INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 3, PP. 673-682
Manuscript received February 5, 2024; revised July, 2024. doi: 10.24425/ijet.2024.149596

Analysis of digital footprints associated with cybersecurity behavior patterns of users of University Information and Education Systems

Valerii Lakhno, Nurgazy Kurbaiyazov, Miroslav Lakhno, Olena Kryvoruchko, Alona Desiatko, Svitlana Tsiutsiura, and Mykola Tsiutsiura

***Abstract*—The analysis of digital footprints (DF) related to the cybersecurity (cyber risk) user behavior of university information and education systems (UIES) involves the study and evaluation of various aspects of activity in the systems. In particular, such analysis includes the study of typical patterns (patterns) of access to UIES, password usage, network activity, compliance with security policies, identification of anomalous behavior, and more. It is shown that user behavior in UIES is represented by sequences of actions and can be analyzed using the sequential analysis method. Such analysis will allow information security (IS) systems of UIES to efficiently process categorical data associated with sequential patterns of user actions. It is shown that analyzing sequential patterns of cyberthreatening user behavior will allow UIES IS systems to identify more complex threats that may be hidden in chains of actions, not just individual events. This will allow for more effective identification of potential threats and prevention of security incidents in the UIES.**

***Keywords*—digital footprints; behavior patterns; users; university information and educational system**

I. Introduction

THE rapid development of information technology (IT) in the second half of the last century and the beginning of the 21st century has had a huge impact on all aspects of human activity, including education. Information technologies have radically changed the sphere of higher education, bringing many innovations that have transformed educational processes in universities. Among such technologies that have taken their rightful place in the business processes of universities are: online education platforms; adaptive learning technologies; virtual laboratories and simulations; digital twins of educational systems; cloud technologies for learning; learning management systems (LMS - Learning Management Systems); technologies for using big data for analytics; collaborative platforms and tools for students to work together, and others. These innovations have not only increased access to education, but also changed the approach to the learning process, making it more interactive, flexible and accessible, as well as significantly contributing to improving the quality of education and preparing students for modern challenges and requirements of the labor market. Note that although digitalization of education has provided universities with many opportunities to improve the quality of education, it is important to strike a balance between traditional teaching methods and innovative IT to ensure maximum efficiency of the educational process.

The development of IT in higher education has brought both new opportunities and new challenges in providing information (cyber) security (hereinafter referred to as IS or CS, depending on the context) to students and university staff. In this aspect, it is important to remember that universities are facing new challenges to IS and/or CS. These challenges are dictated by the need to address the need to:

- *personal data protection. Universities hold a huge amount of sensitive personal data of both students and staff.*
- *respond to the threats of cyber threats. With the increasing use of online learning and data storage tools, the risks of cyberattacks and information leaks from university information systems have increased manifold;*
- *manage access. The digitalization of universities has required effective systems for managing access to information resources, and as a consequence, effective tools are needed to identify and authenticate users and manage their access rights;*
- *IS policy development (or CS);*
- *et al.*

The development of IT in universities and other educational institutions requires constant attention to IS issues. This issue should become an integral part of the educational activities of universities to protect the confidentiality, integrity and availability of data.

That is why new research related to the creation of a secure information and education system (environment) for the university is an extremely important and urgent task.

II. Literature review

Over the past two decades, the number of publications devoted to cybersecurity (CS) of university information and education

Valerii Lakhno and Miroslav Lakhno are with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua, lvaua21@gmail.com)

Nurgazy Kurbaiyazov is with Kazakh National University named after Al-Farabi, Almaty, Kazakhstan (e-mail: kurbaniyazov.nk@gmail.com)

Olena Kryvoruchko, Alona Desiatko, Svitlana Tsiutsiura and Mykola Tsiutsiura are with State University of Trade and Economics, Kyiv, Ukraine (e-mail: ev_kryvoruchko@ukr.net, desyatko@gmail.com, svtsiutsiura@gmail.com, mitsiutsiura@gmail.com)

systems (environments) and other educational institutions has increased significantly. In our opinion, this is due to the growing awareness of the importance of cybersecurity for educational institutions and the ever-changing threat landscape. Academic theorists and practitioners of information security (IS) are actively sharing their knowledge, experience and developments to help universities adapt to new threats and protect their information resources.

In [1] the authors state that the growing use of e-learning systems has not led to an increase in attention to the problem of information security of these systems. The authors attribute this fact to the fact that e-learning systems are open, distributed and interconnected. Accordingly, ensuring the security of such systems is a difficult task that requires separate research. However, the authors predominantly focused on the analysis of CS measures and the application of CS metrics to e-learning systems, primarily in universities. According to the authors of the paper, internal cyber-attacks as well as the lack of appropriate IT policies pose the greatest threats to the CS of such systems.

In [2, 3], the authors noted that universities have become lucrative targets for cyberattacks. Universities and research institutes may have large amounts of research results as well as sensitive personal data of scientists. This makes these organizations attractive targets for cybercriminals as well as hacktivists [4].

As the authors in [5] note, although academic institutions face significant information security risks, attitudes towards the implementation of measures to protect their information assets may vary. In particular, the authors draw attention to the fact that it is not always easy for universities to find a balance between IS (IS) measures and academic openness and the free flow of information. Within the academic environment, collaboration and information sharing both within the institution and with colleagues from outside is the norm. And as noted in [5], although researchers specializing in IS issues and working in universities have published thousands of articles on IS issues, the education sector itself often leaves cybersecurity to the technical staff of educational institutions.

More than 20 years ago, in their paper [6], the authors studied security in online learning and discussed the trade-off between security and accessibility. The authors of this paper may have been among the first to lead a discussion in the early 21st century about the security culture of academia and its relationship with the security services of educational institutions.

In [7, 8] discusses the legal implications of data breaches in higher education in storing student data. Also touched upon is the problem of regulating CSs under state law following U.S. federal law.

In [9], the authors examine the risks associated with social media in higher education institutions in Malaysia. The authors of this study emphasized the risks for teachers.

In [10], the authors conducted a systematic review of the risks of IPM in higher education. According to the authors, while there is an increasing number of publications on university security, there is an acute lack of empirical research. The authors identified the most valuable assets in need of protection in universities and these included: personal data on students and staff; student evaluations and administrative data; financial data; university research data; and university information systems (IS). As the authors have shown, the most frequent threat events for UIES can be considered: malicious software (software) and other forms of compromise of university information assets. Also identified by the authors as significant threats are: scanning of university resources; social engineering attacks; and inadvertent disclosure of information. Although the authors have analyzed the threats to university information assets very thoroughly, however, the paper does not offer even conceptually strategic measures to counteract these risks and threats. As noted by the authors of this paper, the purpose of such a systematic review was only to note the need for additional research in this area.

In [11, 12], the authors present the results of studies concerning the analysis of threats to CS during the implementation of phishing attacks and attacks based on social engineering techniques. The authors conclude that there is a high level of susceptibility to phishing attacks in academia.

It is noted in [13] that the Covid-19 pandemic has had a significant impact on the organization of learning in universities. The widespread use of new IT, in particular, cloud computing, online learning platforms, applications, etc. has led to a substitute increase in the risks of DoS/DDoS attacks, cross-site scripting, spoofing, unauthorized access to data, and infection with malicious UIES programs.

It is noted in [14, 15, 16] that another relatively new challenge in the context of cybersecurity (including for educational institutions, authors), is the task of monitoring and analyzing users' digital footprints.

As it was shown in [17, 18], the analysis of digital footprints (hereinafter referred to as DF) of users (in particular, university teachers and students) is directly relevant to information security issues. This is due to the following factors: the analysis of DF allows to identify potential vulnerabilities in systems and behavioral patterns of users (patterns); analysis of DF helps to monitor and control the activity of users, which is important for detecting abnormal behavior or unauthorized access; the study of DF allows in some cases to improve the strategies of CS, taking into account the habits of users and the peculiarities of their interaction with information systems, etc. The analysis of DF helps to monitor and control the activity of users, which is important for detecting anomalous behavior or unauthorized access. Accordingly, according to the authors, DF analysis can play a key role in understanding threats and security issues in information systems. In our opinion, all the above-mentioned fully applies to the problem of ensuring IS (CS) of UIES, which makes new research in this area relevant.

