УДК 378:356:355:37
DOI https://doi.org/10.32782/2410-2075-2023-16.7

ІНФОРМАЦІЙНА БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ ЯК ЕЛЕМЕНТ БЕЗПЕЧНОГО ОСВІТНЬОГО СЕРЕДОВИЩА

ЦІСАРУК ІРИНА ВАСИЛІВНА
кандидат педагогічних наук,
завідувач кафедри теорії і методики трудового навчання та технологій
Кременецька обласна гуманітарно-педагогічна академія імені Тараса Шевченка
tsisarukiryna@gmail.com
orcid.org/0000-0002-7285-9055

ЦІСАРУК ВІТАЛІЙ ЮРІЙОВИЧ
кандидат педагогічних наук, доцент,
доцент кафедри теорії і методики трудового навчання та технологій
Кременецька обласна гуманітарно-педагогічна академія імені Тараса Шевченка
vitaliytsisaruk87@gmail.com
orcid.org/0000-0001-7376-6523

ОМЕЛЬЧУК ОЛЕКСАНДР ВАСИЛЬОВИЧ
кандидат педагогічних наук, доцент,
доцент кафедри теорії і методики трудового навчання та технологій
Кременецька обласна гуманітарно-педагогічна академія імені Тараса Шевченка
omelchykov@meta.ua
orcid.org/0000-0001-9330-5708

У статті висвітлюється проблематика досягнення інформаційної безпеки учасників освітнього процесу з метою організації безпечного освітнього середовища. Розкрито чотири загальні категорії ризику (ризик, пов'язаний із вмістом матеріалів, які представлені в інтернеті; ризик, пов'язаний із небажаними контактами; комерційний ризик; ризик, пов'язаний із використанням персональних даних), якому піддаються здобувачі освіти під час використання мережі «Інтернет».

У роботі досліджено пріоритетні напрями розвитку інформаційної безпеки студентської молоді в закладах освіти, а також охарактеризовано детальну інформацію (персональні дані здобувачів освіти, викладачів та інших категорій працівників; структурована навчальна інформація, яка забезпечує освітній процес; наукові напрацювання, які наділено ознаками інтелектуальної власності та захищено законодавством), що перебуває в розпорядженні закладів освіти в Україні.

Установлено, що в межах розроблення ефективної стратегії інформаційної безпеки закладів освіти виділяють такі основні напрями, як: нормативно-правове забезпечення, в організаційному плані, профілактична робота, адміністративно-організаційний, фізичний і технічний.

Визначено, що безпека здобувачів освіти є одним із головних завдань цивілізованого суспільства, тому гарантувати їхню безпеку в інтернеті повинні всі, хто причетний до цього суспільства. Одним з основних завдань організації безпечного освітнього середовища є формування різнобічної інтелектуальної особистості, високий моральний рівень якої буде запорукою її інформаційної безпеки, а для цього необхідно підвищувати кваліфікацію педагогів із питань інформаційної безпеки, щоб уміти орієнтувати здобувачів освіти з безпечної поведінки в мережі «Інтернет» і регулярно проводити консультування з питань кібербезпеки, працювати не навздогін, а на випередження.

Ключові слова: *інформаційна безпека, мережа «Інтернет», здобувачі освіти, заклад освіти, ризик.*

Постановка проблеми. Натепер інтернет став невід'ємною частиною нашого повсякденного життя. Використання Мережі в закладах освіти та вдома розширює інформаційний освітній простір і дозволяє підвищити ефективність навчання. Доступ учнів і студентів до інформаційних ресурсів в інтернеті дає можливість користуватися додатковими джерелами для навчання, виконувати завдання для самостійного опрацювання. Завдяки відповідним

сервісам у здобувачів освіти з'являється можливість відвідувати заняття дистанційно та продовжувати освітній процес.

