DOI: https://doi.org/10.32782/PPSS.2023.1.33

ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СТУДЕНТІВ ТА ПРАЦІВНИКІВ ПЕРЕМІЩЕНИХ УНІВЕРСИТЕТІВ

Тетяна Петрівна НЕСТОРЕНКО,

канд. екон. наук, доц.,
доцент кафедри економіки,
підприємництва та фінансів
Бердянського державного
педагогічного університету
https://orcid.org/0000-0001-8294-6235

INFORMATION SECURITY PRINCIPLES OF DISPLACED UNIVERSITIES' STUDENTS AND STAFF

The study focuses on ensuring security in the relocated university network and mitigating information threat risks. Students and staff in occupied territories confront serious threats from occupying authorities, including limited information access, censorship, and insecure personal data. Protecting personal data involves measures like robust passwords, two-factor authentication, and regular software updates. A comprehensive approach includes educational initiatives to foster an informed information culture. Relocated universities need to enact robust network security, with secure networks, firewalls, and intrusion detection. Developing incident response plans and conducting regular training sessions are crucial measures for effective security and risk reduction in the university network.

В результаті широкомасштабного вторгнення російських військ на територію України ряд українських населених пунктів опинився під окупацією, включаючи ті, що знаходяться в Луганській, Донецькій, Херсонській, Запорізькій, Київській, Чернігівській, Сумській та Харківській областях. Деякі з цих територій в 2022 році були звільнені від окупації. Мова йдеться про Київську, Чернігівську, Сумську області, майже всю Харківщину, частини Миколаївської й Запорізької областей та Донбасу, правобережну Херсонщину та острів Зміїний (Одеська область). Протягом 9 років воєнного конфлікту окупанти анексували 18% території України. У 2014 році росія захопила приблизно 7% земель, а після повномасштабного вторгнення в лютому 2022 року ще 10.9%. Решта 0.08% (приблизно 857 кв. км) представляють собою територію України, що окупована росією протягом 2023 року. Проте протягом цього періоду Україні вдалося відновити контроль над 370 кв. км своєї території (рис.1) [3].

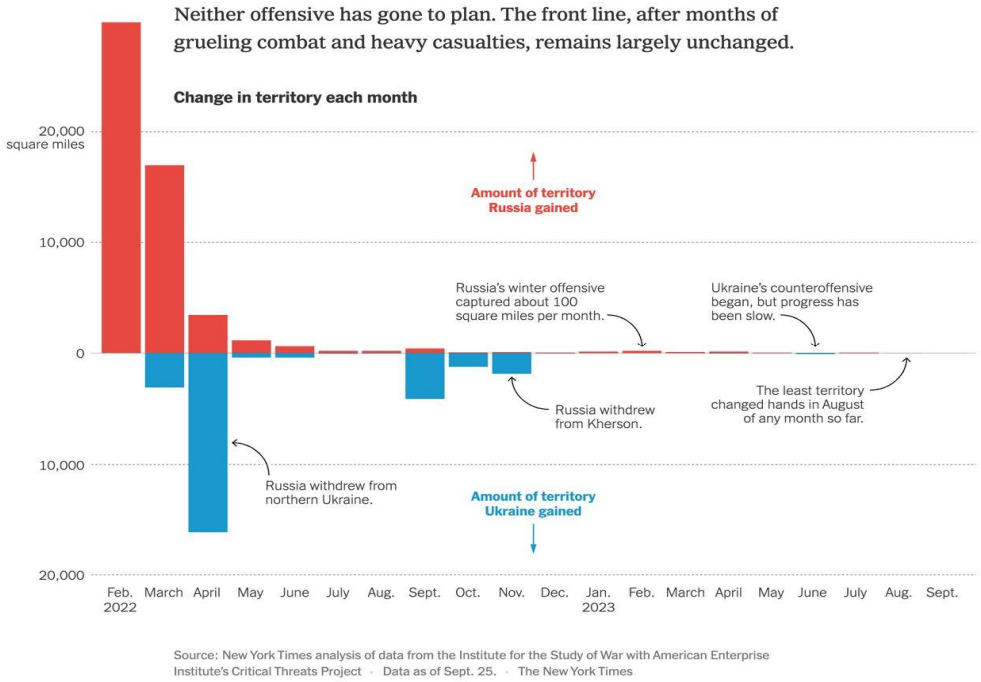

Рис.1. Щомісячні зміни території України, що звільнена ЗСУ /окупована росією
Джерело: [3]