Analyzing the DF of users in an UIES can involve various methods of finding patterns to extract useful information about the activities of students and teachers. One such method is behavior pattern analysis [19]. Such analysis in combination with data clustering methods, associative rules, machine learning methods, etc. Can help analyze many indicators, ranging from the sequence of user actions in the UIES to predicting the success of students in a particular course.

In [20], the authors discuss the possibility of using sequential pattern (pattern) and rule analysis, a subset of data mining techniques in analyzing CS notifications.

In [21], the authors present research results on sequential pattern mining (SPM), to obtain event sequences for all IP addresses in a corporate network. As the authors show in their work, sequences describing malicious user behavior in a corporate network are quite rare.

Each of the above methods has its own advantages and can be effective in analyzing the DF of users in an UIES. A combination of several methods can provide more accurate results.

III. The purpose and objectives of the study.

Supplement the method of sequential analysis of cybersecurity behavior patterns of users of the university information and education system (UIES) with a model of associative rule formation, where each information security event is represented as an element fixed in digital traces characterizing the behavioral patterns of UIES users.

IV. Methods and models

UIES cybersecurity (cyber risk) patterns are typical or characteristic patterns of user behavior. These patterns are related to data security, threat protection, and security compliance in the UIES. Such patterns include:

– *normal behavior. That is, they are patterns of actions that are typical for specific users or groups of users. For example, certain login times, sequence of access to certain UIES resources, typical requests and actions in the system;*

– *anomalous behavior. That is, deviations from typical patterns of behavior that may indicate potential threats to the UIES IS. This may include unusual attempts to access protected UIES resources (e.g., accounts), unusual requests, increased activity, or unauthorized attempts to log into the UIES;*

– *specific threat patterns. This includes patterns that characterize specific types of threats, such as internal or external user attacks, exploit or infiltration attempts, phishing, and other types of cyber attacks on the UIES;*

– *adaptive behavioral changes. This category includes patterns that reflect changes in user behavior over time or in response to security training. For example, users may adapt their behavior patterns to avoid detection or adapt to new security techniques used in the UIES.*

Studying and analyzing such patterns, including through the analysis of users' digital footprints, will enable UIES security systems to detect anomalies promptly, detect IS threats, and adapt to changes in threats, which will ultimately help ensure the UIES's IS and its robust defense against cyberattacks.

As shown in [19], the method of obtaining maximum consistent patterns of user behavior, e.g., in an UIES, is usually associated with sequence analysis techniques such as event sequence or time series analysis. This is because the analysis of user behavior in an UIES often considers sequences of actions or events that the user performs in the system. Sequential analysis techniques, such as frequent sequence or event sequence extraction algorithms, can be applied to extract such patterns of behavior. For example, associative analysis algorithms such as Apriori or FP-Growth [22] can be used to identify frequent sequences of user actions in the system.

In the context of UIES QA, sequential analysis techniques [20, 21] can be an important tool to detect anomalies, protect against threats, and improve the overall security of UIES. In particular, we note that:

Sequential analysis techniques can identify typical user activity patterns in the UIES. Changes in these patterns can indicate potential threats to the CS, such as unusual attempts to access sensitive data or unauthorized user actions in the UIES;

by analyzing DFs and user activity sequences in the UIES, unusual or malicious patterns can be identified that may indicate hacking attempts or cyberattacks on the UIES.

Thus, the use of sequential analysis techniques allows measures to be taken to strengthen UIES defenses, for example, by creating rules or algorithms that can automatically detect and respond to potential UIES SC threats.

Before outlining the mathematical calculations related to the description of user behavior patterns in the UIES in the context of its information security, let us briefly review the terminology that will be used below.

We believe that user behavior patterns are typical patterns or characteristics of actions that users exhibit when interacting with an UIES. In the context of IS and/or CS assurance, analyzing patterns Can be critical. Some typical patterns are summarized in Table I.

TABLE I
EXAMPLES OF TYPICAL USER BEHAVIOR PATTERNS THAT MAY BE RELEVANT TO THE SECURITY OF AN UIES

№	Conditional pattern name	Description
1	Access frequency and typical activity intervals	Users typically have specific time limits for accessing the UIES. Abnormal changes in access frequency may indicate compromise of UIES accounts.
2	Typical queries and operations in UIES	Examination of common user requests in the UIES, helps identify anomalous or suspicious activity. For example, attempts to change account settings in the UIES without prior authorization may indicate account compromise.
3	Location and devices	Analyzing where and from what devices users typically access the UIES can help identify anomalies. For example, logging into the UIES from unusual geographic locations or from an atypical device.
4	User response to security events	How UIES users respond to password change requests, two-factor authentication, and other IS measures can indicate their security awareness and/or the presence of threats.
	Etc.	

Then, an IS event when a user interacts with an UIES is any event or action that may affect the security of information in that system. IS events will be characterized by non-empty unique sets of attributes. Such attributes can include, for example, according to Table I: user, device, time, event type. And also additional (special attributes), which depend on the event type. Let's denote by E the set of all recorded events, i.e.: $E = \{e_1,..., e_n\}$, where $\{e_i\}, i = \overline{1,n} -$ individual IS events in the UIES; $n -$ capacity E .

A user session in an UIES, such as a learning management system (LMS) like Moodle, will be a time period during which the user interacts with the UIES. The session begins when the user logs into the UIES (i.e., authenticates) and ends when the user logs out or automatically terminates the session due to lack of user activity for a certain amount of time. From an IS (and/or CS) perspective, a session is critical because various activities can be performed during an active session, including accessing sensitive data, transferring information, performing operations, etc. Let us denote by S the set of all recorded sessions, i.e., $S = \{s_1,...,s_m\}$, where $\{s_i\}$, $i = \overline{1,m} -$ individual sessions in the UIES; $m -$ capacity S .

A session Can also be described as the placement of E elements without repetition: $s_i = \langle e_{i1},...,e_{ij} \rangle$, where $\{e_{ij}\}$, $i = \overline{1,m}$, $j = \overline{1,h_i} -$ a separate IS event within a single $i -$ session; $h_i -$ power of placement s_i .

The set E will be formed as the result of combining all the sets of sessions that were obtained from the facts of user activities in the UIES. Then if an IS event took place, it belongs to at least one session: $\forall e \in E, \exists_s \in S, e \in s$.

Note that in order to place E elements without repetition, their classification is required. Classes of IS and/or CS in UIES, define the levels of protection and security measures applied to ensure the integrity, confidentiality and availability of information in UIES. Then, a class of IS events Can be interpreted as an arbitrary set of IS events in an UIES, which will have certain properties or attributes. Let $C_E = \{c_1,...,c_l\}, \{c_i\} -$ be the set of all defined classes of IS events characteristic of UIES. There $i = \overline{1,l} -$ is an independent IS class; $l -$ power C_E . For example, the classes of IS (CS) in an UIES may include classes related to: authentication and access control; encryption and data protection; vulnerability management and protection against attacks; IS auditing and monitoring, and others.

Then the IS pattern (R) will be the placement of the elements of C_E with repetitions: $r_i = \langle c_{i1}...,c_{ij} \rangle$, $\{c_{ij}\}, i = \overline{1,q}, j = \overline{1,w_i}, c_{ij} \in C_E -$ a separate IS event for $i -$ the IS pattern; $q -$ the power; R w_i the power of the placement of r_i . Or, in other words, w_i is the set of events in a pattern of IS UIES. We believe that user behavior patterns Can be based on DF analysis, i.e., analysis that provides insight into how users interact with the UIES.

Each IS event in an UIES Can be described as a non-empty set of attributes U (e.g., failed UIES login attempts; unusual account activity; abnormal traffic; failure of UIES services or applications, and others). Accordingly, such a non-empty set, or set of IS event attributes, will be inherent to an object of the set E . We assume that all objects in E and attributes in S are different.

