МРНТИ 20.51.17 DOI 10.48501/3007-6986.2025.15.74.001

Ахметов Б. С. [1], Лахно В. А.[2], Кыдыралина Л. М.[3]
[1]Казахский национальный педагогический университет имени Абая
Казахстан, Алматы
e-mail.ru: bakhytzhan.akhmetov.54@mail.ru
[2]Национальный университет биоресурсов и природопользования
Украина, Киев
[3]НАО" Государственный университет имени Шакарима г. Семей»
Казахстан, Семей

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АДАПТИВНОГО УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА В ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ УНИВЕРСИТЕТА С ИСПОЛЬЗОВАНИЕМ АППАРАТА СЕТЕЙ ПЕТРИ

Аннотация

В связи с переходом большинства учебных заведений, и прежде всего крупных университетов, на информационные платформы обучения и системы электронного документооборота возникает задача усиления киберзащищенности информационно-образовательной среды учебного заведения (ИОСУЗ) от несанкционированного доступа к информационным ресурсам. В докладе рассмотрена модель на основе сети Петри для разграничения полномочий пользователей в сети информационно-образовательной среды университета.

Ключевые слова: кибербезопасность, информационно-образовательная среда университета, моделирование, сети Петри, кибербезопасность, защита информации, электронная информационно-образовательная среда университетов, метод, модель.

Б.С.Ахметов[1], В.А.Лахно[2], Л.М.Кыдыралина[3]
[1] Абай атындағы Қазақ ұлттық педагогикалық университеті
Қазақстан, Алматы
e-mail.ru: bakhytzhan.akhmetov.54@mail.ru
[2] Ұлттық биоресурстар және табиғатты пайдалану университеті
Украина, Киев
[3] ЖОО «Семей қаласының Шәкәрім атындағы мемлекеттік университеті»
Қазақстан, Семей

ПЕТРИ ЖЕЛІСІНІҢ АППАРАТЫН ҚОЛДАНА ОТЫРЫП, ЖОҒАРЫ ОҚУ ОРНЫНЫҢ АҚПАРАТТЫҚ-БІЛІМ БЕРУ ОРТАСЫНДА ҚОЛ ЖЕТКІЗУ ҚҰҚЫҚТАРЫН АДАПТИВТІ БАСҚАРУДЫҢ ТҰЖЫРЫМДАМАЛЫҚ МОДЕЛІ

Аннотация

Көптеген оқу орындарының, ең алдымен ірі университеттердің оқытудың ақпараттық платформаларына және электрондық құжат айналымы жүйелеріне көшуіне байланысты жоғары оқу орнының ақпараттық-білім беру ортасының (ЖООАББО) ақпараттық ресурстарға рұқсатсыз қол жеткізуден киберқауіпсіздігін күшейту міндеті туындайды. Мақалада жоғары оқу орнының ақпараттық-білім беру ортасы желісіндегі пайдаланушылардың өкілеттіктерін ажыратуға арналған Петри желісіне негізделген модель қарастырылған.

Кілт сөздер: киберқауіпсіздік, жоғары оқу орнының ақпараттық-білім беру ортасы, модельдеу, Петри желілері, киберқауіпсіздік, ақпаратты қорғау, университеттердің электрондық ақпараттық-білім беру ортасы, әдісі, моделі.

Akhmetov B. S. [1], Lakhno V. A.[2], Kydyralina L. M.[3]
[1]Kazakh National Pedagogical University named after Abai
Kazakhstan, Almaty
e-mail.ru: bakhytzhan.akhmetov.54@mail.ru

[2]National University of Bioresources and Environmental Management
Ukraine, Kiev
[3]NAO" Shakarim Semey State University"
Kazakhstan, Semey

A CONCEPTUAL MODEL OF ADAPTIVE ACCESS RIGHTS MANAGEMENT IN THE INFORMATION AND EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY USING THE APPARATUS OF PETRI NETS

Abstract

Due to the transition of most educational institutions, and primarily large universities, to information learning platforms and electronic document management systems, the task arises of strengthening the cyber security of the information and educational environment of the educational institution (IOSUZ) from unauthorized access to information resources. The report considers a Petri net-based model for delineating the powers of users in the network of the university's information and educational environment.

