УДК 004.056.5

Л.С. ФОНАР, О.С. КОНОВАЛОВ, Є.Г. ФІЛІППОВ
Національний університет Одеська політехніка

# ДОСЛІДЖЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ВЕБ-ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО НАВЧАННЯ

*Метою проведеного дослідження є аналіз стану безпеки використання Google Classroom в університеті «Одеська політехніка» та змін у адмініструванні навчальної платформи за 2020-2022 роки в умовах вимушеного карантину, воєнного стану та дистанційного навчання. Активне впровадження дистанційного навчання вимагає дослідження захисту інформації при обміні та зберіганні даних. Однією з систем дистанційного навчання університету «Одеська політехніка» є Google Classroom. Основна перевага – безкоштовність сервісів, адміністрування закладом, вхід за допомогою звичайного аккаунту Gmail. Ретельно продумана структура адміністрування та організації роботи сервісу є вирішальною для ефективного управління обліковим записом G Suite for Education. Актуальною проблемою є створення освітнього простору за допомогою веб-технологій та організація безпечного доступу користувачів до ресурсів. Важливим аспектом також є психологічний та педагогічний аспект використання дистанційного навчання, яке може проводитись в синхронному, або асинхронному виді. У роботі проведено дослідження загроз інформаційної безпеки веб-технологій дистанційного навчання Google Classroom для користувачів та порівняння заходів адміністрування у 2020-2022 роках. Для протидії актуальним загрозам для систем дистанційного навчання університету і зменшення ризиків в межах допустимого, використовуються різні механізми і засоби захисту інформації, організаційно-правового, технічного та програмного характеру, які повинні враховувати ряд особливостей, пов'язаних з процесом їх функціонування. Система дистанційної освіти університету повинна бути доступна для здобувачів, викладачів та адміністраторів цілодобово. Забезпечення захисту від загроз повинно здійснюватися як на етапі проектування і розробки самої системи дистанційної освіти, так і в процесі його експлуатації, та внесенням, у разі необхідності, своєчасних корегувань. Проаналізовано адміністрування системи дистанційної освіти університету «Одеська політехніка» та зроблені такі висновки та рекомендації для покращення інформаційної безпеки.*

*Ключові слова: система дистанційного навчання, заклад вищої освіти, захист інформації, Google Classroom, веб-технології, адміністрування.*

L.S. FONAR, O.S. KONOVALOV, E.G. FILIPPOV
Odesa Polytechnic National University

# STUDY OF INFORMATION SECURITY THREATS AT USED WEB TECHNOLOGIES OF DISTANCE EDUCATION

*The purpose of the research is to analyze the state of security of using Google Classroom at the Odesa Polytechnic University and changes in the administration of the educational platform for 2020-2022 in the conditions of forced quarantine, martial law and distance learning. The active implementation of distance learning requires research on information protection during data exchange and storage. One of the distance learning systems of Odesa Polytechnic National University is Google Classroom. The main advantage is free services, institution administration, login using a regular Gmail account. A carefully thought-out structure of administration and organization of the service is crucial to the effective management of the G Suite for Education account. An urgent problem is the creation of an educational space using web technologies and the organization of secure user access to resources. An important aspect is also the psychological and pedagogical aspect of the use of distance learning, which can be conducted in a synchronous or asynchronous form. In the work, a study of threats to the information security of Google Classroom distance learning web technologies for users and a comparison of administration measures in 2020-2022 was carried out. Various mechanisms and means of information protection, of an organizational, legal, technical and programmatic nature, are used to counter actual threats to the university's distance learning systems and to reduce risks within the permissible limits, which must take into account a number of features related to the process of their functioning. The distance education system of the university should be available to students, teachers and administrators around the clock. Ensuring protection against threats should be carried out both at the stage of designing and developing the distance education system itself, as well as during its operation and making, if necessary, timely adjustments. The administration of the distance education system of the Odesa Polytechnic National University was analyzed and the following conclusions and recommendations were made for improving information security.*

