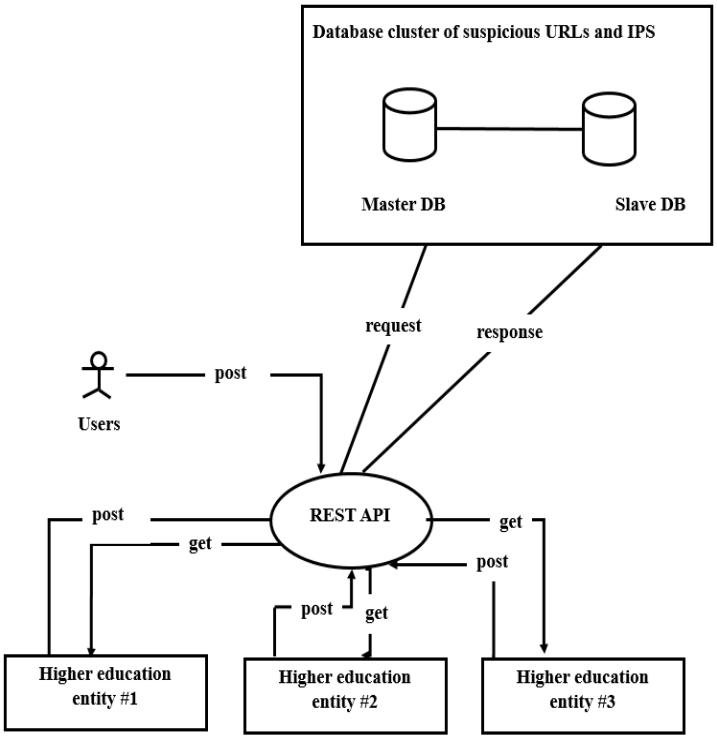

Fig. 3. Proposed high architecture for the implementation and integration

Expert Personal provides a user-friendly interface, simplifying database management tasks, and is open-source; thus, it aligns well with the project's cost-effective requirements.

We focus only on the base forms of words, excluding their endings, as this improves program efficiency by reducing the time required to search for possible word variants. We treated different variants of a word with various endings as single words. For instance, the words "jihad" (жиһад), "jihadtyn'" (жиһадтың), "jihadqa" (жиһадқа), "jihadta" (жиһадта) will be considered the same word. Because one word could have multiple spelling variations, we entered words into the database with all possible variants.

Subsequently, a tool was created using the Visual C# integrated development environment. The tool checks for the presence of extremist keywords in each text and displays any words found [55]. The initial step involved conducting morphological analysis of the input text to determine morphological labels such as the base and end for each word. Subsequently, a query was made to the database, searching for each word in the input text. If a base was found in the database, it was displayed in the output text; otherwise, it was skipped, and the next word was searched.

The developed tool functions effectively, successfully identifying all extremist keywords in the input text. For classification, the authors employed linear SVC, multinomial naive Bayes, logistic regression, classification trees, and random forest. In this experiment, the authors used the open-source machine learning library Scikit-learn. The classification results are presented in Table 3 [56, 57].

Table 3

Classification results

Model	Accuracy
Linear SVC	0.61
Multinomial naive Bayes	0.81
Logistic regression	0.70
Classification trees	0.51
Random forest	0.83

Results and Discussion

There are numerous tunneling services exist in the market. Such examples include Psiphon-3 [58] and Hotspot Shield [59].

Due to many limitations, there are fewer chances that students will use premium services to access blocked content.

There are a tremendous number of free and premium proxies. The IT department cannot block all proxies because some academics may use proxies for research. However, IT departments can monitor the use of proxies by offering their own proxy services. The benefit of doing so will further enhance the analytics of using

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

services beyond the proxy, which can also be traceable.

Another method considers web protocols. In some cases, non-secure HTTP protocols may be blocked, whereas resources are freely accessible in secure HTTPS.

Based on the above recommendations, the university should adopt a reporting tool. To prevent system abuse and identify students, Wi-Fi session credentials should be captured and used in reporting.