Однак використання інтернету в освітній діяльності приховує багато небезпек. Дуже важливо, щоб у всіх закладах освіти була безпечна мережа «Інтернет». За даними досліджень українських учених, натепер в Україні дві третини неповнолітніх виходять у глобальну мережу самостійно, без нагляду батьків і педагогів. Приблизно 40 % здобувачів освіти відвідують вебсторінки небажаного та забороненого змісту. У багатьох розвиваються інтернет-залежність та ігроманія.

Для закладів вищої освіти однією із проблем організації інформаційної безпеки освітнього середовища є той факт, що значна частина студентів на досить високому рівні володіють технічними пристроями, але не зовсім добре дотримуються правил інформаційної безпеки.

Інспектувати, який саме контент переглядають або завантажують студенти, майже неможливо, оскільки мобільні телефони та ґаджети є їхніми особистими речами. Водночас контроль на рівні батьків досить низький, оскільки велика частина студентів проживають у гуртожитках і приїжджають додому лише на вихідні.

Аналіз останніх досліджень та публікацій. Останніми роками проблемі організації безпечного освітнього середовища присвячується значна кількість наукових праць таких дослідників, як К. Варивода, Г. Васянович, В. Іорданова, В. Ковальчук, Г. Костецька, В. Куницький, Я. Малик, Н. Москвіна, О. Обозова, О. Спірін та інші. Проте науковці звертають значну увагу на педагогічні та психологічні аспекти створення умов безпечного освітнього середовища, а інформаційна безпека учасників освітнього процесу залишається малодослідженою.

Метою статті є висвітлення проблематики інформаційної безпеки здобувачів освіти як елемента безпечного освітнього середовища.

Виклад основного матеріалу. Із входженням України в європейський освітній простір законодавство у сфері інформаційної безпеки та контроль за його дотриманням перейшли на вищий рівень. Водночас проблемність ситуації полягає у відсутності єдиної науково розробленої теорії інформаційної безпеки, невідповідності потенційних можливостей інформатизації освіти одержуваним нині результатам. Відсутність законодавчих і нормативно-правових документів, що визначають рівень моральності даних, що циркулюють в інформаційних електронних мережах, загострює проблему виховання молоді, яка безконтрольно використовує ресурси глобальної мережі.

Ми добре розуміємо, що на даному етапі розвитку суспільства відмовлятися від інформаційних технологій неможливо, але безконтрольний доступ до мережі «Інтернет» може призвести до таких негативних наслідків: кіберзалежності; зараження шкідливими програмами під час завантаження файлів; порушення нормального розвитку особистості; неправильного формування моральних цінностей; знайомства з людиною з недобрими намірами [2].

На основі досліджень, спрямованих на аналіз ризику, якому піддаються діти та підлітки під час використання інтернету, можна говорити про чотири загальні категорії ризику [5]:

1) ризик, пов'язаний із вмістом матеріалів, які представлені в інтернеті. Ідеться про ті ситуації, у яких дитина отримує доступ до нелегальної інформації, яка завдає шкоди її здоров'ю та розвитку;

2) ризик, пов'язаний із небажаними контактами. За допомогою соціальних мереж, а також беручи участь у дискусіях (чати, форуми тощо) діти та підлітки можуть завести небажане знайомство. Підлітки в соціальних мережах стають об'єктом пропаганди та маніпуляцій, як наслідок, піддаються радикалізації й екстремістським нахилам, можуть навіть бути залучені до терористичної діяльності. Украй небезпечний стиль поведінки та жаргон (сленг), прийнятий у соціальних мережах,

Сленг породив безліч стереотипних виразів та інтернет-мемів, які містять масу ненормативної лексики та мають яскраво виражений асоціальний, агресивний і ксенофобський характер. Цей аспект необхідно піддати ретельному аналізу та вивченню, беручи до

уваги показники радикалізації та зростання екстремізму в підлітково-молодіжному середовищі;

3) комерційний ризик, пов'язаний із нелегальним скачуванням контенту, з іграми, рекламою;

4) ризик, пов'язаний із використанням персональних даних, оскільки діти та підлітки часто легко надають особисту інформацію про себе, членів сім'ї та своє оточення.

