

ГАРАНТІЇ БЕЗПЕКИ ДАНИХ СУЧАСНИХ ПЛАТФОРМ ДЛЯ ОНЛАЙН-НАВЧАННЯ ТА ВЕДЕННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ОСВІТНІХ УСТАНОВ СИСТЕМИ МВС УКРАЇНИ

DATA SECURITY GUARANTEES OF MODERN PLATFORMS FOR ONLINE LEARNING AND ELECTRONIC DOCUMENT CIRCULATION OF EDUCATIONAL INSTITUTIONS OF THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE

Кудінов В.А., к.ф.-м.н., доцент,
завідувач кафедри інформаційних технологій
Національна академія внутрішніх справ

Корнейко О.В., к.т.н., професор,
професор кафедри інформаційних технологій
Національна академія внутрішніх справ

Пакриш О.Є., к.т.н., доцент,
доцент кафедри інформаційних технологій
Національна академія внутрішніх справ

У статті досліджено комплекс гарантій безпеки даних у критично важливому середовищі – сучасних платформах для онлайн-навчання та ведення електронного документообігу освітніх установ системи МВС України. Актуальність роботи зумовлена інтенсивною діджиталізацією освітнього процесу та необхідністю захисту службової інформації та державних інформаційних ресурсів в умовах воєнного стану та підвищеної активності кіберзагроз. Метою дослідження є ідентифікація, систематизація та обґрунтування комплексу організаційно-правових, технічних та інфраструктурних гарантій безпеки даних, необхідних для забезпечення конфіденційності, цілісності та доступності даних сучасних платформ для онлайн-навчання та ведення електронного документообігу освітніх установ системи МВС України. Методологічну основу становлять загальнонаукові та спеціально-юридичні методи: аналіз, синтез, системно-структурний, порівняльно-правовий, формально-догматичний та експертних оцінок. На основі системного аналізу міжнародного досвіду та української нормативно-правової бази визначено ключові вразливості платформ, пов'язані з використанням вебдоступу та хмарних технологій. Обґрунтовано необхідність застосування стандартів криптографічного захисту та двофакторної автентифікації як базових елементів архітектури безпеки. Запропоновано комплекс заходів для підвищення кіберстійкості платформ, включаючи регулярний аудит безпеки та спеціалізовану підготовку фахівців, відповідальних за кіберзахист об'єктів критичної інфраструктури. Наукова новизна роботи полягає у систематизації та обґрунтуванні комплексної моделі гарантій безпеки даних, адаптованої до гібридного середовища онлайн-навчання та електронного документообігу в освітніх установах зі специфічним статусом, що дозволило розробити конкретні рекомендації щодо підвищення їхньої кіберстійкості в умовах воєнного стану. Практична значущість роботи полягає у наданні науково обґрунтованих рекомендацій щодо вдосконалення відомчих стандартів та протоколів безпеки, спрямованих на захист даних сучасних платформ для онлайн-навчання та ведення електронного документообігу освітніх установ системи МВС України.

Ключові слова: кібербезпека, кіберзахист, онлайн-навчання, електронний документообіг, гарантії безпеки даних, освітні установи, МВС України.

The article examines a set of data security guarantees in a critically important environment – modern platforms for online learning and electronic document circulation of educational institutions of the system of the Ministry of Internal Affairs of Ukraine. The relevance of the work is due to the intensive digitalization of the educational process and the need to protect official information and state information resources in conditions of martial law and increased activity of cyber threats. The purpose of the study is to identify, systematize and substantiate a set of organizational, legal, technical and infrastructural guarantees of data security necessary to ensure the confidentiality, integrity and availability of data of modern platforms for online learning and electronic document circulation of educational institutions of the system of the Ministry of Internal Affairs of Ukraine. The methodological basis is made up of general scientific and special legal methods: analysis, synthesis, system-structural, comparative legal, formal-dogmatic and expert assessments. Based on a systematic analysis of international experience and the Ukrainian regulatory framework, key vulnerabilities of platforms related to the use of web access and cloud technologies have been identified. The need to apply cryptographic protection standards and two-factor authentication as basic elements of the security architecture has been substantiated. A set of measures has been proposed to increase the cyber resilience of platforms, including regular security audits and specialized training of specialists responsible for the cyber protection of critical infrastructure facilities. The scientific novelty of the work lies in the systematization and substantiation of a comprehensive model of data security guarantees adapted to the hybrid environment of online learning and electronic document management in educational institutions with a specific status, which allowed the development of specific recommendations for increasing their cyber resilience in martial law conditions. The practical significance of the work lies in providing scientifically based recommendations for improving departmental standards and security protocols aimed at protecting data of modern platforms for online learning and maintaining electronic document flow of educational institutions of the Ministry of Internal Affairs of Ukraine.