Since this problem arises with the open web, consideration should be given to using the dark web. The TOR (The Onion Router) allows accessing the content from the dark web.

To block only those websites that pose a threat to national security, it is proposed to analyze the content of such websites qualitatively. In this work, it is suggested to create a blacklist of websites in the categories "Global Religion", "Weapons Sales", and "Extremist Materials" that will be available for educational institutions in Kazakhstan. Advanced universities like Al-Farabi Kazakh National University, can provide free access to such blacklists from all other universities in Kazakhstan.

It is also important to develop information security training and awareness to keep IT staff aware, trained, and informed [60]. The procedures include but are not limited to training and educating the IT and general staff about various areas and problems related to information security in the organization. In addition, benchmarks and reporting should be established regularly. For example, an optional general education program for employees should be organized quarterly to inform employees about risks and vulnerabilities and to inform them about ways to deal with such risks at the user level. To assess information security issues, reports on specific issues and resolutions should be developed. These reports will provide significant and relevant information about the new security trends and issues, along with their remedial measures. In addition, these procedures will expand knowledge capital, which will provide significant data for the newly recruited IT staff.

Conclusions

The research covered various aspects of information and network security in the higher education sector at various universities in Kazakhstan. The authors proposed a framework to analyze the illegal use of university network by students. During the study, an experimental setup architecture to integrate various higher education organizations was developed. A log analysis tool was also developed to monitor and filter user-accessed network resources. A corpus and database of keywords were constructed to identify texts with an extremist orientation in Kazakh language. In addition, a tool was developed to check the presence of extremist keywords from a database in the given text. It is worth mentioning that this work is unique, and there is no such dictionary in Kazakh language. We also compared various classification methods. The highest accuracy was obtained using multinomial naive Bayes. At present, our corpus is not very large, and in future, we plan to expand the dataset to increase classification accuracy. In future work, we plan to increase the number of classification categories. The proposed new categories include: Cyberbullying: detecting online harassment and bullying behaviors; Misinformation: identifying false or misleading information; Hate Speech: detecting language that promotes violence or discrimination against specific groups; Self-Harm: identifying content that encourages self-harm or suicide. These additions enhance the comprehensiveness of the classification system, ensuring that a wider range of harmful content is detected and addressed.

Contributions of authors: conceptualization, methodology – **Shynar Mussiraliyeva**; formulation of tasks, analysis – **Milana Bolatbek**, **Shynar Mussiraliyeva**; development of model, software, verification – **Milana Bolatbek**; analysis of results, visualization – **Gulshat Baispay**, **Assel Usmanova**; writing – original draft preparation, writing – review and editing – **Gulshat Baispay, Assel Usmanova**.

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

This work was supported by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP15473412). The project supervisor is Gulshat Baispay.

Data Availability

The associated data are in the data repository.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods in their work.

All the authors have read and agreed to the publication of the finale version of this manuscript.

References

1. "*What is the Blue Whale suicide challenge, how many deaths has the game been linked to and is it in the UK?*" The Sun. Available at: https://www.thesun.co.uk/news/worldnews/3003805/blue-whale-suicide-victims-

russia-uk-deaths-latest/. (Accessed: Dec. 5, 2023).

2. Zhavoronkova, T. V. Usage of the Internet by terrorist and extremist organizations. *Orenburg State University Bulletin*, 2015, vol. 3, no. 178. 30 p.

3. Ravndal, J. A. Anders Behring Breivik's use of the Internet and social media. *Journal of Exit-Deutschland: Zeitschrift für Deradikalisierung und demokratische Kultur*, 2013, vol. 2, pp. 172-185.

4. Anzalone, C. Zachary Chesser: An American Grassroots Jihadist Strategist on Raising the Next Generation of Al-Qaeda Supporters. *Perspectives on Terrorism*, 2010, vol. 4, no. 5.