Разом з ним, станом на листопад 2023 року окупованим залишаються такі міста Запорізької області, як Бердянськ, Василівка, Дніпрорудне, Енергодар, Кам'янка-Дніпровська, Мелітополь, Молочанськ, Пологи, Приморськ, Токмак. Тому три заклади вищої освіти, розташовані на півдні Запорізької області, після повномасштабного вторгнення російської навали змушені були були релокуватися на територію, яка є підконтрольною українській владі, та поки що не мають можливості повернутися в рідні стіни [1, 7]:

Бердянський державний педагогічний університет разом з відокремленим структурним підрозділом "Бердянський економіко-гуманітарний коледж Бердянського державного педагогічного університету" тимчасово переміщений на базу Запорізького національного університету (вул. Жуковського, 66, Запоріжжя).

Мелітопольський державний педагогічний університет імені Богдана Хмельницького тимчасово переміщений на базу Комунального закладу вищої освіти "Хортицька національна навчально-реабілітаційна академія" Запорізької обласної ради (вул. Наукового Містечка, 59, Запоріжжя).

Таврійський державний агротехнологічний університет імені Дмитра Моторного разом з відокремленими структурними підрозділами "Василівський фаховий коледж Таврійського державного агротехнологічного університету імені Дмитра Моторного", "Ногайський фаховий коледж Таврійського державного агротехнологічного університету імені Дмитра Моторного", "Мелітопольський фаховий коледж Таврійського державного агротехнологічного університету імені Дмитра Моторного", "Бердянський фаховий коледж Таврійського державного агротехнологічного університету імені Дмитра Мотор-

ного" тимчасово переміщено на базу Запорізького національного університету (вул. Жуковського, 66, Запоріжжя).

Для приймаючого міста поява переміщеного університету має суттєвий вплив як з економічної точки зору [2], так і з точки зору культурної та наукової динаміки, розвитку інфраструктури, створення кадрового резерву тощо [4].

Варто зазначити, що переміщені університети стають вразливими до інформаційних загроз, оскільки їхні студенти та працівники часто опиняються у нових інформаційних середовищах [5]. В силу різних причин певна частина викладачів, адміністративного персоналу, студентів університетів не виїхала з окупованих територій та продовжує здійснювати роботу або навчання в умовах надзвичайної нестабільності. Ця ситуація підвищує піддатливість університетів до інформаційних загроз, оскільки працівники та студенти можуть опинитися у складних ситуаціях, де вони вимушені приховувати свої відносини з переміщеними університетами через політичні, соціальні чи безпекові обставини. Ця складна обстановка підкреслює необхідність розгортання ефективних заходів з інформаційної безпеки для захисту конфіденційної інформації та забезпечення стійкості університетських інформаційних систем в умовах нестабільності та конфлікту.

Студенти та викладачі, які залишилися на окупованих територіях, стикаються з рядом серйозних загроз з боку окупаційної влади. До таких загроз можна віднести обмежений доступ до інформації, наявність цензури та контролю, відсутність безпеки особистих даних, загроза особистій безпеці (через політичні чи соціальні напруження на окупованих територіях, що може вплинути на їхній статус та свободу).

Визначення та впровадження засад захисту особистих даних студентів та працівників є невід'ємною частиною широкого стратегічного підходу до інформаційної безпеки. Однією з ключових складових є встановлення сильних паролів, що включають у себе комбінації різноманітних символів, цифр та великих/малих літер. Це забезпечує надійний бар'єр для несанкціонованого доступу до особистих даних.

Додатковий рівень безпеки може бути забезпечений за допомогою двофакторної аутентифікації, де крім стандартного пароля вимагається введення додаткового коду або використання біометричних даних. Цей метод робить доступ до інформації значно складнішим для несанкціонованих осіб, зменшуючи ризик витоку чи злому безпеки. Регулярне оновлення програмного забезпечення також має ключове значення для забезпечення безпеки. Це включає в себе оновлення операційних систем, антивірусних програм та інших застосунків. Актуальне програмне забезпечення гарантує, що використовувані заходи безпеки є максимально ефективними та адаптованими до нових загроз. Загальний підхід до захисту особистих даних повинен враховувати не лише технічні аспекти, але й освітні заходи для користувачів, щоб створити свідому інформаційну культуру і сформувати усвідомленість щодо інформаційної безпеки серед студентів, викладачів та працівників переміщених університетів.