Key words: cybersecurity, cyber protection, online learning, electronic document flow, data security guarantees, educational institutions, Ministry of Internal Affairs of Ukraine.

Вступ. Сьогодні спостерігається інтенсивна цифровізація усіх сфер суспільного життя, яка вимагає нових підходів до забезпечення кібербезпеки та кіберзахисту. Так, в умовах воєнного стану, спричиненого широкомасштабним вторгненням РФ в Україну, ця вимога набуває статусу пріоритету національної безпеки. Не винятком стали і освітні установи системи МВС України, які, спираючись на законодавчу базу, невинно діджиталізуються, що значно підвищує ефективність їх функціонування. Зокрема,

онлайн-навчання та ведення електронного документообігу стали ключовими факторами забезпечення безперервності роботи цих освітніх установ. Проте, із впровадженням сучасних платформ виникає гостра необхідність забезпечення надійного захисту їх баз даних. Це робить їх критично важливими об'єктами, що потребують комплексних гарантій безпеки.

Актуальність роботи зумовлена наявністю кіберзагроз, які постійно зростають в світі та Україні, зокрема,

та відсутністю уніфікованої моделі гарантій безпеки, що інтегрувала б організаційно-правові та технологічні аспекти захисту в умовах гібридної освіти. При будь-якому рівні захисту інформаційних ресурсів завжди існують фінансові, технічні та репутаційні кіберризики від можливих атак, що вимагає розробки нових підходів до кіберстійкості. Метою статті є ідентифікація, систематизація та обґрунтування комплексу організаційно-правових, технічних та інфраструктурних гарантій безпеки даних для сучасних інформаційно-комунікаційних систем (далі – ІКС) освітніх установ системи МВС України, що забезпечують освітній процес та електронний документообіг. Для досягнення мети в роботі було використано: системний підхід, порівняльно-правовий метод (для аналізу нормативної бази та стандартів), формально-логічний метод (для уточнення понятійного апарату) та метод експертних оцінок (для ідентифікації реальних загроз та ризиків).

Результати й обговорення.

1. Розглянемо сучасні платформи для онлайн-навчання та ведення електронного документообігу освітніх установ системи МВС України.

З розвитком цифрових технологій заклади вищої освіти (далі – ЗВО) системи МВС України активно впроваджують онлайн-платформи для організації освітнього процесу, ведення електронних журналів, електронного документообігу, створення та подачі звітності, а також обробки фінансових даних. Онлайн-платформи стали невід’ємною частиною сучасної освітньої системи. Вони не лише спрощують доступ до інформації, але й забезпечують гнучкість освітнього процесу, зокрема під час дистанційного або змішаного навчання.

Особливість таких платформ полягає у їхній здатності об’єднувати всі ключові процеси в межах однієї системи. Це включає управління навчальними матеріалами, облік успішності, моніторинг відвідуваності, автоматизацію фінансової звітності та організацію комунікації між учасниками освітнього процесу. Вони підтримують прозорість у системі освіти, що особливо важливо для підвищення довіри учасників освітнього процесу і суспільства до роботи освітніх установ.

В ЗВО системи МВС України для організації освітнього процесу та ведення електронного документообігу активно використовуються такі популярні платформи:

1) «АСУ НЗ» – система, яка використовується для ведення онлайн-журналів, обліку відвідуваності, оцінок та іншої документації. Інтерфейс платформи розроблено таким чином, щоб науково-педагогічні працівники могли швидко вносити оцінки, а адміністрація – отримувати аналітику про успішність здобувачів вищої освіти.