5. *About 500 Kazakhstanis are fighting in Syria and Iraq on the side of ISIS*. Today.kz. Available at: http://today.kz/news/mir/2017-10-31/753466-okolo-500-kazahstantsev-voyuyut-v-sirii-i-irake-na-storone-igil/. [Accessed: Nov. 15, 2023].

6. *«On Countering to Extremism»* The Law of the Republic of Kazakhstan dated 18 February 2005, No.31.

7. *«Criminal Code of the Republic of Kazakhstan»* Code of the Republic of Kazakhstan dated July 16 1997, No. 167.

8. *«On Mass Media»* The Law of the Republic of Kazakhstan dated 23 July 1999, № 451-I.

9. Liu, D., & Park, Y., Anonymous traffic detection based on feature engineering and reinforcement learning, *Sensors*, 2024, vol. 24, no. 7, article no. 2295. DOI: 10.3390/s24072295.

10. Manjunatha, B. A., Shastry, K. A., Naresh, E., Pareek, P. K., & Reddy, K. T. A network intrusion detection framework on sparse deep denoising auto-encoder for dimensionality reduction, *Soft Computing*, 2024, vol. 28, no. 5, pp. 4503-4517. DOI: 10.1007/s00500-023-09408-x.

11. Elmaghraby, R. T., Aziem, N. M. A., Sobh, M. A., & Bahaa-Eldin, A. M. Encrypted network traffic classification based on machine learning, *Ain Shams Engineering Journal*, 2024, vol. 15, no. 2, article no. 102361. DOI: 10.1016/j.asej.2023.102361.

12. Baklizi, M. K., Atoum, I., Alkhazaleh, M., Kanaker, H., Abdullah, N., Al-Wesabi, O. A., & Otoom, A. A. Web Attack Intrusion Detection System Using Machine Learning Techniques. *International Journal of Online & Biomedical Engineering*, 2024, vol. 20, no. 3. DOI: 10.3991/ijoe.v20i03.45249.

13. Govers, J., Feldman, P., Dant, A., & Patros, P. Down the rabbit hole: Detecting online extremism, radicalisation, and politicised hate speech. *ACM Computing Surveys*, 2023, vol. 55, no. 14s, pp. 1-35. DOI: 10.1145/3583067.

14. Mahmood, S., Chadhar, M., & Firmin, S. Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*, 2024, vol. 32, no. 1, article no. e12549. DOI: 10.1111/1468-5973.12549.

15. Piazza, A., Vasudevan, S., & Carr, M. Cybersecurity in UK Universities: mapping (or managing) threat intelligence sharing within the higher education sector. *Journal of Cybersecurity*, 2023, vol. 9, no. 1, article no. tyad019. DOI: 10.1093/cybsec/tyad019.

16. Cheng, E. C., & Wang, T. Institutional strategies for cybersecurity in higher education institutions. *Information*, 2022, vol. 13, no. 4, article no. 192. DOI: 10.3390/info13040192.

17. Ibrahim, M. M., Omar, M. H., Habbal, A. M. M., & Zaini, K. M. Analysis of internet traffic in educational network based on users' preferences. *Journal of Computer Science*, 2014, vol. 10, no. 1, pp. 99-105. DOI: 10.3844/jcssp.2014.99.105.

18. *8 Considerations When Establishing Cybersecurity in Higher Education*. ER.educause, 2023. Available at: https://er.educause.edu/articles/sponsored/2023/10/8-considerations-when-establishing-cybersecurity-in-higher-education. (Accessed: Jan. 17, 2024).

19. *Higher Ed Redefines Fraud Strategies for the Connected Campus*. PYMNTS, 2024. Available at: https://www.pymnts.com/safety-and-security/2024/higher-eds-redefine-cybersecurity-strategies-for-the-connected-campus/. (Accessed: Jan. 17, 2024).

20. *Cybersecurity in Higher Education: Protecting Student Data and Campus Networks*. Apporto, 2023. Available at: https://www.apporto.com/cybersecurity-in-higher-education-protecting-student-data-and-campus-networks/. (Accessed: Jan. 17, 2024).