Note that the attribute sets of IS event attributes of an UIES may vary depending on the context and system specifics, but several common attributes can be characteristic of most recorded IS events in an UIES: timestamps (time and date when the IS event occurred); event source (user, application, device, etc.); event type (e.g., login attempt, configuration change, etc.); importance level; event outcome; and additional attributes. Most of these attributes can be established based on the analysis of user DFs in the UIES.

Sequential analysis in information security is aimed at identifying regularities and patterns in the sequences of events occurring in the UIES. The method of searching for patterns in sequences of IS events in the UIES can be used to analyze and predict possible future IS events based on past actions of the UIES user. That is, in fact, the DFs associated with cybersecurity (or dangerous) patterns of user behavior in the UIES are analyzed. The main essence of the method is as follows:

Step 1: Obtaining data. First, it is necessary to collect data on IS events, including DF-based data. This data may include audit logs, system logs, access data, and other information resources.

Step 2: Representation as sequences. The IS event data is converted into sequences (e.g., as associative rules), where each IS event is represented as an element of a sequence of user behavioral patterns. For example, if login attempts are analyzed, each user login attempt will be a separate element of the sequence.

Step 3: Extracting patterns and regularities. Next, sequence analysis techniques are applied to identify frequently occurring patterns of cybersecurity (cyber risk) user behavior in the UIES, sequences of events or combinations of events. This can be done using various algorithms such as sequence mining or frequent subsequence mining algorithms.

Step 4: Build a model and predict patterns of user behavior in the UIES. Based on the identified patterns, models can be used to predict future events or detect abnormal patterns of cybersecurity (cyber risk) user behavior in the UIES.

Step 5: Evaluation and optimization. The method of finding patterns in IS event sequences requires continuous evaluation and optimization of models, as user behavior and UIES can change over time.

Within the framework of this work, we note that the goal of sequential analysis of users' digital footprints in an UIES is to obtain frequently occurring subsequences of classes of information security events in a given session S of a user. Therefore, based on [19, 23], we propose an augmented model for searching for patterns of cyber-secure (cyber-dangerous) behavior of users in the UIES during a session.

Suppose that $\chi_p^{s'}$ is the value of the membership function $i -$ of a pattern's associative feature (R). This value Can be calculated as the number of non-overlapping ordered occurrences of P in a single session s' . I.e. $S' -$ is the set of all saved user sessions in the UIES (after filtering and classification according to the criteria of cyber-secure (cyber-dangerous) behavior). Then $S' = \{s_1^{'},..., s_m^{'}\}$ where $\{s_1^{'}\}$, $i = \overline{1,m} -$ is a separate session; m is the capacity of S' .

According to [19, 23] associative rules in data analysis are generalized statements about associations between different elements of the data set. Then, the associative rule $A = (X,Y)$ on the set of IS UIES IS features we will assume dependencies characterizing the functions: $\sup(X \Rightarrow Y)$ - support, $conf(X \Rightarrow Y)$ - trustworthiness. When analyzing the DF of users in UIES, associative rules can be applied by IS analysts to identify patterns and relationships between different IS actions or events. Support ($\sup(X \Rightarrow Y)$) in associative rules determines how often a set of items (or IS events) appear together in a common data set. It is measured as the frequency of occurrence of that set in the common data. The greater the support, the more important this set is for associative rule generation. Correspondingly, Confidence ($conf(X \Rightarrow Y)$) will show how often a rule is true when the first set of elements is encountered, i.e. Confidence is defined as the probability of the second set appearing given that the first set is encountered. In Table II, we provide some examples of such associative rules characterizing cyber risky and cyber insecure user behavior in UIES.

TABLE II
EXAMPLES OF ASSOCIATIVE RULES CHARACTERIZING CYBER RISKY AND CYBER INSECURE BEHAVIOR OF USERS IN UIES

An example of associative rules for cyber risk behavior:	An example of associative rules for cybersecurity behavior:
Pattern: A user often opens email attachments from unknown sources in the UIES. Associative rule: If a user opens attachments from unknown senders in the UIES, they may be putting the system at risk. Support $(\sup)$: 70% Credibility $(conf)$: 80%	**Pattern**: The user always terminates the session and logs out of the UIES when finished. Associative rule: If the user has completed work, the user ends the session and logs out. Support $(\sup)$: 80% Credibility $(conf)$: 90%
Pattern: User ignores warnings about dangerous actions in the UIES. Associative rule: If a user ignores warnings, there is an increased risk of unsafe behavior. Support $(\sup)$: 65% Credibility $(conf)$: 75%	**Pattern**: The user always authenticates to the UIES before accessing sensitive data. Associative rule: If a user accesses sensitive data, the user is authenticated. Support $(\sup)$: 75% Reliability $(conf)$: 85%

Applying these concepts to the IS (IS) patterns of an UIES would involve analyzing sequences of user actions. For example, detecting patterns of typical secure login to an UIES or sequences of actions that indicate anomalous user activity. Using $\sup(X \Rightarrow Y)$ and $conf(X \Rightarrow Y)$, the most relevant IS patterns can be picked out and potential threats in the UIES can be identified. The support and validity of $A = (X, Y)$ builds on the support of the multiple attributes of U , discussed above. The task associated with finding consistent patterns of cyber-secure (cyber-threatening) user behavior in the UIES is to detect the maximum sequences that have support above a given threshold for $\sup$ and $conf$. In order to classify IS events it is necessary to calculate the validity of the rule, i.e. $conf(X \Rightarrow Y) = \max f(E \to C_E)$.

In the context of IS UIES IS, the IS event pattern length and session length are important to us. These parameters can be important for access control, authentication, and IS provisioning of an UIES. Short sessions can improve security because they reduce the time in which an attacker can capture credentials or gain access to the system, while long sessions can be convenient for users but can create vulnerabilities. Determining the length of an IS event pattern is also important for effective IS monitoring of an UIES. This parameter can help an IS incident detection and intrusion prevention system (IDS/IPS) recognize and respond to certain scenarios or anomalies in the UIES based on known behavior patterns or characteristics of certain events.

Let us represent $\sup(X \Rightarrow Y)$ through the number of occurrences of patterns (r) in a single session s' - $\gamma_p^{s'}$, i.e.:

$$\gamma_p^{s'} = \left(\chi_p^{s'} \cdot z\right) \Big/ d \, , 0 \le \gamma_p^{s'} \in \qquad (1)$$

where z — is the length of the IS event pattern in the UIES; d – is the length of the user session in the UIES.

Note that the length of an IS event pattern in an UIES is usually determined by the number of characters, bytes, or bits that represent the event itself or a piece of security-related information in the UIES. This can be a set of defined parameters, a sequence of events, or specific data monitored or logged in a security monitoring system, e.g., using IDS/IPS - Splunk, Suricata, or others). Accordingly, the length of the user's session in the UIES (the length of an UIES session is generally defined as the period of time that a user remains connected or active in the UIES and may be measured, for example, in minutes or hours, or in actions, such as the number of requests to the UIES or user activity).