2) «Moodle»–LMS (Learning Management System), яка дозволяє створювати дистанційні курси, надавати доступ до навчальних матеріалів, вести облік успішності здобувачів вищої освіти, проводити тести та інші форми оцінювання. Moodle широко використовується у закладах вищої освіти. Одна з ключових переваг Moodle – її гнучкість у налаштуванні і можливість роботи як на локальному сервері, так і в хмарному середовищі.

3) «Google Classroom» та «Microsoft Teams» – інструменти, що надають функції для організації онлайн-занять, можливості застосування різних форм завдань, а також для організації електронного документообігу. Їхні переваги полягають у доступності з будь-якого пристрою, інтеграції з іншими сервісами та можливості одночасної роботи великої кількості користувачів.

4) «Система електронної взаємодії органів виконавчої влади» (СЕВ ОВВ) – призначена для автоматизації процесів створення, надсилання, передавання, одержання, оброблення, використання, зберігання, знищення електронних документів та копій паперових документів в електронному вигляді з використанням електронного циф-

рового підпису, які не містять інформацію з обмеженим доступом, та контролю за виконанням актів, протокольних рішень Кабінету Міністрів України та інших документів [1].

5) «Система електронного документообігу МВС України» (МІА: СЕД) – забезпечує можливість автоматизації роботи з електронними документами в діловодстві – створення документів, їх поширення та контроль документообігу всередині підприємства або електронному міжвідомчому обміні. Забезпечує організацію універсального вебдоступу до корпоративних документів, з розподіленим авторизованим доступом, з можливістю ефективної віддаленої роботи з ними [2, с. 2].

2. Розглянемо гарантії безпеки даних на сучасних платформах освітніх установ системи МВС України.

Як відомо, правове забезпечення кібербезпеки в Україні регулюється законами України «Про інформацію» [3], «Про національну безпеку України» [4], «Про основні засади забезпечення кібербезпеки України» [5], указами Президента України «Про Стратегію національної безпеки України» [6] та «Про Стратегію кібербезпеки України» [7], «Конвенцією про кіберзлочинність» [8].

Одним із найбільш важливих аспектів використання онлайн-платформ є питання захисту даних, оскільки вони містять не лише інформацію про учасників освітнього процесу, а й фінансові документи, що потребує підвищеної конфіденційності та гарантій різних рівнів безпеки даних, а саме:

1) шифрування даних (якщо потрібна передача конфіденційної інформації через мережу Інтернет, то вона повинна відбуватися за допомогою шифрування, тому більшість сучасних платформ використовують протоколи HTTPS, а також більш складні методи шифрування для забезпечення недоступності даних для сторонніх осіб);

2) багаторівнева аутентифікація (використання двофакторної аутентифікації (2FA) забезпечує додатковий рівень захисту, дозволяючи користувачам підтверджувати свою особу через другий пристрій, наприклад, мобільний телефон);

3) захист від DDoS атак (платформи повинні мати належну інфраструктуру для захисту від атак на рівні мережі, що забезпечує їхню безперебійну роботу навіть у разі спроби блокування доступу);

4) резервне копіювання даних (постійне створення резервних копій зберігає критично важливу інформацію та забезпечує її відновлення у разі технічного збою або втрати доступу до основного сервера);

5) моніторинг активності (платформи повинні мати системи фіксації усіх спроб доступу, змін даних або підозрілих активностей, що дозволяє швидко виявляти зловмисні дії).