21. *Network Security*. University of Twente. Available at: https://www.utwente.nl/en/digital-society/research/Cybersecurity_tuccr/activities/network-security/. (Accessed: Jan. 17, 2024).

22. Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, 2023, vol. 23, iss. 8, article no. 4060. DOI: 10.3390/s23084060.

23. Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation. *Symmetry*, 2023, vol. 15, iss. 3, article no. 677. DOI: 10.3390/sym15030677.

24. Markin, Y. V., & Sanarov, A. S. The modern network traffic analyzers overview. Preprinty ISP RAN (Preprints of ISP RAS), No. 27, 2014.

25. Tufail, S. et al. A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. *Energies*, 2021, vol. 14, no. 18, article no. 5894. DOI: 10.3390/en14185894

26. Olowu, T. O., Dharmasena, S., Hernandez, A., & Sarwat, A. Impact Analysis of Cyber Attacks on Smart Grid: A Review and Case Study. In: Tyagi, H., Chakraborty, P.R., Powar, S., Agarwal, A.K. (eds) *New Research Directions in Solar Energy Technologies*,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

2021, Energy, Environment, and Sustainability. Springer, Singapore, pp. 31-51. DOI: 10.1007/978-981-16-0594-9_3.

27. Djenna, A., Harous, S., & Saidouni, D. E. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 2021, vol. 11, no. 10, article no. 4580. DOI: 10.3390/app11104580.

28. Joshi, M., & Hadi, T. H. A review of network traffic analysis and prediction techniques. *arXiv. Computer Science. Networking and Internet Architecture*, 2015. DOI: 10.48550/arXiv.1507.05722.

29. Getman, A. I., Markin, Y. V., Evstropov, E. F., & Obydenkov, D. O. Review of problems and methods for solving them in the field of network traffic classification. *Proceedings of ISP RAS*, 2017, vol. 29, iss. 3, pp. 117-150. DOI: 10.15514/ISPRAS-2017-29(3)-8.

30. Getman, A. I., & Ikonnikova, M. K. A Survey of Network Traffic Classification Methods Using Machine Learning. Program Comput Soft, 2022, vol. 48, pp. 413–423. DOI: 10.1134/S0361768822070052.

31. Parati, N., Amdani, S. Y., & Asole, S. S. Network Traffic Classification: Analysis and Applications. *International Journal of Scientific Research in Science and Technology (IJSRST)*, 2022, vol. 9, no. 2, pp. 218-225. Available at: https://ijsrst.com/IJSRST229243. (Accessed: Jan. 17, 2024).

32. Miller, S., Curran, K., & Lunney, T. Detection of virtual private network traffic using machine learning. *International Journal of Wireless Networks and Broadband Technologies (IJWNBT)*, 2020, vol. 9, no. 2, pp. 60-80. DOI: 10.4018/IJWNBT.2020070104.

33. Aswad, S. A., & Sonuç, E. Classification of VPN network traffic flow using time related features on Apache Spark. *Proc. 4th Int. Symp. on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Istanbul, Turkey, 2020, pp. 1–8. DOI: 10.1109/ISMSIT50672.2020.9254893

34. Izadi, S., Ahmadi, M., & Nikbazm, R. Network traffic classification using convolutional neural network and ant-lion optimization. *Computers and Electrical Engineering*, 2022, vol. 101, article no. 108024. DOI: 10.1016/j.compeleceng.2022.108024.

35. Ikonnikova, M. K., & Getman, A. I. A survey of Network Traffic Classification Methods Using Machine Learning," Trudy ISP RAN/Proc. ISP RAS, vol. 32, issue 6, 2020. DOI: 10.15514/ISPRAS–2020–32(6)–11

36. Bujlow, T. *Classification and Analysis of Computer Network Traffic*. Networking & Security Department of Electronic Systems, Aalborg University, June 3, 2014.