*Keywords: distance learning system, higher education institution, information protection, Google Classroom, web technologies, administration.*

https://doi.org/10.32782/mathematical-modelling/2022-5-1-13

## Постановка проблеми

Актуальною проблемою системи вищої освіти в Україні за останні роки є аналіз використання веб-технологій для дистанційного навчання в умовах пандемії та воєнного стану. Вимушений перехід багатьох закладів освіти у веб-простір вимагає аналізу безпеки користування різноманітними сервісами. Важливим є дослідження загроз інформаційної безпеки для персональних даних студентів та викладачів, систем оцінювання, збору та зберігання даних. Також використання он-лайн сервісів у освіті підвищує вимоги до автентифікації користувачів, бо дистанційне навчання у багатьох випадках ускладнює об'єктивність оцінювання знань. Разом з тим, використання веб-технологій може полегшити збір даних, зменшити паперовий документообіг між викладачем та здобувачами, спростити доступ до матеріалів, лекцій, методичних вказівок та іноді навіть покращити комунікацію між учасниками навчального процесу. Метою проведеного дослідження є аналіз стану безпеки використання Google Classroom в університеті «Одеська політехніка» та змін у адмініструванні навчальної платформи за 2020-2022 роки в умовах вимушеного карантину, воєнного стану та дистанційного навчання.

## Аналіз останніх досліджень і публікацій

Використання веб-технологій дистанційного навчання (ВТДН) надає можливість здобувачам отримувати необхідні знання віддалено від навчального закладу в будь-який зручний час. Права та обов'язки учасників навчального процесу при ВТДН регулюються «Положенням про дистанційне навчання» [1] та Законом України про вищу освіту [2].

При впровадженні систем дистанційного навчання перед закладом та здобувачами освіти постають проблеми добору програмних засобів та раціонального використання освітніх інформаційних ресурсів, створених на їх основі [3, 4]. Тому актуальною проблемою є створення освітнього простору за допомогою веб-технологій та організація безпечного доступу користувачів до ресурсів. Важливим аспектом також є психологічний та педагогічний аспект використання дистанційного навчання, яке може проводитись в синхронному або асинхронному виді.

Організаційна підтримка здобувачів з боку викладача під час дистанційного викладання курсів дисциплін в переважній більшості формує позитивну та дружнє середовище навчання. Необхідно забезпечувати наявність засобів оперативної електронної комунікації учасників навчального процесу з адміністрацію навчального закладу, викладачем, між собою. Найчастіше це можливо організувати за допомогою форуму, чату, електронної пошти, сторінок в соціальних мережах, мессенджерів тощо [5, 6].

Разом з тим, використання веб-технологій у дистанційному освітньому середовищі має свої переваги [7 - 12]: можливість зберігати великі масиви даних, спрощення публікації, розміщення навчальних матеріалів, безперервність освітнього процесу, групова спрямованість (корпоративність), спільна робота викладачів і студентів, активація самостійної діяльності, можливість інтеграції навчальних дисциплін тощо.

## Мета дослідження

Метою проведеного дослідження є аналіз стану безпеки використання Google Classroom в Національному університеті «Одеська політехніка» та змін у адмініструванні навчальної платформи за 2020-2022 роки в умовах вимушеного карантину, воєнного стану та дистанційного навчання та надання рекомендацій для підвищення інформаційної безпеки користувачів ресурсу.

## Викладення основного матеріалу дослідження

Використання Google Classroom [13, 14] у освітньому процесі відповідає [1]: це інформаційно-комунікаційні технології дистанційного навчання – технології створення, накопичення, зберігання та доступу до веб-ресурсів (електронних ресурсів) навчальних дисциплін (програм),

https://doi.org/10.32782/mathematical-modelling/2022-5-1-13

а також забезпечення організації і супроводу навчального процесу за допомогою спеціалізованого програмного забезпечення та засобів інформаційно-комунікаційного зв'язку, у тому числі Інтернету. Google Classroom дозволяють працювати зі добувачами як в асинхронному режимі, так і в синхронному – за допомогою сервісу Google Workspace for Education Fundamentals, це набір безкоштовних інструментів і сервісів Google, розроблених спеціально для навчальних закладів і організацій, що займаються домашнім навчанням. Конфіденційність персональних даних користувачів забезпечується сервісами компанії Google та адміністрацією.

Дані користувачів, які створюються в сервісах Google Classroom, або завантажені туди, шифруються при зберіганні. Крім того, всі сервіси G Suite працюють через протокол HTTPS, тому дані також захищені при передачі між центрами обробки даних та при доступі з окремого пристрою.