Проаналізуємо рівні захисту вищезазначених платформ:

1) «АСУ НЗ» – використовуються хмарні сервери із багаторівневим шифруванням, підтримка безпеки через ізоляцію даних кожного структурного підрозділу; 2) «Moodle» – гнучкі налаштування прав доступу, підтримка HTTPS-протоколу, резервне копіювання на локальні сервери; 3) «Google Classroom» та «Microsoft Teams» – резервування даних на географічно розподілених серверах; 4) «Система електронної взаємодії органів виконавчої влади» (СЕВ ОВВ) – Державна служба спеціального зв’язку та захисту інформації України зареєструвала атестат відповідності 20 грудня 2019 р. за № 20965, у якому засвідчено, що комплексна система захисту інформації ядра системи електронної взаємодії органів виконавчої влади версія 2.0 забезпечує захист інформації відповідно до вимог нормативних документів системи технічного захисту інформації в Україні» [1]; 5) «Система електронного документообігу МВС України» (МІА: СЕД) – забезпечує можливість підписувати документи за допомогою

електронного підпису і зашифровувати їх; дозволяє розмежувати повноваження, доступ до документів і дій над ними співробітникам організації та здійснювати контроль за доступом до документів [2].

Такі платформи, як Google Classroom [9] та Microsoft Teams [10], забезпечують надійний захист даних завдяки використанню сучасних технологій безпеки, які постійно оновлюються для протидії новим загрозам [11], але й вони не завжди досконалі. Про це свідчить історія кібератак на освітні онлайн-ресурси [12, 13]. Наприклад, у 2017 році через хакерську атаку на Moodle були скомпрометовані дані понад 1 млн користувачів, серед яких облікові записи учасників освітнього процесу. У 2020 році Zoom став мішенню численних атак через різке зростання його популярності під час пандемії. В Україні освітні платформи неодноразово ставали мішенню DDoS атак, які порушували доступ до системи на декілька годин.

Для надійного захисту сучасних платформ для онлайн-навчання та ведення електронного документообігу освітніх установ системи МВС України необхідно створити комплексну систему захисту інформації (далі – КСЗІ) в них [14].

Відповідно до рубрики «Термінологія законодавства» веб-порталу Верховної Ради України [15] під КСЗІ розуміють «взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації» [16] або «сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації» [17]. Таким чином, КСЗІ – це сукупність організаційних та інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

Створення КСЗІ в ІКС здійснюється відповідно до вимог нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003 -2005 [18] на підставі технічного завдання, розробленого згідно з вимогами нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-001 -99 [19].

Метою створення КСЗІ сучасних платформ ЗВО МВС України є забезпечення захисту інформації, що циркулює в них, та самих ІКС. Захист інформації має здійснюватися шляхом протидії загрозам, які можна очікувати внаслідок дій порушника на всіх технологічних етапах її обробки і в усіх режимах функціонування платформ. Завдання цієї КСЗІ – це забезпечення конфіденційності, цілісності, доступності інформації баз даних шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованих дій (у тому числі з використанням комп'ютерних вірусів), які можуть призвести до її випадкової або умисної модифікації чи знищення. Об'єктом захисту КСЗІ є інформація, в будь-якому її вигляді та формі подання.

Для здійснення захисту інформації на всіх стадіях життєвого циклу сучасних платформ для онлайн-навчання

та ведення електронного документообігу освітніх установ системи МВС України у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

– організаційно-правові та інженерно-технічні заходи, які реалізуються поза обчислювальною системою платформи;

– апаратні, програмно-апаратні та програмні засоби захисту від несанкціонованого доступу, реалізації функцій криптографічного захисту інформації та забезпечення доступності інформації, яка обробляється й зберігається в ІКС.

Відповідно до вимог нормативно-правових актів та нормативних документів, що регламентують впровадження КСЗІ в ІКС, експертний висновок та Атестат відповідності є кінцевим результатом виконання робіт з побудови КСЗІ в системі.

У відповідності до вимог КСЗІ на автоматизованих робочих місцях користувачів обов'язково мають бути встановлені технічні засоби та спеціалізоване програмне забезпечення:

1. Програмне забезпечення антивірусного захисту – комплекс програмних модулів для виявлення та знешкодження комп'ютерних вірусів і шкідливих програм в режимі реального часу.

2. Програмний комплекс клієнта захисту, що призначений для здійснення автентифікації користувачів на шлюзі захисту і встановлення захищеного з'єднання для передачі даних.