Keywords: cybersecurity, information and educational environment of the university, modeling, Petri nets, cybersecurity, information protection, electronic information and educational environment of universities, method, model.

Введение. Современный уровень применения информационных технологий(ИТ) и систем (ИТС) в образовании достиг высочайшего уровня. При этом появился новый термин – информационно-образовательная среда университета (ИОСУ) [1, 2].

Как и любой объект информатизации ИОСУ требует решения задач по защите информации и кибербезопасности (КрБ) [3]. При этом большинство специалистов в области ИТ отмечают необходимость первоочередного приоритета заданиям сохранения целостности, конфиденциальности и доступности информации, вне зависимости от ее функционального назначения [4,5].

Методы исследования .Общей первоначальной задачей при построении эффективных систем защиты и КрБ ИОСУ, остается задача обследования конкретного объекта защиты, формирование моделей потенциального нарушителя (компьютерного злоумышленника – КЗЛ) и киберугроз [1–5]. Реализация вышеуказанных шагов позволит в конечном итоге получить адекватные требования к системам защиты информации (СЗИ) ИОСУ.

В условиях усложнения сценариев кибератак аналитикам служб информационной безопасности (ИБ) необходимо достаточно оперативно реагировать на кибератаки, аномалии угрозы. Это делает актуальной задачу поиска новых способов повышения результативности принятия решений в заданиях реагирования на попытки деструктивного вмешательства со стороны КЗЛ или недобросовестного персонала в работу объектов информатизации, в том числе, ИОСУ.

По мнению большого числа специалистов, достаточно перспективным представляется возможность описания функциональных моделей различных систем защиты ИОСУ в терминах теории сети Петри[4, 5, 7, 8].

Такое представление позволит аналитикам ИБ и ЗИ детализировать киберугрозы в ИОСУ. Кроме того, в последующем, возможно определение состояний, которые потенциально определяют уязвимости ИОСУ перед новыми киберугрозами. Также рассматривается перспективность применения данной модели основе сетей Петри (и Петри–Маркова) и раскрашенных сетей Петри в качестве математической и алгоритмической составляющих, проектируемой интеллектуализированной системы поддержки принятия решений (ИСППР) в процессе анализа кибеугроз для ИОСУ. По нашему мнению, данные суждения делают нашу работу релевантной и повышают результативность в ходе работ по созданию ИСППР в задачах ЗИ и КрБ ИОСУ.

В работах [3–5, 8, 9] были представлены результаты исследований, посвященных применению сетей Петри для описания модели киберугроз. И хотя данные работы внесли несомненный теоретический вклад в данном вопросе, на наш взгляд предлагаемые авторами модели несколько затруднительно реализовать программно, в частности в ИСППР по ЗИ и КрБ ИОСУ.

Основываясь на работах [3], [5] модели угроз возможно построить, используя достаточно наглядную табличную форму отображения угроз при актуализации вопроса оценки защищенности ИОСУ. Но как было указанно ранее, данный подход к составлению моделей угроз трудоемок. А кроме

того, рост количества угроз делает подобный табличный формат представления сложным для восприятия, особенно специалистам с небольшим опытом работы в сфере КрБ.

Сети Петри (и Петри–Маркова) успешно использовались и для описания моделей нарушителя[10, 11]. Однако, авторы не рассматривали возможность корректировки модели нарушителя (КЗЛ) в ИОСУ, в частности путем объединения ее с моделями на основе теории графов, что позволило бы более точно описать переходы состояний в процессе вероятного преодоления КЗЛ периметров (рубежей) киберзащиты ИОСУ.