The number of sessions of a particular UIES user during, for example, a calendar year or an individual semester may be different. Accordingly, there is a need to aggregate the support value [23]. The value characterizing the total support for a user's cyber risk behavior pattern in an UIES can be calculated as follows:

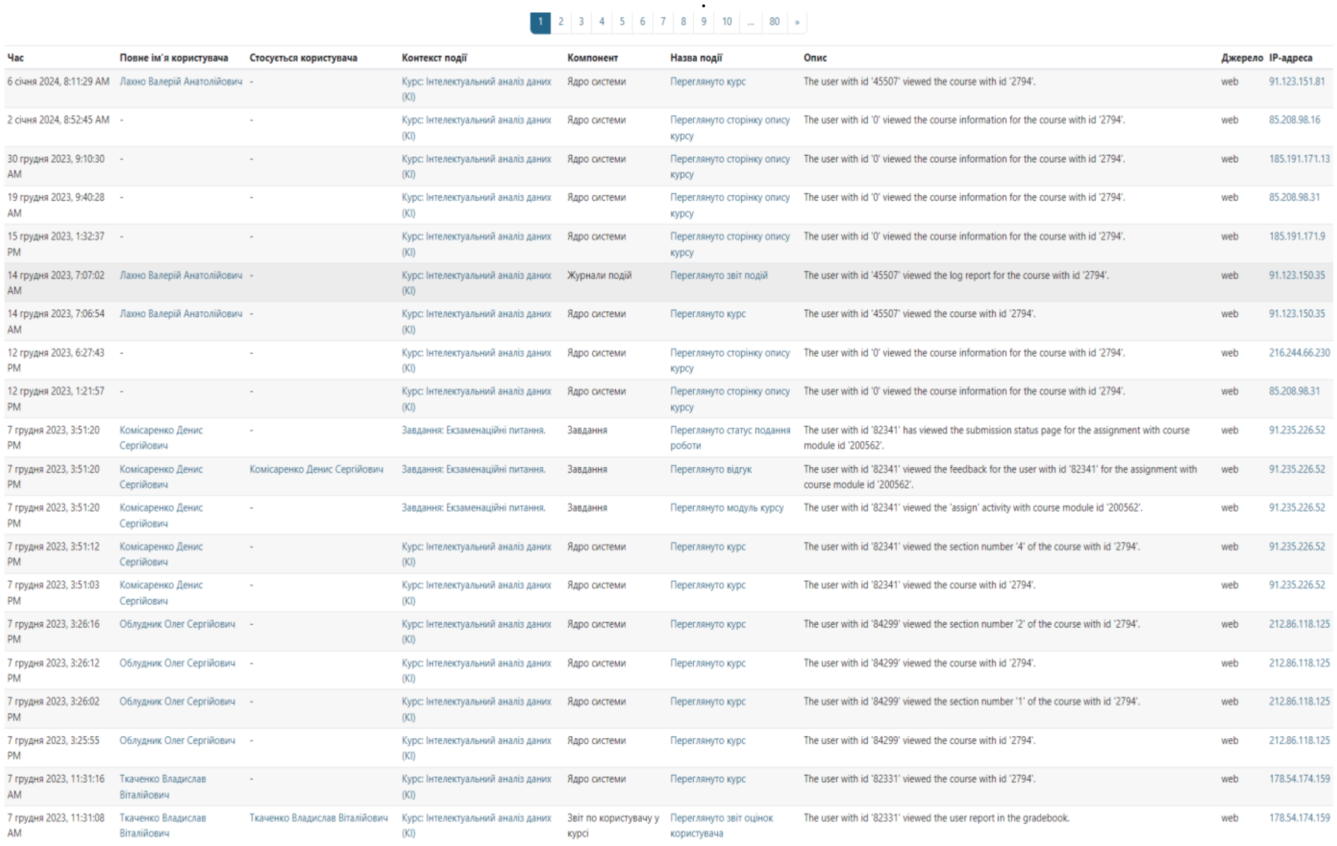
$$\gamma_p^{s'} = \sum_{i=1}^{m} \left(\left(\left(\chi_p^{s'} \cdot z\right) \Big/ d_i \right) \cdot \left(d_i \Big/ n' \right) \right) \le \gamma_p^{S'} \in \mathbb{R} \le 1, \qquad (2)$$

where n' – is the total number of user sessions in the UIES during, for example, a semester or academic year (after classification and filtering).

Dependencies (1) and (2) allow determining the value of support for different sequential patterns of cyberthreat (cybersecurity) behavior of users in the UIES. This will allow describing the support value as a share of the content of a pattern of cyber-secure (cyber-dangerous) user behavior in the UIES during a session.

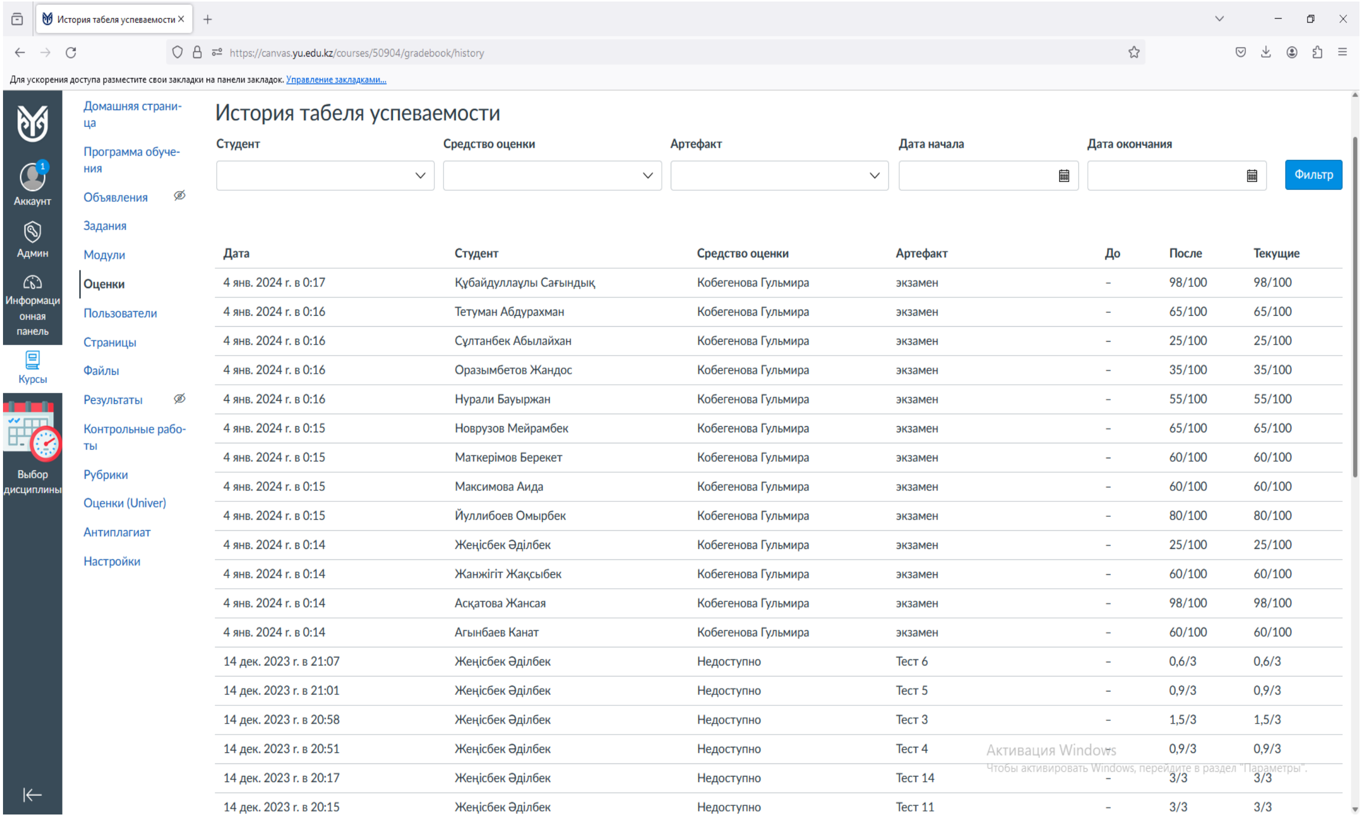
V. THE EXPERIMENT

The raw data for the analysis of DFs related to cybersecurity patterns of user behavior in UIES were taken from 3 different information and education systems of three universities in two countries. These learning management system (LMS)) are: Moodle - National University of Bioresources and Nature Management of Ukraine (Ukraine), see Fig. 1 a); LMS Canvas - Esenov University (Kazakhstan), see Fig. 1 b); Microsoft Teams - State Trade and Economic University (Ukraine), see Fig. 1 c).