Організаційні блоки дозволяють розподіляти на сегменти користувачів та надавати різноманітні послуги, налаштування та дозволи різним користувачам. Ретельно продумана структура адміністрування та організації роботи сервісу є вирішальною для ефективного управління обліковим записом G Suite for Education. На початку впровадження сервісу в начальному закладі в консолі адміністратора Google всі користувачі і пристрої об'єднані лише в один організаційний підрозділ, цей підрозділ називають організаційним підрозділом верхнього рівня. Тому на початковому етапі всі налаштування адміністратора застосовуються до всіх користувачів та пристроїв у обліковому записі.

Щоб створити різні налаштування для різних груп користувачів або пристроїв, необхідно додати підрозділ нижчого рівня, для цього використовують групи. Організаційні блоки першого рівня організовані за ролями «студенти» та «викладачі».

Для кожного користувача (студента та викладача університету), якому необхідно створити окремий акаунт, потрібно додати до таблиці наступну інформацію в стовпці: ім'я, прізвище, адреса електронної пошти, шлях до організаційного підрозділу. Заповнивши таблицю, її зберігають як файл CSV (.csv) в кодуванні UTF-8.

Потенційні загрози інформації системи відділу технологій дистанційного навчання (ВТДН) викладено у табл.1.

Коли адміністратор перевіряєте викладачів, він забороняє «не викладачу» створювати Класи. Якщо викладач помилково ідентифікував себе як «студент», адміністратор повинен власноруч додати викладача в групу «Викладачі», щоб надати можливість створювати класи. У загальному випадку Адміністратор може вказати, хто має право в університеті створювати Класи. Можливі такі варіанти налаштувань:

1. Item 1
2. Item 2
3. Item 3

або:

– всі в цьому домені (викладачі та студенти);
– викладачі, які очікують підтвердження і перевірені викладачі;
– тільки перевірені викладачі.

В університеті «Одеська політехніка» створювати Класи можуть тільки перевірені викладачі.

Зловмисник, як зовнішній так і внутрішній, при реалізації атаки може переслідувати такі цілі:

– перевищення привілеїв;
– отримання несанкціонованого доступу до ресурсів;
– отримання контролю над курсом;
– отримання доступу до внутрішньої системи університету;
– крадіжка інтелектуальної власності;
– крадіжка оціночних матеріалів;
– отримання доступу до персональних даних;
– розголошення персональних даних;

https://doi.org/10.32782/mathematical-modelling/2022-5-1-13

– внесення змін до бази даних навчальних відомостей з оцінками та модулями;
– отримання несанкціонованого доступу до службової інформації навчального закладу;
– порушення цілісності або знищення навчальних матеріалів;
– порушення цілісності або знищення даних про навчальний процес;
– порушення доступності до матеріалів навчальних курсів для користувачів.

При реалізації атак зловмисник може використати:
– уразливості в веб-додатках
– уразливості в сервісах;
– слабкі паролі;
– недоліки процесу аутентифікації;
– помилки в конфігурації і адмініструванні;
– шкідливе програмне забезпечення;
– слабкості системи захисту інформації;
– спам, фішінг.

Таблиця 1

Потенційні загрози веб-технологій дистанційного навчання

| Елемент ВТДН | Загрози | Наслідки |
|---|---|---|
| Веб-інтерфейс (обмін інформацією, доступ до курсів і матеріалів) | Підробка міжсайтових запитів – CSRF, атаки на браузер клієнта, віддалене виконання коду і відмова в обслуговуванні сервісів web-додатків, спам, фішинг. | Порушення конфіденційності, цілісності і доступності інформації і сервісів веб-додатків. |
| Сервер ВТДН (підсистеми: управління навчальними курсами; тестування, календар, адміністрування) | Перебір паролів, підвищення привілеїв користувачів, помилки адміністрування, сканування портів. | Порушення конфіденційності, цілісності і доступності інформації, проникнення в ІС. |
| База даних (навчальні курси, списки академічних груп, персональні дані, бібліотеки, відомості) | випадкове або навмисне видалення / модифікація даних в БД і журналах транзакцій, крадіжка персональних даних, несанкціонований доступу до бази даних і журналів. | Відмова від зобов'язань і скоєних дій, порушення авторського права, порушення цілісності і конфіденційності. |

Для протидії актуальним загрозам для систем дистанційного навчання університету і зменшення ризиків в межах допустимого, використовуються різні механізми і засоби захисту інформації, організаційно-правового, технічного та програмного характеру, які повинні враховувати ряд особливостей, пов'язаних з процесом їх функціонування:

– система дистанційної освіти університету повинна бути доступна для здобувачі, викладачів та адміністраторів цілодобово;

– міжмережеві екрани і застосування SSL не завжди забезпечують захист від злому системи дистанційної освіти, оскільки доступ до веб-сайту з зовнішніх мереж повинен бути завжди відкритий;

Отже, забезпечення захисту від загроз повинно здійснюватися як на етапі проектування і розробки самої системи дистанційної освіти, так і в процесі його експлуатації та внесенням, у разі необхідності, своєчасних корегувань.