Важливо відзначити, що інтернет поки що нікому загалом не належить, як і не існує натепер єдиних законів, що регулюють Мережу по всьому світу, але боротьба за кібербезпеку, насамперед за безпеку молоді в інтернеті, – основний виклик часу в розвитку глобального мережевого простору, і, звичайно, Україна тут не є винятком.

Натепер пріоритетними напрямами розвитку інформаційної безпеки студентської молоді в закладах освіти є:

– удосконалення державної інформаційної безпеки, зокрема й щодо інформаційної безпеки;

– взаємодія органів освіти, правоохоронних органів і органів місцевої влади щодо запобігання негативним чинникам в інформаційній сфері серед молоді;

– удосконалення освітніх програм, заходів щодо інформаційної безпеки студентської молоді;

– ознайомлення здобувачів освіти з основними чинниками маніпулювання громадською свідомістю, зокрема й щодо розповсюдження недостовірної, неповної або упередженої інформації;

– формування національної свідомості студентів; виховання поваги до державної символіки, шанобливого ставлення до українських традицій і представників інших національностей, що живуть у країні;

– формування у здобувачів освіти почуття патріотизму, любові до рідного краю, національної гордості, розуміння особистого ставлення до подій, що відбуваються в Україні [9].

З метою подолання негативного впливу інтернету заклад освіти повинен здійснювати цілеспрямовану виховну роботу з педагогічним колективом, студентами, батьками.

Безпека здобувачів освіти є одним із головних завдань цивілізованого суспільства, тому убезпечувати їх в інтернеті повинні всі, хто причетний до цього суспільства.

Проблематика інформаційної безпеки найчастіше розглядається в контексті відповідної теми з курсу інформатики. Ми вважаємо, що ця проблема давно стала міждисциплінарною та має вирішуватися комплексно. Велику роль у її вирішенні відіграють якість виховного процесу та рівень довіри студента до батьків, куратора, викладачів.

Окреслимо детальніше інформацію, що наявна в розпорядженні закладів освіти в Україні:

1. Персональні дані здобувачів освіти, викладачів та інших категорій працівників. В Україні відповідно до вимог Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1 червня 2010 р. було ухвалено Закон України «Про захист персональних даних» [6]. Даним нормативно-правовим актом передбачено комплекс заходів із захисту приватної інформації та зазначено відповідальність за її неправомірне поширення.

2. Структурована навчальна інформація, яка забезпечує освітній процес (навчальні програми, бібліотеки, бази даних). Захист вказаної інформації здійснюється у зв'язку з необхідністю унеможливлення її повного або часткового пошкодження, тобто зменшення ризиків порушення або цілковитого припинення функціонування закладу освіти на певний період часу. Водночас навчальна інформація може включати елементи інтелектуальної власності, що були розроблені працівниками освітнього закладу відповідно до чинного законодавства або отримані в інших структурах (беручи до уваги деякі правовідносини).

3. Наукові напрацювання, які наділено ознаками інтелектуальної власності та захищено законодавством. Специфіка функціонування закладів освіти, перебусім закладів вищої освіти, передбачає здійснення викладацьким персоналом наукових досліджень, активну участь у грантових програмах тощо. Наукові результати, які отримані під час дослі-

джень, і згенеровані у процесі дані повинні бути захищені як продукти інтелектуальної власності. Також особливу увагу необхідно приділяти обмеженню доступу до інформації, яка генерується під час апробації та не набула вигляду комплексного наукового продукту, що опубліковано або запатентовано відповідними науковцями [1].

У межах розроблення ефективної стратегії інформаційної безпеки закладів освіти виділяють такі основні напрями [6; 9].