Час	Повне ім'я користувача	Стосується користувача	Контекст події	Компонент	Назва події	Опис	Джерело	IP-адреса
6 січня 2024, 8:11:29 AM	Лахно Валерій Анатолійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '45507' viewed the course with id '2794'.	web	91.123.151.81
2 січня 2024, 8:52:45 AM	-	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто сторінку опису курсу	The user with id '0' viewed the course information for the course with id '2794'.	web	85.208.98.16
30 грудня 2023, 9:10:30 AM	-	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто сторінку опису курсу	The user with id '0' viewed the course information for the course with id '2794'.	web	185.191.171.13
19 грудня 2023, 9:40:28 AM	-	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто сторінку опису курсу	The user with id '0' viewed the course information for the course with id '2794'.	web	85.208.98.31
15 грудня 2023, 1:32:37 PM	-	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто сторінку опису курсу	The user with id '0' viewed the course information for the course with id '2794'.	web	185.191.171.9
14 грудня 2023, 7:07:02 AM	Лахно Валерій Анатолійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Журнали подій	Переглянуто звіт подій	The user with id '45507' viewed the log report for the course with id '2794'.	web	91.123.150.35
14 грудня 2023, 7:06:54 AM	Лахно Валерій Анатолійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '45507' viewed the course with id '2794'.	web	91.123.150.35
12 грудня 2023, 6:27:43 PM	-	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто сторінку опису курсу	The user with id '0' viewed the course information for the course with id '2794'.	web	216.244.66.230
12 грудня 2023, 1:21:57 PM	-	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто сторінку опису курсу	The user with id '0' viewed the course information for the course with id '2794'.	web	85.208.98.31
7 грудня 2023, 3:51:20 PM	Комісаренко Денис Сергійович	-	Завдання: Екзаменаційні питання.	Завдання	Переглянуто статус подання роботи	The user with id '82341' has viewed the submission status page for the assignment with course module id '200562'.	web	91.235.226.52
7 грудня 2023, 3:51:20 PM	Комісаренко Денис Сергійович	Комісаренко Денис Сергійович	Завдання: Екзаменаційні питання.	Завдання	Переглянуто відгук	The user with id '82341' viewed the feedback for the user with id '82341' for the assignment with course module id '200562'.	web	91.235.226.52
7 грудня 2023, 3:51:20 PM	Комісаренко Денис Сергійович	-	Завдання: Екзаменаційні питання.	Завдання	Переглянуто модуль курсу	The user with id '82341' viewed the 'assign' activity with course module id '200562'.	web	91.235.226.52
7 грудня 2023, 3:51:12 PM	Комісаренко Денис Сергійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '82341' viewed the section number '4' of the course with id '2794'.	web	91.235.226.52
7 грудня 2023, 3:51:03 PM	Комісаренко Денис Сергійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '82341' viewed the course with id '2794'.	web	91.235.226.52
7 грудня 2023, 3:26:16 PM	Облудник Олег Сергійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '84299' viewed the section number '2' of the course with id '2794'.	web	212.86.118.125
7 грудня 2023, 3:26:12 PM	Облудник Олег Сергійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '84299' viewed the course with id '2794'.	web	212.86.118.125
7 грудня 2023, 3:26:02 PM	Облудник Олег Сергійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '84299' viewed the section number '1' of the course with id '2794'.	web	212.86.118.125
7 грудня 2023, 3:25:55 PM	Облудник Олег Сергійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '84299' viewed the course with id '2794'.	web	212.86.118.125
7 грудня 2023, 11:31:16 AM	Ткаченко Владислав Віталійович	-	Курс: Інтелектуальний аналіз даних (КІ)	Ядро системи	Переглянуто курс	The user with id '82331' viewed the course with id '2794'.	web	178.54.174.159
7 грудня 2023, 11:31:08 AM	Ткаченко Владислав Віталійович	Ткаченко Владислав Віталійович	Курс: Інтелектуальний аналіз даних (КІ)	Звіт по користувачу у курсі	Переглянуто звіт оцінок користувача	The user with id '82331' viewed the user report in the gradebook.	web	178.54.174.159

a) LMS Moodle Log Viewer Page

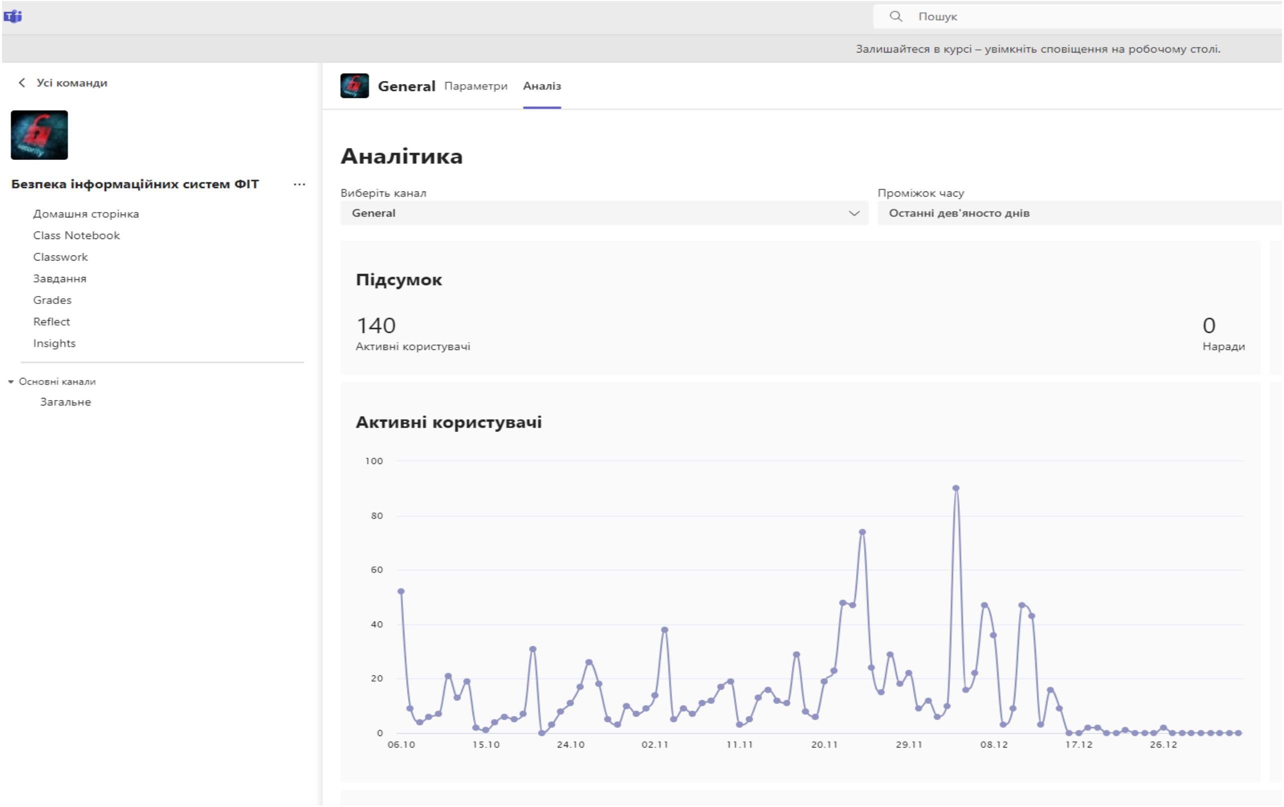


История табеля успеваемости

Студент:
Средство оценки:
Артефакт:
Дата начала:
Дата окончания:

Дата	Студент	Средство оценки	Артефакт	До	После	Текущие
4 янв. 2024 г. в 0:17	Құбайдуллаұлы Сағындық	Кобегенова Гульмира	экзамен	–	98/100	98/100
4 янв. 2024 г. в 0:16	Тетуман Абдурахман	Кобегенова Гульмира	экзамен	–	65/100	65/100
4 янв. 2024 г. в 0:16	Сұлтанбек Абылайхан	Кобегенова Гульмира	экзамен	–	25/100	25/100
4 янв. 2024 г. в 0:16	Оразымбетов Жандос	Кобегенова Гульмира	экзамен	–	35/100	35/100
4 янв. 2024 г. в 0:16	Нурали Бауыржан	Кобегенова Гульмира	экзамен	–	55/100	55/100
4 янв. 2024 г. в 0:15	Новрузов Мейрамбек	Кобегенова Гульмира	экзамен	–	65/100	65/100
4 янв. 2024 г. в 0:15	Маткерімов Берекет	Кобегенова Гульмира	экзамен	–	60/100	60/100
4 янв. 2024 г. в 0:15	Максимова Аида	Кобегенова Гульмира	экзамен	–	60/100	60/100
4 янв. 2024 г. в 0:15	Йуллибоев Омырбек	Кобегенова Гульмира	экзамен	–	80/100	80/100
4 янв. 2024 г. в 0:14	Жеңісбек Әділбек	Кобегенова Гульмира	экзамен	–	25/100	25/100
4 янв. 2024 г. в 0:14	Жанжігіт Жақсыбек	Кобегенова Гульмира	экзамен	–	60/100	60/100
4 янв. 2024 г. в 0:14	Асқатова Жансая	Кобегенова Гульмира	экзамен	–	98/100	98/100
4 янв. 2024 г. в 0:14	Агынбаев Канат	Кобегенова Гульмира	экзамен	–	60/100	60/100
14 дек. 2023 г. в 21:07	Жеңісбек Әділбек	Недоступно	Тест 6	–	0,6/3	0,6/3
14 дек. 2023 г. в 21:01	Жеңісбек Әділбек	Недоступно	Тест 5	–	0,9/3	0,9/3
14 дек. 2023 г. в 20:58	Жеңісбек Әділбек	Недоступно	Тест 3	–	1,5/3	1,5/3
14 дек. 2023 г. в 20:51	Жеңісбек Әділбек	Недоступно	Тест 4	–	0,9/3	0,9/3
14 дек. 2023 г. в 20:17	Жеңісбек Әділбек	Недоступно	Тест 14	–	3/3	3/3
14 дек. 2023 г. в 20:15	Жеңісбек Әділбек	Недоступно	Тест 11	–	3/3	3/3

b) LMS Canvas log view page



Виберіть канал: General

Проміжок часу: Останні дев'яносто днів

140 Активні користувачі

0 Наради

c) *c) Page of viewing logs in Microsoft Teams*

Fig. 1. Log view pages for different UIESs

To analyze the DF, a script was developed in the algorithmic language Pytnon, which allowed us to practically test the proposed model. Below is the structure of the pattern that describes cyberthreatening actions of a user in the UIES.

```
class CyberSecurityPattern:
    def __init__(self):
        self.user_actions = []
    def track_user_action(self, action):
        self.user_actions.append(action)
    def analyze_digital_footprint(self):
        # Here we Can implement the analysis
        # of digital traces of an UIES user
        #, For example, checking typical actions,
        # of UIES resource utilization templates and others
        pass
# Example of use
cyber_pattern = CyberSecurityPattern()
cyber_pattern.track_user_action("login_attempt")
cyber_pattern.track_user_action("file_download")
cyber_pattern.track_user_action("data_transfer")
cyber_pattern.analyze_digital_footprint()
```

The above code creates a CyberSecurityPattern class that allows tracking user actions in the UIES and analyzing their digital footprints. As part of the research, various cyber risk (cybersecurity) patterns were tested by adding specific functions to analyze user actions in the UIES.

Then the scheme of obtaining and analyzing patterns of cyber-secure (cyber-dangerous) user behavior in the UIES based on the analysis of their digital traces will look like this, see Fig. 2.

Given that user behavior is represented by sequences of actions, the sequential analysis method allows the system to efficiently process categorical data associated with sequential patterns of UIES user actions. Analyzing sequential patterns allows the system to identify more complex threats that may be hidden in chains of actions, not just individual events. Conceptually, the Pytnon code for analyzing logs (digital traces) describing patterns of cyberthreat behavior of users in an UIES would look like this:

```
#There is a log file in CSV or text format, where each line represents
a log entry
# Example string: timestamp, user_id, action_type,
resource_accessed

# Loading the log file
def load_logs(file_path):
    logs = []
    with open(file_path, 'r') as file:
        for line in file:
            # Splitting the log line into separate fields (may need to be
adapted depending on the format)
            log_entry = line.strip().split(',')
            logs.append(log_entry)
    return logs
```

```
# Example of log analysis to identify resource access patterns
def analyze_logs(logs):
    user_actions = {} # Dictionary for storing user actions
    for logs in logs:
        timestamp, user_id, action_type, resource_accessed = log
        # Check if a record exists for this user
        if user_id not in user_actions:
            user_actions[user_id] = []
        # Adding an action to a user record
        user_actions[user_id].append({'timestamp': timestamp, 'action_type': action_type, 'resource': resource_accessed})
    return user_actions

# Example of use
log_file_path = 'path_to_log_file.log'
logs = load_logs(log_file_path)
user_actions = analyze_logs(logs)

# Example of outputting user access patterns
for user_id, actions in user_actions.items():
    print(f "User {user_id}:")
    for action in actions:
        print(f "Timestamp: {action['timestamp']}, Action: {action['action_type']}, Resource: {action['resource']}")
```

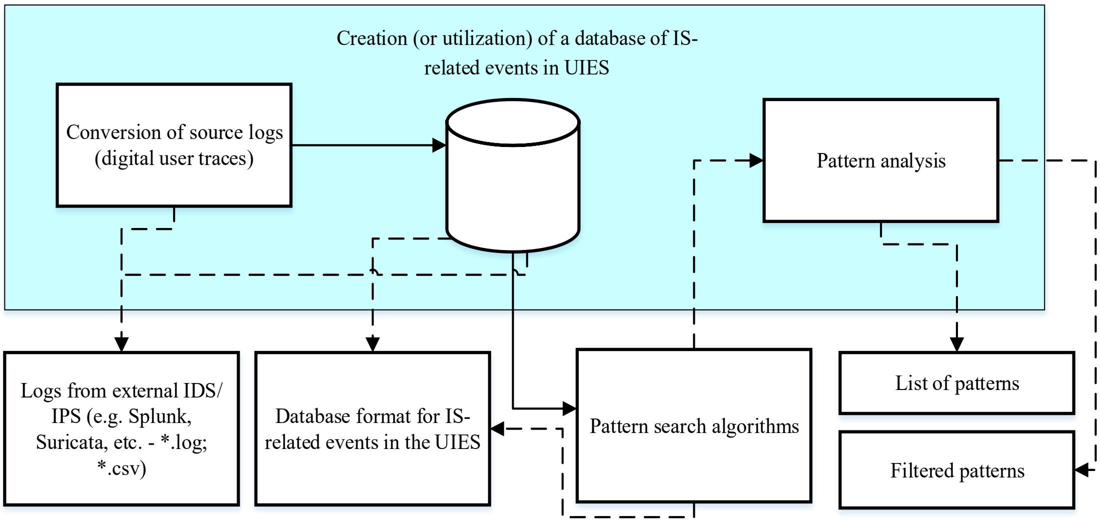

Creation (or utilization) of a database of IS-related events in UIES
Conversion of source logs (digital user traces)
Pattern analysis
Logs from external IDS/ IPS (e.g. Splunk, Suricata, etc. - *.log; *.csv)
Database format for IS-related events in the UIES
Pattern search algorithms
List of patterns
Filtered patterns

Fig. 2. Scheme for obtaining and analyzing patterns of cybersecurity (cyber risk) user behavior in UIES based on the analysis of their digital traces

The above code shows the steps for loading logs from a file, analyzing user actions in the UIES, and outputting resource access patterns. In reality, the algorithms for analyzing and processing data may be more complex and depend on the specific goals of the UIES security analysis.

To test the model, patterns of cyber-dangerous and cyber-secure behavior of users in the system were generated, see Table 3. In total, more than 200 patterns were generated.