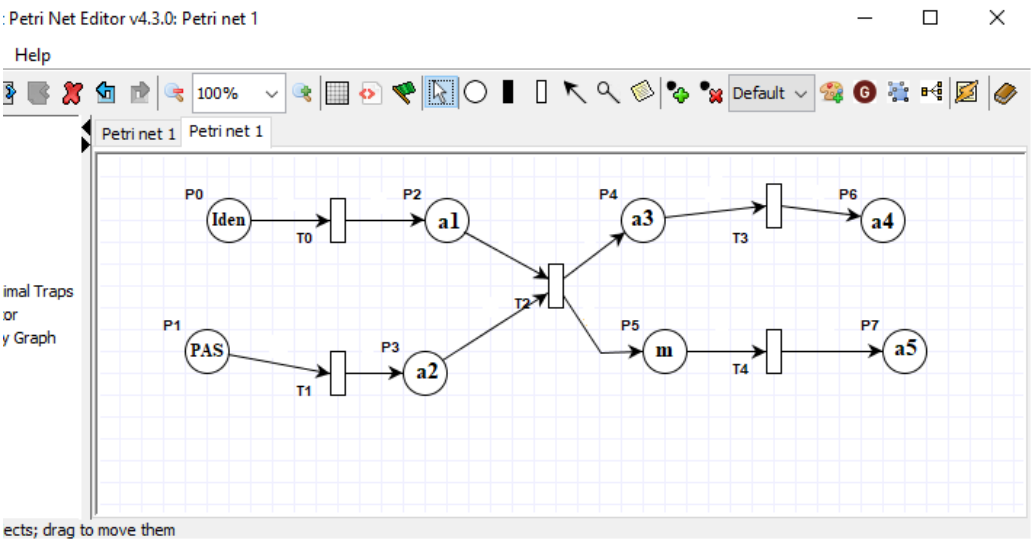
В работах [3, 8, 9] модели СЗИ рассматривались как предварительно выделенные в сети Петри последовательности элементарных операций, из которых возможна кибератака. Модели позволяли просчитывать вероятности реализации разных атак за отведенный промежуток времени. Однако, рассмотренные в [9, 10] модели не позволяли рассчитать временные характеристики в процессе реализации новых киберугроз.

В работах [5, 7], также предлагались модели, основанные на сетях Петри и описывающие процессы реализации угроз в информационных системах (ИС). И ходя данные модели позволяли провести оценку многих параметров защищенности объектов, в частности, вероятности реализации угроз, времени на реализацию угроз, согласованность действий КЗЛ они представляются не до конца завершенными. В частности, в данных работах не изучен вопрос разрешения конфликтных ситуаций, возникающих при изменении состояний ИС в ходе атак, относящихся к разным классам. Это обстоятельство, на наш взгляд ограничивает практическую применимость данных исследований.

Таким образом, синтез новых моделей, а также дополнение существующих моделей и методов адаптивного управления киберзащитойИОСУ с использованием возможностей аппарата сетей Петри и учитывая потенциал визуализации сетей Петри,может стать эффективным инструментарием для прогнозирования состояния защищенности для ИОСУ и других крупных учебных заведений. Это позволит значительно упростить понимание для новых киберугроз и в дальнейшем возможно результативное применениепредлагаемых подходов аналитиками служб ЗИ, ИБ и КрБ различных объектов информатизации.

Результаты исследования. Классический вариант идентификации пользователей при входе в ИОСУ производится по паролю. Пользователи ресурсами ИОСУосуществляют ввод/изменение данных, например, вовремя загрузки ответов на учебные задания или иных случаях.

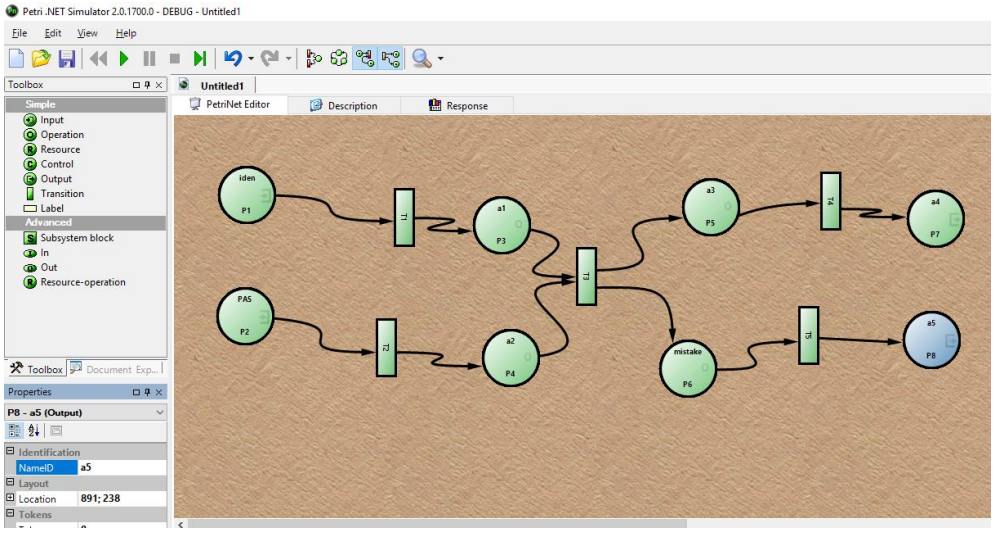
Выполним имитационное моделирование в среде PIPE v4.3.0 для классической схемы идентификации (аутентификации). На рис. 1 представлена блок-схема алгоритма и сеть Петри входа пользователя в ИОСУ для классической схемы.Аналогичная модель для среды Petri.NetSimulator. 2.017. показана на рис. 2.