37. Alisha, C. *A Summary of Network Traffic Monitoring and Analysis Techniques*. Available at: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html. (Accessed: Jan. 17, 2024).

38. Daadoo, M. Network Traffic Monitoring Analysis System with Built-in Monitoring Data Gathering. *European Journal of Social Sciences*, 2017, vol. 54, no. 1, pp. 79-91. Available at: http://www.europeanjournalofsocialsciences.com/. (Accessed: Jan. 17, 2024).

39. Hu, F., Zhang, S., Lin, X., Wu, L., Liao, N., & & Song, Y. Network traffic classification model based on attention mechanism and spatiotemporal features. *EURASIP Journal on Information Security*, 2023, article no. 6. DOI: 10.1186/s13635-023-00141-4.

40. Gupta, S., & Singh, B. An intelligent multi-layer framework with SHAP integration for botnet detection and classification. *Computers & Security*, 2024, vol. 140, article no. 103783. DOI: 10.2139/ssrn.4592818.

41. Vadhil, F. A., Salihi, M. L., & Nanne, M. F. Machine learning-based intrusion detection system for detecting web attacks. *IAES International Journal of Artificial Intelligence*, 2024, vol. 13, no. 1, pp. 711-721. DOI: 10.11591/ijai.v13.i1.pp711-721.

42. Liao, N., & Guan, J. Multi-scale Convolutional Feature Fusion Network Based on Attention Mechanism for IoT Traffic Classification. *International Journal of Computational Intelligence Systems*, 2024, vol. 17, article no. 36. DOI: 10.1007/s44196-024-00421-y.

43. Coscia, A., Dentamaro, V., Galantucci, S., Maci, A., & Pirlo, G. Automatic decision tree-based NIDPS ruleset generation for DoS/DDoS attacks. *Journal of Information Security and Applications*, 2024, vol. 82, article no. 103736. DOI: 10.1016/j.jisa.2024.103736.

44. Talukder, M. A., Islam, M. M., Uddin, M. A., et al. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *Journal of Big Data*, 2024, vol. 11, article no. 33. DOI: 10.1186/s40537-024-00886-w.

45. Kostin, D. V., & Shelukhin, O. I. Sravnitel'nyy analiz algoritmov mashinnogo obucheniya dlya klassifikatsii setevogo zashifrovannogo trafika [Comparative analysis of machine learning algorithms for classification of network encrypted traffic). *T-Comm-Telecommunications and Transport*, 2016, vol. 10, no. 9, pp. 43-52. (In Russian).

46. Devyatkin, D., Smirnov, I., Ananyeva, M., Kobozeva, M., Chepovskiy, A., & Solovyev, F. Exploring linguistic features for extremist texts detection (on the material of Russian-speaking illegal texts). *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, Beijing, China, 2017, pp. 188-190. DOI: 10.1109/ISI.2017.8004907.

47. Zhang, J., Xiang, Y., Wang, Y., Zhou, W., & Xiang, Y. Network traffic classification using correlation information. *IEEE Transactions on Parallel and Distributed Systems*, 2012, vol. 24, no. 1, pp. 104-117. DOI: 10.1109/TPDS.2012.98.

49. Chandrasekaran, B. *Survey of network traffic models*. Washington University in St. Louis CSE, 567, 2009.

50. Gessert, F., Friedrich, S., Wingerath, W., Schaarschmidt, M., & Ritter, N. Towards a Scalable and Unified REST API for Cloud Data Stores. Available at: https://www.baqend.com/paper/dmc.pdf. (Accessed: Jan. 17, 2024).

51. Bolatbek, M., & Mussiraliyeva, S. Detection of extremist messages in web resources in the Kazakh language. *Lodz Papers in Pragmatics*, 2023, vol. 19, no. 2, pp. 415-425. DOI: 10.1515/lpp-2023-0020.