TABLE III
EXAMPLES OF LOGS (DIGITAL TRACES) FOR PATTERNS CHARACTERIZING CYBER RISK AND CYBERSECURITY BEHAVIOR OF USERS IN UIES

Cyber Risk Behavior	Cybersecurity behavior
[Date and Time]: 2024-01-06 11:45:32 [Event]: Attempted to download a file containing a virus [User]: User_Name_2 [Action]: Click on a malicious link [Description]: Identify suspicious email, refuse to enter personal information.	[Date and Time]: 2024-01-06 10:15:23 [Event]: Successful authentication [User]: User_Name [Action]: Successful login to the university system [Description]: Enter correct credentials. Multi-factor authentication.

The experiments evaluated the maximum sets for which the support of $\sup(\{r_1,...,r_n\}) \geq \text{minsupp}$ was computed and for $\forall C_E$ the classification of items based on the rule $\sup(\{r_1,...,r_n,C_E\}) \geq \text{minsupp}$ [24] is performed. A series of tests for cyber risk behavior patterns of users based on the analysis of their DFs were performed for different values of the support level factor $0{,}01 \leq \text{minsupp} \leq 1$. The results are shown in Figure 3, which shows the maximum pattern extraction time $(t, \sec)$ as a function of the support level value $(\text{minsupp}, \%)$.

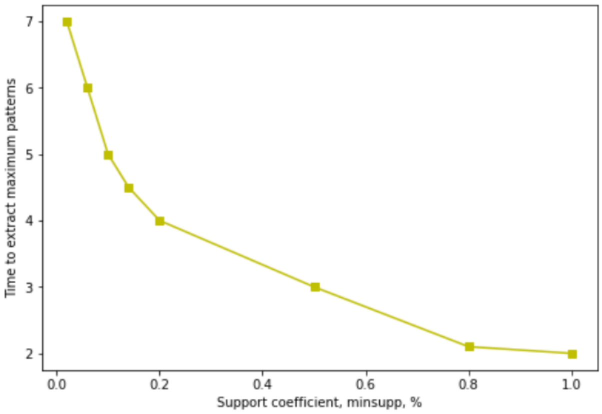


Fig. 3. Extraction time of maximum $(t, \sec)$ patterns depending on the support level value $(\text{minsupp}, \%)$

Fixing the time of extracting maximum patterns from support level values was performed using the time library. Below is a small code fragment for measuring the time of extract_max_patterns function execution for different support levels.

```
import time
from itertools import combinations

# Function to extract the maximum patterns
def extract_max_patterns(data, support_level):
  patterns = []
  for i in range(len(data)):
    for j in range(i + 1, len(data)):
      pattern = data[i:j+1]
      # Checking for pattern support
      support = sum(1 for seq in data if all(item in seq for item in pattern))
      if support >= support_level and all(p not in pattern for p in patterns):
        patterns.append(pattern)
  return patterns

# Generating data for testing
data = [....]
# Support level values for testing
support_levels = [...]

# Measuring pattern retrieval time for different support levels
for level in support_levels:
  start_time = time.time()
  patterns = extract_max_patterns(data, level)
  end_time = time.time()
  print(f "Support level: {level}, Execution time: {end_time - start_time}
seconds")
```

The database of patterns characterizing cyber risk and cybersecurity behavior of users in UIES is still in the stage of formation, so the best value of the length of the generated sequential patterns has not been experimentally investigated yet.

VI. Discussion of the Results of Experimental Studies

As shown in Figure 3, the best results were obtained for *minsupp = 0,02*. However, at this stage of the study, we did not compare the proposed approach with other methods, such as those outlined in [19, 20, 21, 23], which also identify maximum patterns with a minimum support value. Improving the efficiency of the search for maximal consistent patterns allows for faster detection of user behavior characteristics. Optimization of search algorithms, as shown in [19, 20, 21, 23] will reduce the reduction of processing time, which is important for rapid response to potential security threats to the UIES. Reducing the support level leads to an increase in the number of patterns, as a lower threshold is set for including sequences in the analysis results. This corresponds to the task of finding sequential patterns with support above a given threshold: when this threshold is lowered, sequences that may have been previously excluded due to insufficient support appear in the results. However, it is important to consider the balance between the number of patterns retrieved and their relevance for detecting UIES IS threats. Improving the efficiency of the search should be accompanied by an analysis of the retrieved patterns for their relevance and potential threat to the UIES IS.

The proposed model still requires more detailed program development. At this stage, the goal was to confirm or deny the performance of this approach in general for the analysis of digital traces associated with cybersecurity patterns of behavior of users of university information and education systems. As the preliminary results have shown, this approach will allow us to work effectively with categorical input information in the course of extracting associative dependencies related to cyber-secure or cyber-dangerous behavior of UIES users, and, accordingly, to make more rational decisions to ensure the IS and CS of UIES at lower time costs. Another promising area of research seems to us to combine DF analysis methods with the concept of using a digital twin in the field of education, which will allow us not only to more accurately and quickly identify threats to the IS UIES, but also to create a learning environment that is optimized from the point of view of IS and quality of education. However, this direction requires separate research.

Conclusion

The study found that the method of obtaining maximum sequential patterns of cybersecure user behavior based on sequential analysis of digital footprint (DF) has many advantages in ensuring information security (IS) of the university information and education system (IES). In particular, the use of the approach proposed in this paper based on the method of obtaining maximum sequential patterns of cybersecurity user behavior based on sequential analysis of DF allows to detect anomalous user behavior. And this can indicate potential threats to the IS of UIES. It is also shown that sequential DF analysis will allow the system to detect new or previously unknown IS threats, as the UIES and its security loops can quickly adapt to changes in user behavior patterns. It is shown that by examining consistent patterns of cyber threat user behavior, typical system usage scenarios can be identified, facilitating the identification of normal user behavior from abnormal behavior. Sequential pattern data can further be used to improve machine learning models, which will enable the IS UIES system to become more accurate in detecting threats and taking preventive IS measures. Thus, the use of the DF sequential analysis method will improve the ability of the IS UIES system to detect and respond to IS threats on time, as well as allow for more efficient processing and analysis of categorical data on user actions in the UIES.

References

[1] Bandara, I., Ioras, F., & Maher, K. (2014). Cyber security concerns in e-learning education. In ICERI2014 Proceedings (pp. 728-734). https://doi.org/10.13140/2.1.4451.3604

[2] Bongiovanni Ivano, The least secure places in the universe? A systematic literature review on information security management in higher education, Computers & Security, Volume 86, 2019, Pages 350-357, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.07.003

[3] Garrison, Chlotia & Ncube, C. (2010). Lessons Learned from University Data Breaches. Palmetto Business and Economic Review. 13. 27-37.

[4] FireEye, Inc. Cyber tHreats to the Education Industry. White Paper. Library DFtalog, 2016. Available online: www.fireeye.com (accessed on January 28, 2021).

[5] Yilmaz, Rustu & Yalman, Yıldıray. (2016). A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. TEM Journal. 5. 180-191. https://doi.org/10.18421/TEM52-10

[6] Adams, A.; Blanford, A. Security and Online Learning: To Protect and Prohibit. In Usability Evaluation of Online Learning Programs; UK: IDEA Publishing,, 2003; pp. 331-359.

[7] Beaudin, K. (2017), The Legal Implications of Storing Student Data: Preparing for and Responding to Data Breaches. New Directions for Institutional Research, 2016: 37-48. https://doi.org/10.1002/ir.20202.

[8] Beaudin, K. College and university data breaches: Regulating higher education cybersecurity under state and federal law. J. Coll. Univ. Law 2015, 41, 657-693.