У 2020 році приєднатися до курсу можна було наступними способами [15]: перейти за посиланням, яке відправлено викладачем; вказати код курсу, наданий викладачем; прийняти запрошення, надіслане викладачем на електронну пошту. У 2021 році політика доступу була змінена та зараз приєднатися до Класу можна лише за запрошенням, висланим викладачем на електронну пошту по університетським акаунтам. Цей спосіб захищає дані курсу від доступу сторонніх користувачів. При запрошенні студентів до групи викладача з домену університету,

https://doi.org/10.32782/mathematical-modelling/2022-5-1-13

йому не обов'язково знати або окремо збирати електронні пошти кожного студента, достатньо лише знати прізвище та ім'я – всі акаунти вже внесені адміністратором до системи та викладач може знайти потрібного студента без його пошти.

В університеті «Одеська політехніка» система налаштована так, що викладач сам створює групи та додає до них користувачів, груп може бути декілька. Викладач може додати іншого викладача університету в групу по університетському акаунту, але не може додати викладачів зі сторонніми акаунатами (у 2020 році ця можливість ще зберігалась). Ця заборона також підвищує захист даних та унеможливлює сторонній доступ до конфіденціальної інформації (наприклад особисті дані студентів груп, до яких помилково запросили стороннього викладача).

У 2020 в групах до матеріалів курсу окремо були налаштовані наступні параметри: якщо викладач надав доступ до групи користувачеві з особистим обліковим записом (не з домену університету), то йому буде наданий доступ до перегляду документів групи, але буде діяти заборона на виконання тестів. Це давало можливість налаштувати перегляд файлів для членів групи, незалежно від того, через який акаунт був виконаний вхід, документи для перегляду були доступні у будь-якому випадку, а на проходження тесту налаштований захист, який передбачав, що студент повинен перебувати в групі саме з акаунту університету. Але з 2021 року перегляд тестів також можливий лише з університетських акаунтів, що збільшило захист інформації від стороннього доступу.

## Висновки

Проаналізувавши адміністрування системи дистанційної освіти університету «Одеська політехніка», можна зробити такі висновки та рекомендації:

– налаштування декількох облікових записів адміністраторів та суперадміністраторів може допомогти при втраті або зламу облікового запису суперадміністратора;

– необхідно обов'язково вимагати двоетапну перевірку для облікових записів та використовувати ключі безпеки для двоетапної аутентифікації;

– необхідна заборона користування обліковим записом суперадміністратора для повсякденних дій;

– необхідно налаштувати попередження адміністратора по електронній пошті для відстеження активності потенційних ризиків безпеки, наприклад, підозрілих спробах входу в систему, зламу мобільних пристроїв або змін, внесених іншим адміністратором;

– заборона додавати до груп Google Classroom сторонніх викладачів та студентів посилює заходи безпеки та захист персональних даних користувачів;

– якщо необхідно видалити обліковий запис викладача, то потрібно переконатися, що його Класи з матеріалами та роботами по дисциплінам більше не використовуються студентами або іншими викладачами. Якщо Клас використовується, необхідно передати право володіння іншому викладачеві, щоб не втратити доступ до даних.

## Список використаної літератури

1. Про затвердження Положення про дистанційне навчання https://zakon.rada.gov.ua/laws/show/z0703-13#n18
2. Про вищу освіту: Закон України від 27.10.2022 https://zakon.rada.gov.ua/laws/show/1556-18#Tex
3. Олексюк В. П. Єдина система автентифікації як крок до створення освітнього простору загальноосвітнього навчального закладу. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 2, Комп'ютерно-орієнтовані системи навчання : Збірник наукових праць* / М-во освіти і науки України, Нац. пед. ун-т ім. М.П. Драгоманова. – К. : Вид-во НПУ ім. М.П. Драгоманова, Вип. 13 (20). 2012. С. 188-193.
4. Назар М. М. Компоненти продуктивного дистанційного навчального курсу. *Новітні комп'ютерні технології,* Том 17, 2019. С. 114-128. https://doi.org/10.55056/nocote.v17i0.954