52. Mussiraliyeva, S., Bolatbek, M., Omarov, B., Bagitova, K., & Alimzhanova, Zh. Bigram based Deep Neural Network for Extremism Detection in Online User Generated Contents in the Kazakh Language. *Int. Conf. on Computational Collective Intelligence (ICCCI)*, Greece, 2021, pp. 559-570. DOI: 10.1007/978-3-030-88113-9_45.

53. Targeir, A., & Perera, S. *Mapping Extremist Forums using Text Mining*. Master thesis, University of Agder, 2013. Available at; https://core.ac.uk/download/pdf/225888029.pdf. (Accessed: Feb. 12, 2024).

54. "tf–idf," Wikipedia. Available at: https://en.wikipedia.org/wiki/Tf%E2%80%93idf. (Accessed: Feb. 12, 2024).

55. *Integrated development environment Visual C*. Available at: https://www.visualstudio.com. [Accessed: Jan. 17, 2024].

56. Mussiraliyeva, S., Bolatbek, M., Sagynay, M., Zhumakhanova, A., Yeltay, Z., & Medetbek, Z. Identifying Cyber-Threatening Texts in the Kazakh Segment of Web Resources. *Proc. 2023 7th Int. Conf. on Advances in Artificial Intelligence (ICAAI '23)*, Association for Computing Machinery, New York, NY, USA, pp. 68–72, 2024. DOI: 10.1145/3633598.3633610.

57. Mussiraliyeva, S., Bolatbek, M., Zhumakhanova, A., Sagynay, M., & Bagitova, K. Development of a Software Module for Collecting and Analyzing Web Content to Determine Extremist Direction in the Text," In: Ullah, A., Anwar, S., Calandra, D., & Di Fuccio, R. (eds) *Proc. Int. Conf. on Information Technology and Applications (ICITA), Lecture Notes in Networks and Systems*, Springer, Singapore, 2024, vol. 839. DOI: 10.1007/978-981-99-8324-7_10.

58. *Psiphon3*. Available at: https://www.psiphon3.com/. (Accessed: Feb. 5, 2024).

59. *Hotspot Shield – Free VPN for Secure, Private, and Unrestricted Internet Access*. Available at: https://www.hotspotshield.com/. (Accessed: Feb. 5, 2024).

60. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 2010, vol. 34, no. 3, pp. 523-548. DOI: 10.2307/25750690.

Received 17.02.2024, Accepted 15.04.2024

СИСТЕМА ДЛЯ ВИЯВЛЕННЯ ТА ПОМ'ЯКШЕННЯ НАСЛІДКІВ КІБЕРЗЛОЧИННОЇ ДІЯЛЬНОСТІ З ВИКОРИСТАННЯМ УНІВЕРСИТЕТСЬКИХ МЕРЕЖ В КАЗАХСТАНІ

Мілана Болатбек, Гулшат Байспай, Шинар Мусіралієва, Асел Усманова

Зростаюча поширеність інцидентів інформаційної безпеки в секторі вищої освіти підкреслює нагальну потребу в надійних заходах кібербезпеки. У цьому документі пропонується комплексна структура, призначена для аналізу незаконного використання інтернет-ресурсів в університетських мережах по всьому Казахстану. Предметом статті є виявлення та запобігання кіберзлочинній діяльності з використанням університетських мереж Казахстану. Мета полягає в тому, щоб розробити комплексну структуру, яка об'єднує кілька освітніх організацій для посилення спільних зусиль безпеки, зосереджуючись на моніторингу мережевої активності та класифікації текстів за допомогою методів машинного навчання. Завдання, які необхідно вирішити: формалізувати процедуру інтеграції кількох освітніх організацій у спільну структуру кібербезпеки; розробити інструмент аналізу журналів, призначений для моніторингу мережевої діяльності в університетських мережах; створити новий словник екстремістських термінів казахською мовою для категоризації текстів; реалізувати вдосконалені моделі машинного навчання для класифікації мережевого трафіку. Використовувані методи: інструменти аналізу журналів для моніторингу в режимі реального часу та виявлення аномалій у мережевій діяльності, методи обробки природної мови (NLP) для розробки спеціалізованого словника екстремістських термінів казахською мовою, моделі машинного навчання для класифікації мережевого трафіку та виявлення потенційних кіберзагроз, спільна розробка архітектури для інтеграції зусиль мережевої безпеки в кількох установах. Було отримано наступні результати: розроблено та впроваджено комплексний інструмент аналізу журналів, що забезпечує моніторинг мережевої діяльності в мережах університету в режимі реального часу; створено казахський словник екстремістських термінів, що полегшує категоризацію та аналіз текстів,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