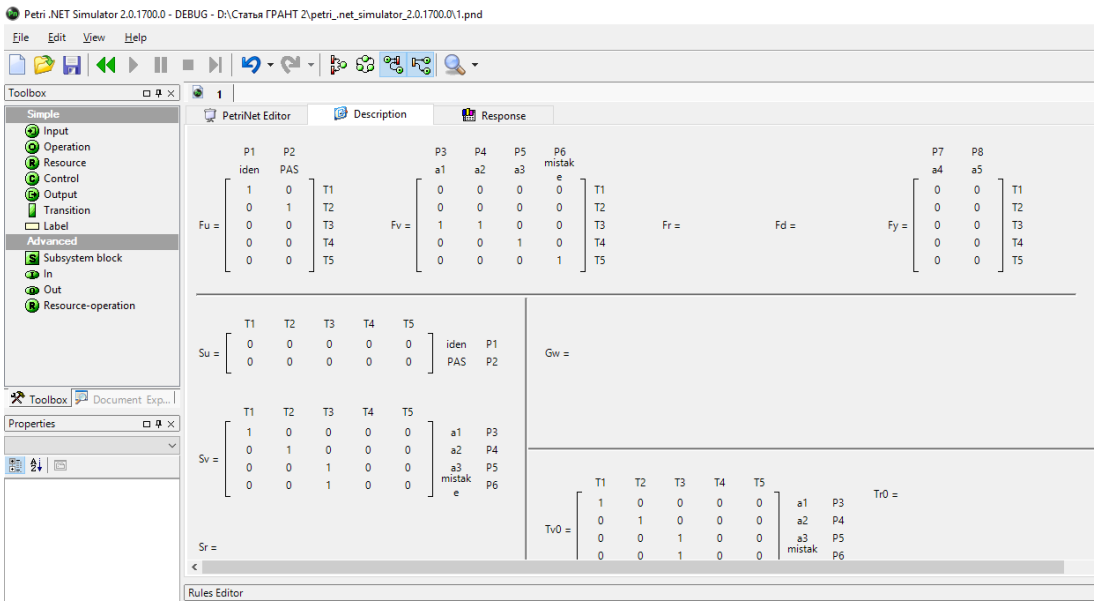
Принятые обозначения: $P0(PAS)$ – пароль, вводимый абонентом в сети ИОСУ для аутентификации (1 –пароль, соответствующий требованиям; фишки другого типа – неправильные и

(или) некорректные пароли); $P1(Iden)$ – идентификатор, используемый пользователем для идентификации вИОСУ; $a1$ – ввод пароля при запросе ИОСУ; $a2$ – идентификатор введённыйабонентом (пользователем); $a3$ – идентификатор прошел проверку паролем, и аутентификация успешно завершена; $a4$ – санкционированный вход пользователя ИОСУ; $a5$ – право доступа пользователя ИОСУ не предоставлено; $T0 - T4$ – отображают совокупность условий перехода.