Нормативно-правове забезпечення є основою діяльності освітнього закладу з усіх напрямів. У закладі освіти має бути сформований пакет нормативно-правової документації державного, регіонального та внутрішнього рівнів із питань інформаційної безпеки. До таких документів належать документи з контентної фільтрації, з обробки персональної інформації, положення та регламенти з роботи в інтернеті як викладачів, так і студентів, різні положення про організацію профілактичної роботи з медіабезпеки, про форми профілактичної роботи зі здобувачами освіти щодо інтернет-безпеки, правила безпечної поведінки в мережі «Інтернет». У закладі освіти наказами мають бути призначені особи, відповідальні за контентну фільтрацію, за роботу з персональними даними, за організацією роботи здобувачів освіти в інтернеті тощо.

В *організаційному плані* щодо гарантування інформаційної та медіабезпеки в освітній установі має виконуватися низка заходів техніко-технологічної спрямованості:

– установлення лише ліцензійного програмного забезпечення;

– підключення до системи контентної фільтрації;

– установлення антивірусних програм;

– установлення та налаштування програм-фільтрів, брандмауерів.

До організаційних заходів належать:

– розроблення та реалізація правил інтернет-безпеки;

– організація роботи здобувачів освіти в інтернеті за розкладом з обмеженням часу та під наглядом викладачів або лаборантів;

– регулярна перевірка заходів, що вживаються в галузі інтернет-безпеки в освітній установі.

Для організації *профілактичної роботи* з медіабезпеки зі здобувачами освіти викладач повинен знати проблеми та небезпеки, які загрожують користувачу в інтернеті, та бути готовим дати рекомендації щодо вирішення цих проблем.

Для організації профілактичних заходів в освітній установі необхідно періодично проводити моніторинг, діагностику проблем з інтернет-безпеки серед молоді.

Адміністративно-організаційний аспект передбачає розроблення внутрішніх директив для регулювання деталей використання комп'ютерного обладнання, поводження з інформацією та її носіями. Окрім того, потрібні правила для студентів, які користуються інтернетом у комп'ютерних класах, порядок блокування небезпечного контенту для цієї групи та заборона використання персональних медіа.

Фізичний напрям передбачає формування пропускної системи за рівнем доступу до приміщень, де розміщено носій інформації навчального закладу. Лише авторизовані користувачі повинні мати доступ до сайту, використання ними інформації має бути лише в межах їхніх прав доступу до даних. Установлені паролі необхідно регулярно змінювати, щоб мінімізувати ризик отримання інформації або її компрометації третіми сторонами.

Технічний напрям. Для забезпечення якісного захисту інформації в навчальних закладах необхідно використовувати спеціалізоване програмне забезпечення для виявлення потенційних загроз і вжиття заходів проти них. В умовах обмеженого фінансування заходів, спрямованих на гарантування інформаційної безпеки в навчальних закладах, більшість закладів використовують лише антивірусні та безкоштовні продукти для протидії незаконному проникненню в інформаційні системи. Необхідно встановити фільтри для обмеження доступу студентів до окремих ресурсів в інтернеті. Наявна потреба в контролі доступу персоналу та студентів до електронної пошти. Також необхідно заборонити копіювання окремих видів

інформації з комп'ютерів у навчальних закладах [10]. Ефективна стратегія інформаційної безпеки передбачає комплексне використання вищезазначених сфер захисту даних. Ключові ролі на етапі запобігання незаконному доступу до інформації покладено на посадових осіб, які безпосередньо здійснюють комплекс заходів із захисту даних. Поряд із закладами освіти виховні функції у сфері інформаційної грамотності та безпеки учнів мають виконувати батьки.

Висновки. Формування інформаційної культури та безпеки – процес тривалий і складний, але важливий і необхідний. Інтернет може стати всесвітньою енциклопедією, що об'єднує інформаційні ресурси з усього світу. Завдання дорослих (педагогів, батьків) – сформувати різнобічну інтелектуальну особистість, високий моральний рівень якої буде запорукою її інформаційної безпеки. А для цього необхідно підвищувати кваліфікацію педагогів із питань інформаційної безпеки, щоб уміти орієнтувати здобувачів освіти з безпечної поведінки в інтернеті. Регулярно проводити консультування з питань кібербезпеки та працювати не навздогін, а на випередження.