Переміщені університети мають активно впроваджувати комплексні заходи забезпечення безпеки в мережі, щоб захистити важливу інформацію та

інфраструктуру від потенційних інформаційних загроз. Це має передбачати наступні заходи:

– розгортання сучасних технологій для створення захищених мереж, які забезпечують конфіденційність та цілісність даних, а також доступ лише авторизованим користувачам;

– встановлення та налагодження мережевих брандмауерів для моніторингу та фільтрації трафіку, що входить та виходить з університетської мережі, з метою захисту від небажаних атак та забезпечення безпеки даних;

– використання систем виявлення вторгнень для постійного моніторингу мережевої активності та вчасного виявлення можливих загроз чи аномалій в системі;

– розробка та впровадження докладного плану реагування на інциденти, який визначає кроки та процедури для негайного реагування під час інформаційних атак. Цей план має охоплювати відновлення даних, ізоляцію атак та співпрацю з кібербезпековими експертами. Для розробки плану дій доцільно використовувати досвід, напрацьований закладами освіти під час пандемії Covid-19 [6];

– проведення систематичних аудитів безпеки для виявлення потенційних вразливостей та удосконалення системи захисту від нових методів атак;

– організація та проведення регулярних тренінгів та навчань для викладачів, персоналу та студентів щодо безпечного користування мережевими ресурсами та виявлення підозрілих активностей;

– забезпечення захисту персональних даних викладачів, працівників та студентів, які знаходяться на окупованій території.

Впровадження цих заходів допоможе забезпечити ефективний рівень безпеки в мережі переміщених університетів та зменшити ризики, що пов'язані з інформаційними загрозами.

Список використаних джерел:

1. Інформація про тимчасово переміщені заклади вищої освіти, що належать до сфери управління Міністерства освіти і науки України. Міністерство освіти і науки України. URL: http://surl.li/nkzeu (дата звернення: 21.11.20230).

2. Несторенко Т. П. Значення університету для економіки міста: приклад впливу переміщеного університету. Вісник Хмельницького національного університету, №5, т. 1, 2021 (298), 223-227. https://doi.org/10.31891/2307-5740-2021-298-5(1)-39 (дата звернення: 15.11.20230).

3. Подставной Д. Скільки українських територій було звільнено та окуповано у 2023 році: інфографіка від NYT. Telegraf. 28.09.2023. URL: http://surl.li/nkxqh (дата звернення: 20.11.20230).

4. Abyzova L., Babenko O., Nestorenko T., Reshetova I., Semeniuk M., Shevchenko O. Educational management in Ukraine: the place of displaced universities. Sustainable Development Goals: The 2030 Agenda & Does environmental diplomacy reflect new challenges regarding climate change? Workshop 8.11.2017. University of Economics in Bratislava, Bratislava. URL: https://cutt.ly/SYcVUXq (дата звернення: 15.11.20230).

5. Nestorenko T., Nestorenko O., Peliova J. Displaced and fake universities – experience of Ukraine. Economic, Political and Legal Issues of International Relations 2017. 9. - 10. júna 2017, Virt, Volume of Scientific Papers // Ekonomická univerzita v Bratislave, Fakulta medzinárodných vzťahov, pp.265-271. URL: https://cutt.ly/hYcVSgE (дата звернення: 16.11.20230).

6. Ostenda A., Istomina D., Kravchenko N., Alekseeva G., Nestorenko T., Horbatiuk L. Роль засобів ІКТ в організації процес у інформування учнів під час карантину. Zeszyty naukowe

WST, Польща, 2022, nr 14, S. 109-126. https://doi.org/10.54264/0037 (дата звернення: 17.11.20230).

7. Peliova J., Nestorenko T., Kovachov S., Suchikova Y., Nestorenko O. Adapting to adversity: a case study of asynchronous learning implementation in a relocated university amidst war. Zeszyty Naukowe Wyższej Szkoły Technicznej w Katowicach. 2023, nr 16, 119-132. https://doi.org/10.54264/0067 (дата звернення: 15.11.20230).