Рисунок 1- Сеть Петри входа пользователя в ИОСУ для классической схемыидентификации (аутентификации)PIPE v4.3.0



а)

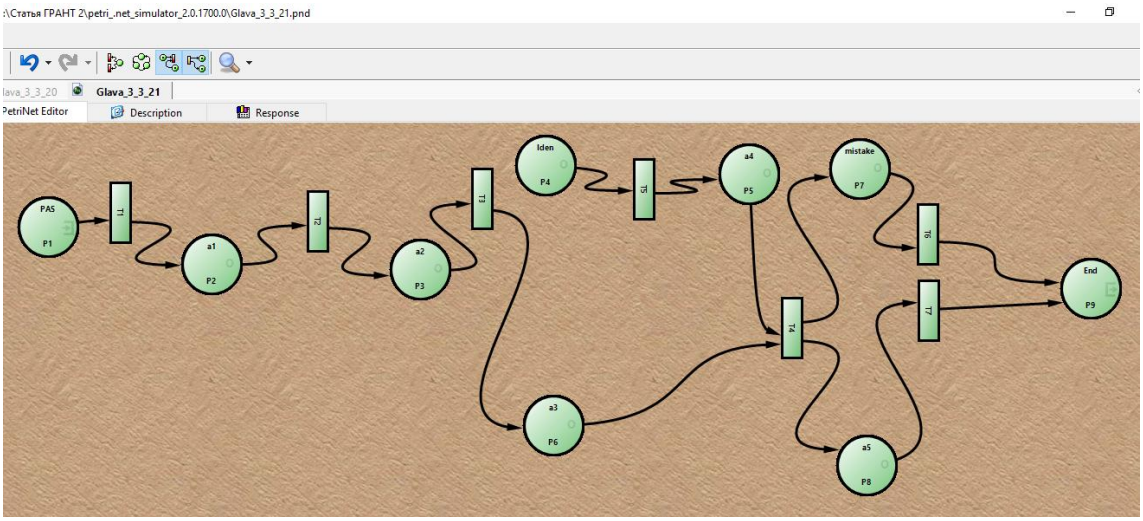


б)

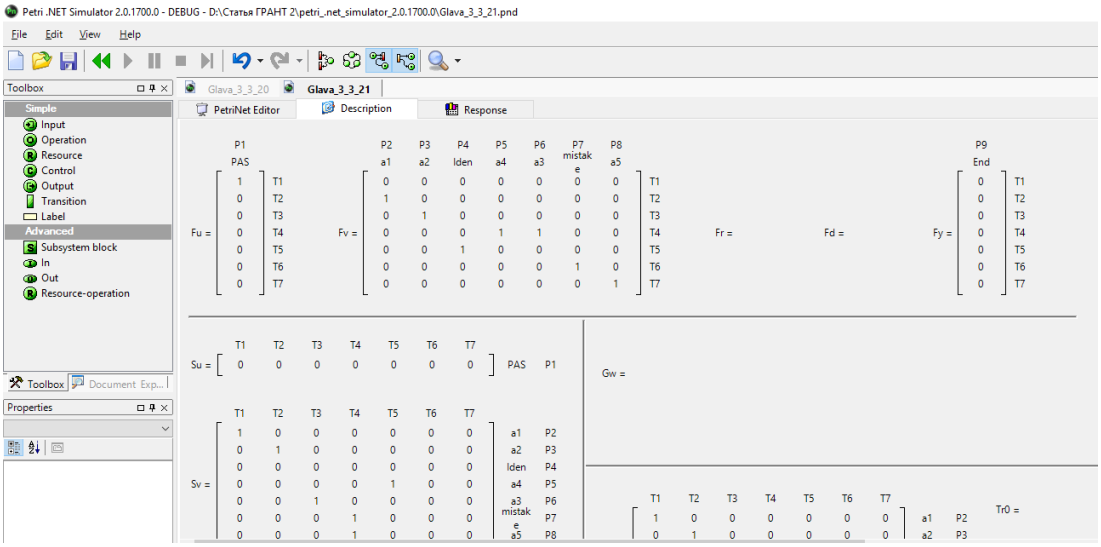
а) модель сети; б) фрагмент результатов моделирования

Рисунок 2- Сеть Петри входа пользователя в ИОСУ для классической схемыидентификации (аутентификации)Petri.NetSimulator. 2.017.

Руководствуясь ранее разработанной схемой (см. рис. 3.16–3.17), выполним имитационное моделирование для схемы аутентификации субъекта в ИОСУ на основе обновляемыхНДУ, см. рис. 3.



а)



а) модель сети; б) фрагмент результатов моделирования

Рисунок 3- Имитационное моделирование для схемы аутентификации субъекта в ИОСУ на основе обновляемыхНДУ с использованием нотации сетей Петри (Petri.NetSimulator. 2.017.)