пов'язаних із потенційними загрозами безпеці; передові моделі машинного навчання були успішно застосовані для класифікації мережевого трафіку, покращуючи виявлення та пом'якшення кіберзагроз; було створено експериментальну архітектуру, яка об'єднує кілька освітніх організацій, сприяючи спільним зусиллям у сфері кібербезпеки. Висновки. Наукова новизна отриманих результатів полягає в наступному: 1) розроблено надійну структуру для спільної кібербезпеки в навчальних закладах, що використовує аналіз журналів і методи машинного навчання; 2) створення спеціалізованого словника екстремістських термінів казахською мовою значно підвищило точність категоризації текстів, пов'язаних з кібербезпекою; 3) застосування передових моделей машинного навчання до класифікації мережевого трафіку забезпечило методологічний підхід до ефективного управління та захисту мережевої інфраструктури; 4) експериментальна архітектура продемонструвала потенціал для підвищення безпеки завдяки співпраці між освітніми організаціями, пропонуючи стратегічні рекомендації щодо покращення інформаційної безпеки в академічному середовищі. Результати цього дослідження роблять внесок у ширшу сферу кібербезпеки, забезпечуючи структурований підхід до виявлення та пом'якшення кіберзагроз в освітньому контексті. Ця структура має потенційні застосування, що поширюються на глобальні системи безпеки, спрямовані на створення безпечнішого середовища використання Інтернету та зниження ризиків, пов'язаних із кіберзагрозами та неавторизованим доступом до даних.

Ключові слова: кібербезпека; вища освіта; Класифікація мережевого трафіку; Машинне навчання; Казахстан; Інтернет-безпека; аналіз логів; виявлення екстремізму.

Мілана Болатбек – PhD, старш. викл. каф. Інформаційних систем КазНУ імені аль-Фарабі, Алмати, Казахстан.

Гулшат Байспай – відповідний автор, старш. викл. каф. Інформаційних систем КазНУ імені аль-Фарабі, Алмати, Казахстан.

Шынар Мусіралієва – канд. фіз.-мат. наук, зав. каф. Інформаційних систем КазНУ імені аль-Фарабі, Алмати, Казахстан.

Асел Усманова – викл. каф. Інформаційних систем КазНУ імені аль-Фарабі. Алмати, Казахстан.

Milana Bolatbek – PhD, Senior Lecturer at the Department of Information Systems of Al-Farabi Kazakh National University. Almaty, Kazakhstan,
e-mail: bolatbek.milana@gmail.com, ORCID: 0000-0002-2153-180X, Scopus Author ID: 57202834055.

Gulshat Baispay – corresponding author, Senior Lecturer at the Department of Information Systems of Al-Farabi Kazakh National University. Almaty, Kazakhstan,
e-mail: gulshat.bgb2@gmail.com, ORCID: 0000-0003-4292-2938, Scopus Author ID: 57221648127.

Shynar Mussiraliyeva – Candidate of Physical and Mathematical Sciences, Head of the Department of Information Systems at Al-Farabi Kazakh National University. Almaty, Kazakhstan,
e-mail mussiraliyevash@gmail.com, ORCID: 0000-0001-5794-3649, Scopus Author ID: 57202216979.

Assel Usmanova – Lecturer at the Department of Information Systems of Al-Farabi Kazakh National University. Almaty, Kazakhstan,
e-mail: Usmanova.assel1@gmail.com, ORCID: 0009-0004-3411-1881.