https://doi.org/10.32782/mathematical-modelling/2022-5-1-13

5. Назар М. М. Специфіка психологічного впливу навчання користувачів мережі Інтернет. *Освіта дорослих в Україні : IX Міжнар. наук.-практ. конф*., (Київ, 11–17 вер. 2008 р.) : зб. наук. праць. К. : ЕКМО, 2008. С. 102-104.
6. Дяченко О.Ф. Дидактичні можливості хмарних технологій при вивченні інформатичних дисциплін бакалаврів із системного аналізу. *Новітні комп'ютерні технології*, Том 17, 2019. – С.159-162. https://doi.org/10.55056/nocote.v17i0.959
7. Рашевська Н. В., Семеріков С. О., Словак К. І., Стрюк А. М. Модель комбінованого навчання у вищій школі України : збірник наукових праць. Харків : Міськдрук, 2011. С. 54-59.
8. Khoroshylova I., Baidala V. Role of information and communication technology in education. Сучасні тенденції організаційно-методологічного забезпечення підготовки фахівців: проблеми та шляхи їх вирішення в умовах глобалізації та євроекономічної інтеграції: *Зб. матеріалів Всеукр. наук.-метод. інтернет-конф. з проблем вищої освіти і науки*, Харків, 18 лист. 2019 р. / Харків. нац. автомобільно-дорожній ун-т. Харків : ХНАДУ, 2019. С. 330–333.
9. Мерзликін О. В., Семеріков С. О. Перспективні хмарні технології в освіті. Хмарні технології в сучасному університеті (ХТСУ-2015): *Матеріали доповідей науково-практичного семінару*. Черкаси : ЧДТУ, 2015. С. 31-33.
10. Anna V. Iatsyshyn, Valeriia O. Kovach, Yevhen O. Romanenko, Andrii V. Iatsyshyn Cloud services application ways for preparation of future PhD [Electronic resource]. *Cloud Technologies in Education: Proceedings of the 6th Workshop on Cloud Technologies in Education* (CTE 2018), Kryvyi Rih, Ukraine, December 21, 2018 / Edited by : Arnold E. Kiv, Vladimir N. Soloviev. P. 197-216. (CEUR Workshop Proceedings (CEUR-WS.org), Vol. 2433). Access mode : http://ceur-ws.org/Vol-2433/paper12.pdf
11. Tuncay, E.: Effective use of cloud computing in educational institutions. Procedia. *Social and Behavioral Sciences* 2(2), 2010. P. 938–942. https://doi.org/10.1016/j.sbspro.2010.03.130
12. Вакалюк Т. А. Хмарні технології в освіті : навч.-метод. посіб. для студентів фізико-математичного факультету. Житомир: вид-во ЖДУ, 2016. 72 с.
13. Classroom https://edu.google.com/products/classroom/?modal_active=none
14. Education Fundamentals https://edu.google.com/products/workspace-for-education/education-fundamentals/
15. Дорофєєва І., Фонар Л. Аналіз стану інформаційної безпеки систем дистанційної освіти Moodle та Google Classroom. *Матеріали конференцій Молодіжної наукової ліги*. Вінниця, 2020. С. 27-29. https://doi.org/10.36074/27.11.2020.v2.02

**References**

1. About the approval of the Regulations on distance learning URL: https://zakon.rada.gov.ua/laws/show/z0703-13#n18
2. Law of Ukraine on Higher Education URL: https://zakon.rada.gov.ua/laws/show/1556-18#Tex
3. Oleksyuk, V. (2012). Yedyna systema avtentyfikatsii yak krok do stvorennia osvitnoho prostoru zahalnoosvitnoho navchalnoho zakladu. [Unified authentication as a step towards the creation of the educational space of general educational institutions]. *Scientific journal of NPU named after M. P. Drahomanov. Series 2. Computer-oriented educational systems : collection of scientific* . K. : NPU named after M. P. Drahomanov, **13** (20), 188–193. URL: http://elar.fizmat.tnpu.edu.ua/handle/123456789/87. (in Ukrainian)
4. Nazar, M. M. (2019). Komponenty produktyvnoho dystantsiinoho navchalnoho kursu [Components of efficient distance learning course]. *New Computer Technology*, **17**, 114–128. Retrieved from https://ccjournals.eu/ojs/index.php/nocote/article/view/954
5. Nazar, M. M. (2008). Spetsyfika psykholohichnoho vplyvu navchannia korystuvachiv merezhi Internet [Specificity of psychological influence of training of Internet users]. *Osvita doroslykh*