В таблице 1 показаны обозначения, принятые в имитационной модели для схемы аутентификации субъекта в ИОСУ на основе обновляемыхНДУ, представленной на рис. 3. (в базисе сетей Петри).

Таблица 1

Обозначения, принятые в имитационной модели для схемы аутентификации субъекта в ИОСУ на основе обновляемыхНДУ, представленной на рис. 3.20 (в базисе сетей Петри)

Позиции	
Обозначение принятые на схеме см. рис. 3.20	Описаниепозиции для пользователя

PAS	пароль, введенный абонентом ИОСУ для аутентификации
Iden	проверка представительского набора
*a*1	ввод пароля при запросе ИОСУ
*a*2	идентификатор введённый абонентом (пользователем) совпал с «эталоном» детектирующего набора (ДеН)
*a*3	НДУ определил, что идентификатор введённый абонентом совпал с «эталоном» ДеН
*a*4	НДУ определил, что пароль введённый абонентом совпал с «эталоном» ДеН
*a*5	проверка абонента ИОСУ пройдена
mistake	проверка непройдена, формирование результирующих данных и корректирование НДУ в ИОСУ
Переходы	
$T1..T7$	Отображают совокупность условий перехода (и модификации) маркеров из одной позиции сети в другие. Условия определены набором априорных данных.

В таблице 2 показан фрагмент для набора выходных данных, которые были получены в ходе сравнения вычислительных экспериментов и опытной проверки, предложенной схемы аутентификации для случая задачи анализа поведения субъекта в ИОСУ.

Таблица 2

Фрагмент для набора выходных данных в ходе экспериментов

$rev \cdot$ $\cdot \zeta \cdot$ $\cdot \lvert Tr \rvert$	t, s	Вероятность обнаружения потенциально опасных субъектов ИОСУ							
		Стандартная аутентификация субъекта в ИОСУ, ·100%		Аутентификации субъекта в ИОСУ на основе ОНДУ, ·100%					
		$\alpha = 0{,}1$	$\alpha = 0{,}9$	$\alpha = 0{,}1$				$\alpha = 0{,}9$	
				$P_m = 0{,}7$		$P_m = 0{,}98$		$P_m = 0{,}7$	
				ξ					
				0,1	0,3	0,1	0,3	0,1	0,3
1	50	59,2	0,2	100	99,9	99,3	99,2	77,2	71
	160	59,2	0,1	60,1	59,9	59,1	59,1	0,8	0,4
10	50	61,3	0,4	99,9	98,1	98,4	96	77,3	70,9
	160	60,1	0,4	60, 2	59,1	60,2	59,7	0,6	0,3

Примечания: P_m – вероятность того, что ошибочно будут отождествляться данные НДУ и данные, которые представлены субъектом. (пороговый предел схожести наборов определен заранее); ξ – коэффициент, характеризующий возможность применять результаты проверки на основе конкретного НДУ к нескольким подвидам угроз.

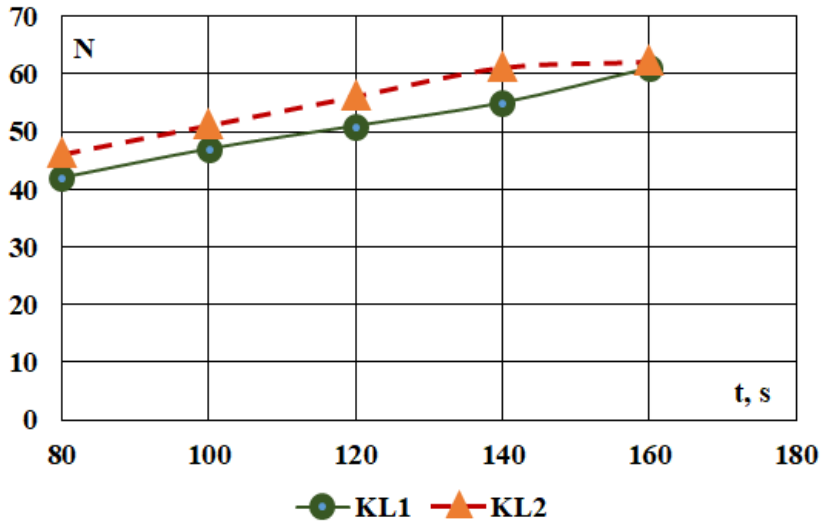
На рис. 3.20б) показаны результаты тестирования, предложенной схемы аутентификации для случая задачи анализа поведения субъекта в ИОСУ.