У якості засобів комплексного захисту інформації використовуються виключно ті засоби комплексного захисту інформації, які мають чинний, позитивний експертний висновок Адміністрації Держспецзв'язку в сфері комплексного захисту інформації. Вони реалізують захист конфіденційності та контроль цілісності даних, які передаються по каналах зв'язку в цих платформах.

Основними результатами реалізації у повному обсязі КСЗІ в ІКС буде забезпечення належного рівня конфіденційності, цілісності, доступності інформації.

Висновки. Таким чином, гарантії безпеки даних сучасних платформ для онлайн-навчання та ведення електронного документообігу освітніх установ системи МВС України повинні бути сфокусовані на комплексному, системному підході до захисту, що поєднує технічні, правові та організаційні аспекти у специфічному, критичному для держави, середовищі. В роботі систематизовано та обґрунтовано комплексну модель гарантій безпеки даних, адаптовану до гібридного середовища онлайн-навчання та електронного документообігу в освітніх установах зі специфічним статусом, що дозволило розробити конкретні рекомендації щодо підвищення їхньої кіберстійкості в умовах воєнного стану.

ЛІТЕРАТУРА

1. Система електронної взаємодії органів виконавчої влади (СЕВ ОБВ). Дія : [сайт]. URL: <https://se.dii.gov.ua/sev-ovv>.
2. Сохацький М., Федоренко В. Система електронного документообігу «МІА: Документообіг» : посібн. користувача МІА:СЕД (04 січ. 2023 р.). Київ : ДП «ІНФОТЕХ». URL: <https://axiosis.github.io/books/crm/mia-sed.pdf>.
3. Про внесення змін до Закону України «Про інформацію» : Закон України від 13 січ. 2011 р. № 2938-VI // *Відомості Верховної Ради України*. 2011. № 32. Ст. 313.
4. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII // *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII // *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
6. Про рішення Ради національної безпеки і оборони України від 14 верес. 2020 р. «Про Стратегію національної безпеки України» : Указ Президента України від 14 верес. 2020 р. № 392/2020.
7. Про рішення Ради національної безпеки і оборони України від 14 трав. 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 14 трав. 2021 р. № 447/2021.
8. Конвенція про кіберзлочинність від 23 листоп. 2001 р. № 994_575. Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV від 07 верес. 2005 р. // *Відомості Верховної Ради України*. 2006. № 5-6. Ст. 71.
9. Google Classroom: посібн. для навч. закладів. Google for Education : [сайт]. URL: edu.google.com.
10. Microsoft Teams для освіти: функції та безпека. Microsoft : [сайт]. URL: <http://www.microsoft.com>.

11. Ринок кібербезпеки в Україні: зростання, виклики та інновації. *SPEKA* : [сайт]. URL: <https://speka.media/rinok-kiberbezpeki-v-ukrayini-rist-vikliki-ta-innovaciyi-93lyx4>.
12. Устименко І. О. Платформи для онлайн-навчання в Україні: переваги та недоліки. *Інтернет-технології в освіті*. 2021. № 2. С. 90-99.
13. Шевченко Т. П. Цифрові платформи в освіті: огляд основних можливостей та загрози. *Інформаційні технології в освіті*. 2019. № 1(6). С. 47-55.
14. Кудінов В. А. Загальний порядок побудови комплексної системи захисту інформації в інформаційно-телекомунікаційній системі «Інформаційний портал Національної поліції України». *Кібербезпека в Україні: правові та організаційні питання*: матеріали III міжнар. наук.-практ. конф. (Одеса, 19 листоп. 2021 р.). Одеса: Одеський держ. ун-т внутр. справ, 2021. С. 56–58.
15. «Термінологія законодавства» веб-порталу Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/main/termin>.
16. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР (редакція від 19.04.2014). URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed20140419#n22>.
17. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах : Постанова Кабінету Міністрів України від 16 листоп. 2002 р. № 1772. URL: <https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF/ed20070101/conv/#Text>.
18. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003 -2005) : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 08 листоп. 2005 р. № 125 із змінами. URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>.
19. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (НД ТЗІ 3.7-001-99) : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квіт. 1999 р. № 22 із змінами. URL: <https://tzi.com.ua/downloads/3.7-001-99.pdf>.