*v Ukraini : IX Mizhnar. nauk.-prakt. konf.,* (Kyiv, 11–17 ver. 2008 r.) : zb. nauk. prats. – K. : EKMO, 102-104.
6. Djachenko, O. F. (2019). Dydaktychni mozhlyvosti khmarnykh tekhnolohii pry vyvchenni informatychnykh dystsyplin bakalavriv iz systemnoho analizu. [The didactic potential of cloud technologies in the study of computing disciplines by bachelors in system analysis]. *New Computer Technology*, **17**, 159-162. Retrieved from https://ccjournals.eu/ojs/index.php/nocote/article/view/959
7. Rashevska. N. V., Semerikov. S. O., Slovak. K. I., & Striuk, A. M. (2011). Model kombinovanoho navchannia u vyshchii shkoli Ukrainy [The blended learning model in Ukrainian higher education]. Sbornik nauchnykh trudov. Kharkiv : Miskdruk, 54-59. (In Ukrainian)
8. Khoroshylova, I., & Baidala, V. (2019). Role of information and communication technology in education. Suchasni tendentsii orhanizatsiino-metodolohichnoho zabezpechennia pidhotovky fakhivtsiv: problemy ta shliakhy yikh vyrishennia v umovakh hlobalizatsii ta yevroekonomichnoi intehratsii : *zb. materialiv Vseukr. nauk.-metod. internet-konf. z problem vyshchoi osvity i nauky*, Kharkiv, 18 lyst. 2019 r. / Kharkiv. nats. avtomobilno-dorozhnii un-t. Kharkiv : KhNADU, 330–333.
9. Merzlykin, O. V., & Semerikov, S. O. (2015). Perspektyvni khmarni tekhnolohii v osviti [Prospective cloud technologies in education]. In: *Materialy dopovidei naukovo-praktychnoho seminaru "Khmarni tekhnolohii v suchasnomu universyteti"* (KhTSU–2015), ChDTU, Cherkasy, 31–33.
10. Iatsyshyn, A.V., Kovach, V.O., Romanenko, O.Y., & Iatsyshyn, A.V.(2018). Cloud services application ways for preparation of future PhD [Electronic resource]. *Cloud Technologies in Education : Proceedings of the 6th Workshop on Cloud Technologies in Education*, Kryvyi Rih, Ukraine, December 21, Edited by : Arnold E. Kiv, Vladimir N. Soloviev. 197-216. (CEUR Workshop Proceedings (CEUR-WS.org), Vol. 2433). Access mode : http://ceur-ws.org/Vol-2433/paper12.pdf
11. Tuncay, E. (2010). Effective use of cloud computing in educational institutions. Procedia. *Social and Behavioral Sciences*. **2**(2), 938–942. doi:10.1016/j.sbspro.2010.03.130
12. Vakaliuk, T.A. (2016). Khmarni tekhnolohii v osviti [Cloud technology in education]. ZhSU Publishing House, Zhytomyr
13. Classroom https://edu.google.com/products/classroom/?modal_active=none
14. Education Fundamentals https://edu.google.com/products/workspace-for-education/education-fundamentals/
15. Dorofeeva, I., & Fonar, L. (2020). Analiz stanu informatsiinoi bezpeky system dystantsiinoi osvity Moodle ta Google Classroom. [Analysis of the information security state of distance education systems moodle and google classroom]. *Conference Proceedings of the Youth Science League,* 27-29, doi:10.36074/27.11.2020.v2.02.

Фонар Людмила Сергіївна – к.т.н., доцент кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка». Email: fonar_1_s@ukr.net, ORCID: 0000-0002-7478-6742.

Коновалов Олександр Сергійович – аспірант кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка». Email: akonovalov.lux@gmail.com ORCID: 0000-0001-8023-9633.

Філіппов Євген Геннадійович – аспірант кафедри штучного інтелекту та аналізу даних Національного університету «Одеська політехніка». Email: 7161160@gmail.com ORCID: 0000-0002-9034-176X.

https://doi.org/10.32782/mathematical-modelling/2022-5-1-13