На графиках рис. 4 показаны зависимости для модуля системы парольной защиты ИОСУ. При этом анализируется скорость распознавания субъекта в ИОСУ от количества введенных субъектом символов.

В экспериментах было принято, что длина пароля равна 8 символам, а количество возможных попыток ввода пароля 3. Количество наборов, задействованных в детектировании составляло 250.

Таким образом, было показано, что даже если злоумышленник узнал пароль, ему сложно подделать машинную манеру авторизованного абонента, обязательно вести за ним долгое время наблюдение и затем тренироваться ИОСУ. Следовательно, предложенная схема аутентификации субъекта в ИОСУ на основе ОНДУ, достаточно эффективна для задач идентификации абонента в системе.

Основные положення. К достоинствам исследования можно отнести тот факт, что предложенные решения, в частности, разработанные программные модули для аутентификации по сравнению с результатами исследований, представленных в работах [7–9, 15], показали большую вероятность обнаружения потенциально опасных субъектов в информационных системах и сетях предприятий, и меньшую вероятность того, что НДУ ошибочно будут отождествляться с данными предоставленными абонентом сети.



*KL*1 – аутентификация субъекта в процессе клавиатурного распознавания в ИОСУ на основе применения ОНДУ; *KL*2 – защита с помощью обычных паролей для субъекта;N – количество переходов при работе субъекта в ИОСУ с клавиатуры.

Рисунок 4- Результаты тестирования, предложенной схемы аутентификации для случая задачи анализа поведения субъекта в ИОСУ (на примере системы дистанционного обучения)

Заключение. Созданные на основе предложенных решений программные продукты, позволили автоматизировать контроль, сопровождение и изменение учётных записей абонентов сетей двух крупных университетов в Украине. При этом в программном продукте «Анализатор угроз» [14,15] была заложена возможность корректировать уровни доступа абонентов к информационным ресурсам и автоматизирована аутентификация пользователей в ИОСУ.

На нынешнем этапе исследований, определенным недостатком работы, является не большая степень апробации, предложенных решений. Эксперименты пока проведены только на платформах двух университетов: Национальный университет Биоресурсов и природопользования Украины и Европейский университет.

Перспектива дальнейших исследований определяется возможностями применения полученных результатов для последующей алгоритмизации процессов, связанных с анализом защищённости ИОСУ. Также возможна программная автоматизация обработки данных о возможных киберугрозах в процессе применения селективного алгоритма обработки обновляемых наборов данных с программно-аппаратных средств детектирования СЗИ и КрБ образовательного учреждения.

Список литературы

1. Liu, C. W., Huang, P., & Lucas, H. (2017). IT Centralization, Security Outsourcing, and Cybersecurity Breaches: Evidence from the US Higher Education.

2. Demers, G., Harrington, S., Cianci, M., & Green, N. (2017). Protecting Colleges & Universities Against Real Losses in a Virtual World, 33 J. Marshall J. Info. Tech. & Privacy L. 101 (2017). The John Marshall Journal of Information Technology & Privacy Law, 33(2), 3.

3. Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. JournalofEducationandLearning, 12(1), 150–158.

4. Diaz, L. J., Anderson, M. C., Wolak, J. T., &Opderbeck, D. (2017). The Risks and Liability of Governing Board Members to Address Cyber Security Risks in Higher Education. JC & UL, 43, p. 49.

5. Ghernaouti, S., &Wanner, B. (2018). Research and Education as Key Success Factors for Developing a Cybersecurity Culture. In Cybersecurity Best Practices (pp. 539-552). Springer Vieweg, Wiesbaden. DOI.org/10.1007/978-3-658-21655-9_38

6. Caelli, W. J., & Liu, V. (2018). Cybersecurity education at formal university level: An Australian perspective. In Journal for the Colloquium for Information Systems Security Education (Vol. 5, No. 2, pp. 26–44). CISSE.