[9] Hussain, H.S.; Din, R.; Khidzir, N.Z.; Daud, K.A.M.; Ahmad, S. Risk and Threat via Online Social Network among Academia at Higher Education. Journal of Physics: Conference Series, Volume 1018, 1st International Conference on Big Data and Cloud Computing (ICoBiC) 2017 25–27 November 2017, Kuching, Sarawak, Malaysia, 012008. https://doi.org/10.1088/1742-6596/1018/1/012008

[10] Ulven, Joachim Bjørge, and Gaute Wangen. 2021. "A Systematic Review of Cybersecurity Risks in Higher Education" *Future Internet* 13, no. 2: 39. https://doi.org/10.3390/fi13020039

[11] Diaz, A.; Sherman, A.T.; Joshi, A. Phishing in an Academic Community: A Study of User Susceptibility and Behavior. arXiv 2018, https://arxiv.org/pdf/1811.06078.pdf

[12] Cuchta, Tom & Blackwood, Brian & Devine, Thomas & Niichel, Robert & Daniels, Kristina & Lutjens, Caleb & Maibach, Sydney & Stephenson, Ryan. (2019). Human Risk Factors in Cybersecurity. In Proceedings of the 20th Annual SIG Conference on Information Technology Education, Tacoma, WA, USA, October 3-5, 2019; pp. 87-92. https://doi.org/10.1145/3349266.3351407

[13] Alexei, Arina & Alexei, Anatolie. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. International Journal of Scientific & Technology Research. Volume 10. 128-133.

[14] Fertik, M., & Thompson, D. (2015). The reputation economy: How to optimize your digital footprint in a world where your reputation is your most valuable asset. Hachette UK.

[15] France Belanger, Robert E. Crossler, Dealing with digital traces: Understanding protective behaviors on mobile devices, The Journal of Strategic Information Systems, Volume 28, Issue 1, 2019, Pages 34-49, ISSN 0963-8687, https://doi.org/10.1016/j.jsis.2018.11.002

[16] Gregory Vial, Reflections on quality requirements for digital trace data in IS research, Decision Support Systems, Volume 126, 2019, 113133, ISSN 0167-9236, https://doi.org/10.1016/j.dss.2019.113133.

[17] Mary-Jane Sule, Marco Zennaro, Godwin Thomas, Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends, Technology in Society, Volume 67, 2021, 101734, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2021.101734

[18] Curtotti, D., Nocerino, W., & Pallante, C. (2023, September). University of Foggia: Promoting an Interdisciplinary Path in Security Issues, from the Crime Scene to Cyber Security. In IAI ACADEMIC CONFERENCE PROCEEDINGS (p. 21).

[19] Kureychik, V. V., Bova, V. V., & Kravchenko, Yu. A. (2020). Metod poiska posledovatelnykh patternov povedeniya polzovateley v internet-prostranstve. Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskie nauki, (4 (214)), 6-21.

[20] Martin Husák, Jaroslav Kašpar, Elias Bou-Harb, and Pavel Čeleda. 2017. On the Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 22, 1–10. https://doi.org/10.1145/3098954.3098981

[21] Anna L. Buczak, Daniel S. Berman, Sean W. Yen, Lanier A. Watkins, Lien T. Duong, and Jeffrey S. Chavis. 2017. Using sequential pattern mining for common event format (CEF) cyber data. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research (CISRC '17). Association for Computing Machinery, New York, NY, USA, Article 2, 1–4. https://doi.org/10.1145/3064814.3064822

[22] M. Hossain, A. H. M. S. Sattar and M. K. Paul, "Market Basket Analysis Using Apriori and FP Growth Algorithm," 2019 22nd International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2019, pp. 1-6, https://doi.org/10.1109/ICCIT48885.2019.9038197

[23] Wedyan, Suzan. (2014). Review and Comparison of Associative Classification Data Mining Approaches. International Journal of Computer, Information, Systems and Control Engineering, 2014, Vol. 8, pp. 34-45. https://doi.org/10.5281/zenodo.1336440

[24] Fournier-Viger, P., Wu, CW., Tseng, V.S. (2013). Mining Maximal Sequential Patterns without Candidate Maintenance. In: Motoda, H., Wu, Z., Cao, L., Zaiane, O., Yao, M., Wang, W. (eds) Advanced Data Mining and Applications. ADMA 2013. Lecture Notes in Computer Science(), vol 8346. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-53914-5_15

[25] Lakhno, V., Akhmetov, B., Smirnov, O., Chubaievskyi, V., Khorolska, K., Bebeshko, B. (2023). Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm. In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. Springer, Singapore. https://doi.org/10.1007/978-981-19-1844-5_2

[26] Lakhno, V. et al. (2023). The Model of Server Virtualization System Protection in the Educational Institution Local Network. In: Shakya, S., Papakostas, G., Kamel, K.A. (eds) Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-99-0835-6_33

[27] B. Bebeshko, K. Khorolska and A. Desiatko, "Analysis and Modeling of Price Changes on the Exchange Market Based on Structural Market Data," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021, pp. 151-156, https://doi.org/10.1109/PICST54195.2021.9772208

[28] Mathew, Alex. (2023). The Power of Cybersecurity Data Science in Protecting Digital Footprints. Cognizance Journal of Multidisciplinary Studies. 3. 1-4. https://doi.org/10.47760/cognizance.2023.v03i02.001

[29] Mazhar, Tehseen & Talpur, Dhani Bux & Hanif, Saba & Ullah, Inam & Adhikari, Deepak & Anwar, M.. (2023). Analysis of Cybersecurity Issues and Solutions in Education. https://doi.org/10.1201/9781003369042-5

[30] V. Lakhno, V. Malyukov, B. Akhmetov, B. Yagaliyeva, O. Kryvoruchko and A. Desiatko, "University Distributed Computer Network Vulnerability Assessment," 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST), Astana, Kazakhstan, 2023, pp. 141-144, https://doi.org/10.1109/SIST58284.2023.10223501

[31] B.S. Akhmetov, V. Lakhno, B.B. Akhmetov, A. Zhilkishbayev, N. Izbasova, O. Kryvoruchko, A. Desiatko, Application of a Genetic Algorithm for the Selection of the Optimal Composition of Protection Tools of the Information and Educational System of the University, Procedia Computer Science, Volume 215, 2022, Pages 598-607, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.062.

[32] Buriachok, V., Korshun, N., Zhyltsov, O., Sokolov, V., Skladannyi, P. (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspa, G. (eds) Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-031-35467-0_32

[33] Khorolska, K., Bebeshko, B., Desiatko, A., & Lazorenko, V. (2021). 3D models classification with use of convolution neural network. Paper presented at the CEUR Workshop Proceedings, 3179 25-34. http://ceur-ws.org/Vol-3179/Paper_3.pdf

[34] Khorolska, K., Lazorenko, V., Bebeshko, B., Desiatko, A., Kharchenko, O., Yaremych, V. (2022). Usage of Clustering in Decision Support System. In: Raj, J.S., Palanisamy, R., Perikos, I., Shi, Y. (eds) Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol 213. Springer, Singapore. https://doi.org/10.1007/978-981-16-2422-3_49

[35] Bandara, Indrachapa & Ioras, Florin. (2022). Higher education strategy to reduce an organization's digital carbon footprint derived from cybersecurity policies. https://doi.org/10.21125/edulearn.2022.2209

[36] Hakimi, Musawer & Quchi, Mohammad Mustafa & Fazil, Abdul Wajid. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID). 3. 20-33. https://doi.org/10.58471/esaprom.v3i01.3832

[37] Mincewicz, Wojciech. (2023). Education in the field of cybersecurity at universities in poland. Zeszyty Naukowe SGSP. 86. 117-125. https://doi.org/10.5604/01.3001.0053.7149

[38] Biloshchytskyi, A., Tsiutsiura, S., Kuchansky, A., Serbin, O., Tsiutsiura, M., Biloshchytska, S., & Faizullin, A. (2022). Development of mathematical models of the project-vector space of educational environments. Eastern-European Journal of Enterprise Technologies, 5(4(119), 50–61. https://doi.org/10.15587/1729-4061.2022.266262

[39] A. Peleschyshyn, R. Korzh, O. Trach and M. Tsiutsiura, "Building of Information Activity Management System of Higher Educational Establishment in the Social Environments of the Internet," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 58-61, https://doi.org/10.1109/AIACT.2019.8847912

[40] R. Korzh, A. Peleshchyshyn, O. Trach and M. Tsiutsiura, "Analysis of the integrity and completeness of the higher education institution informational image coverage," 2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2019, pp. 48-50, https://doi.org/10.1109/STC-CSIT.2019.8929759