Вирішення завдання щодо гарантування інформаційної безпеки потребує комплексного підходу, вирішення безлічі технічних, законодавчих, організаційних психолого-педагогічних завдань. Ці напрями мають стати основою для вирішення проблем кібербезпеки в закладах освіти.

Перспективами подальших розвідок убачаємо розроблення методичних рекомендацій щодо формування інформаційної безпеки здобувачів вищої освіти з метою організації сприятливого безпечного освітнього середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Варивода К. Інформаційна безпека підлітків в інтернет-мережі. *Молодий вчений*. 2016. № 3. С. 365–368.
2. Ковальчук В. Проблеми інформаційної безпеки дітей різних вікових категорій. URL: file:///C:/Users/1/Downloads /komp_2010_8_17.pdf (дата звернення: 20.10.2022).
3. Конституція України : Закон від 28 червня 1996 р. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141 (зі змінами, внесеними Законом України «Про внесення змін до Конституції України (щодо правосуддя)» від 2 червня 2016 р. *Відомості Верховної Ради України*. 2016. № 28. Ст. 532).
4. Куницький В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід. *Державне управління: теорія та практика.* 2011. URL: http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf (дата звернення: 10.03.2023).
5. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. *Ефективність державного управління*. 2015. Вип. 44. С. 13–20.
6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр. : Закон України від 9 січня 2007 р. № 537–V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E (дата звернення: 22.12.2022).
7. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 р. № 287/2015. URL: http://zakon5.rada.gov.ua/laws/show/287/2015 (дата звернення: 18.02.2023).
8. Про Стратегію інформаційної безпеки : Указ Президента України від 28 грудня 2021 р. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 04.04.2023).
9. Спірін О., Ковальчук В. Методика забезпечення онлайн-безпеки старшокласників у навчально-виховному процесі школи. *Інформаційні технології і засоби навчання.* 2011. № 1 (21). URL: http://www.journal.iitta.gov.ua (дата звернення: 04.04.2023).

INFORMATION SECURITY OF PARTICIPANTS IN THE EDUCATIONAL PROCESS AS AN ELEMENT OF A SECURE EDUCATIONAL ENVIRONMENT

TSISARUK IRYNA VASYLIVNA
Candidate of Pedagogical Sciences,
Senior Lecturer of the Department of Theory and Methods of Labor Education and Technology
Kremenets Taras Shevchenko Regional Academy of Humanities and Pedagogy

TSISARUK VITALIY YURIIOVYCH
Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor of the Theory and Methods of Labor Education and Technology
Kremenets Taras Shevchenko Regional Academy of Humanities and Pedagogy

OMELCHUK OLEKSANDR VASYLOVYCH
Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor of the Theory and Methods of Labor Education and Technology
Kremenets Taras Shevchenko Regional Academy of Humanities and Pedagogy

Currently, the Internet has become an integral part of our everyday life. The use of the network in educational institutions and at home expands the informational educational space and makes it possible to increase the effectiveness of education. However, the use of the Internet in educational activities hides many dangers.

Purpose. Investigate the issue of information security of education seekers as an element of a safe educational environment.

The following methods were used for the research: study of scientific-pedagogical and methodical literature on the research topic; analysis, synthesis, generalization, comparison, generalization of advanced pedagogical experience and study.

It was determined that the safety of education seekers is one of the main tasks of a civilized society, therefore everyone involved in this society should ensure their safety on the Internet. It was established that within the framework of the development of an effective information security strategy of educational institutions, the following main directions are distinguished: regulatory and legal support, in the organizational plan, preventive work, administrative-organizational, physical and technical. A safe educational environment is formed in educational institutions if the mentioned directions are implemented.

In the article highlights the issues of ensuring information security of participants in the educational process with the aim of organizing a safe educational environment. Four general categories of risk (risk related to the content of materials presented on the Internet; risk related to unwanted contacts; commercial risk; risk related to the use of personal data) to which students of education are exposed using the network are revealed Internet. The paper examines the priority areas of information security development of student youth in educational institutions.