7. Krishnamoorthy, S., Rueda, L., Saad, S., &Elmiligi, H. (2018, May). Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning. In Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications (pp. 50–57). ACM. doi:10.1145/3230820.3230829

8. Turkanović, M., Brumen, B., &Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. AdHocNetworks, 20, pp. 96–112. doi.org/10.1016/j.adhoc.2014.03.009

9. Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. AdHocNetworks, 36, pp. 58-80. doi.org/10.1016/j.adhoc.2015.05.020

10. Appel, M., Konigorski, U., & Walther, M. (2018). A Graph Metric for Model Predictive Control of Petri Nets. IFAC-PapersOnLine, 51(2), pp.254–259.

11. Gao, Z., Zhao, C., Shang, C., & Tan, C. (2017, October). The optimal control of mine drainage systems based on hybrid Petri nets. In Chinese Automation Congress (CAC), 2017 (pp. 78–83). IEEE.

12. Narayanan, M., &Cherukuri, A. K. (2018). Verification of Cloud Based Information Integration Architecture using Colored Petri Nets. International Journal of Computer Network and Information Security, 10(2), 1.

13. V. A. Lakhno, Y. N. Tkach, T.A. Petrenko, S.V. Zaitsev, V. M. Bazylevych. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks, Eastern-European Journal of Enterprise Technologies, No 6/9 (84), 2016, pp. 32–44.

14. G. Beketova, B. Akhmetov, A. Korchenko, V, Lakhno, A. Tereshuk. Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition. Computer modelling and new technologies, Vol. 21, No. 2, 2017, pp. 7–16.

15. Lakhno V., Petrov Al., Petrov Ant. Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport, Information Systems Architecture and Technology : 38th International Conference on Information Systems Architecture and Technology (ISAT 2017), Wroclaw, 17–19 September 2017 : proceedings, Wroclaw : Springer, 2017, pp. 113–127.

Сведения об авторе

Ахметов Бахытжан Сражатдинович
Должность: доктор технических наук, профессор, Казахский национальный педагогический университет имени Абая
Почтовый индекс: Алматы, Казахстан
Сот.тел: 87775528911
E-mail: bakhytzhan.akhmetov.54@mail.ru
Лахно Валерий Анатольевич
Должность: Национальный университет биоресурсов и природопользования Украины

Почтовый индекс: Киев, Украина.
Сот.тел: 480506029690
E-mail: va964@nubip.edu.ua
Кыдыралина Лазат Муктаровна
Должность: PhD
Почтовый индекс: 071412, Республика Казахстана, г. Семей
Сот.тел: 87756238166
E-mail: lazat_75@mail.ru

Автор туралы мәлімет
Ахметов Бахытжан Сражатдинович
Лауазымы: Абай атындағы Қазақ ұлттық педагогикалық университеті, техника ғылымдарының докторы, профессор
Пошталық мекен-жайы: Алматы қ., Казақстан
Ұялы тел: 87775528911
E-mail: bakhytzhan.akhmetov.54@mail.ru
Лахно Валерий Анатольевич
Лауазымы: профессор,Украинаның биоресурстар және табиғатты пайдалану ұлттық университеті
Пошталық мекен-жайы: Киев, Украина.
Ұялы тел: 480506029690
E-mail: va964@nubip.edu.ua
Кыдыралина Лазат Муктаровна
Лауазымы: PhD
Пошталық мекен-жайы: 071412, Қазақстан Республикасы, Семей қ.
Ұялы тел: 87756238166
E-mail: lazat_75@mail.ru

Information about the author
Akhmetov Bakhytzhan Srazhatdinovich
Position: Doctor of Technical Sciences, professor, Abai Kazakh National Pedagogical University
Postal address: Republic of Kazakhstan, Almaty
Cell phone: 87775528911
E-mail: bakhytzhan.akhmetov.54@mail.ru
Lakhno Valery Anatolyevich
Position: Department of Computer systems, networks and Cybersecurity,
National University of Life and Environmental Sciences of Ukraine
Postal address: Kyiv, Ukraine.
Cell phone: 480506029690
E-mail: va964@nubip.edu.ua
Kydyralina Lazat Muktarovna
Position: PhD
Postal address: 071412, Republic of Kazakhstan, Semey
Cell phone: 87756238166
E-mail: lazat_75@mail.ru