Formation of information culture and security is a long and difficult process, but important and necessary. The Internet can become a global encyclopedia, uniting information resources from around the world. The task of adults (teachers, parents) is to form a versatile intellectual personality whose high moral level will be a guarantee of its information security. And for this, it is necessary to improve the qualifications of teachers in the field of information security in order to be able to orient students of education on safe behavior on the Internet. Regularly hold consultations on cyber security issues and work not to catch up, but to be ahead of the curve.

Solving the task of ensuring information security requires a comprehensive approach, solving a multitude of technical, legislative, organizational, psychological and pedagogical tasks. These directions should become the basis for solving cyber security problems in educational institutions.

Key words: *information security, Internet network, education seekers, educational institution, risk.*

REFERENCES

1. Varyvoda, K.S. (2016). Informatsiina bezpeka pidlitkiv v Internet merezhi [Information security of teenagers on the Internet]. *Molodyi vchenyi.* № 3. S. 365–368 [in Ukrainian].
2. Kovalchuk, V.N. Problemy informatsiinoi bezpeky ditei riznykh vikovykh katehorii [Problems of information security of children of different age categories]. Retrieved from: file:///C:/Users/1/Downloads /komp_2010_8_17.pdf (data zvernennia: 20.10.2022) [in Ukrainian].
3. Konstytutsiia Ukrainy vid 28 chervnia 1996 roku. *Vidomosti Verkhovnoi Rady Ukrainy.* 1996. № 30. St. 141 (zi zminamy, vnesenymy Zakonom Ukrainy “Pro vnesennia zmin do Konstytutsii Ukrainy

(shchodo pravosuddia)" vid 2 chervnia 2016 roku. *Vidomosti Verkhovnoi Rady Ukrainy.* 2016. № 28. St. 532) [Constitution of Ukraine dated June 28, 1996] [in Ukrainian].

4. Kunytskyi, V.V. (2011). Zakhyst nepovnolitnikh v informatsiinomu prostori yak obiekt humanitarnoi ekspertyzy: ukrainskyi ta zarubizhnyi dosvid [Protection of minors in the information space as an object of humanitarian expertise: Ukrainian and foreign experience]. *Derzhavne upravlinnia: teoriia ta praktyka*. Retrieved from: http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf (data zvernennia: 10.03.2023) [in Ukrainian].
5. Malyk, Ya. (2015). Informatsiina bezpeka Ukrainy: stan ta perspektyvy rozvytku [Information security of Ukraine: state and prospects for development]. *Efektyvnist derzhavnoho upravlinnia.* Vyp. 44. S. 13–20 [in Ukrainian].
6. Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 rr. : Zakon Ukrainy vid 9 sichnia 2007 r. № 537–V [About Basic principles of the development of information society in Ukraine in 2007–2015: Zakon Ukrainy vid 9 January 2007 y. № 537-V]. Retrieved from: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E (data zvernennia: 22.12.2022) [in Ukrainian].
7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 26.05.2015 № 287/2015 [On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine dated May 26, 2015 № 287/2015]. Retrieved from: http://zakon5.rada.gov.ua/laws/show/287/2015 (data zvernennia: 18.02.2023) [in Ukrainian].
8. Pro Stratehiiu informatsiinoi bezpeky : Ukaz Prezydenta Ukrainy 28 hrudnia 2021 roku [About the Information Security Strategy: Decree of the President of Ukraine on December 28, 2021]. Retrieved from: /https://zakon.rada.gov.ua/laws/show/685/2021#Text (data zvernennia: 04.04.2023) [in Ukrainian].
9. Spirin, O.M., Kovalchuk, V.N. Metodyka zabezpechennia on-lain bezpeky starshoklasnykiv u navchalno-vykhovnomu protsesi shkoly [The method of ensuring the online safety of high school students in the educational process of the school]. *Informatsiini tekhnolohii i zasoby navchannia*. 2011. № 1 (21). Retrieved from: http://www.journal.iitta.gov.ua (data zvernennia: 04.04.2023) [in Ukrainian].