УДК 37:002, 004:37.042:37:005

Литвинчук А. О.
кандидат економічних наук, перший заступник директора ДНУ «Інститут освітньої аналітики», Київ, Україна, a.litvinchuk@iea.gov.ua
ORCID ID: https://orcid.org/0000-0002-7523-558X

Кир'янов А. В.
заступник директора з науково-проектної роботи та ІТ ДНУ «Інститут освітньої аналітики», Київ, Україна, a.kiryanoff@iea.gov.ua
ORCID ID: https://orcid.org/0000-0003-0452-7689

Іриневич Ю. В.
кандидат економічних наук, старший науковий співробітник відділу освітньої статистики і аналітики ДНУ «Інститут освітньої аналітики», Київ, Україна, nnaru1@ukr.net
ORCID ID: https://orcid.org/0000-0003-1755-5240

Гайдук І. С.
науковий співробітник сектору організації автоматизованого збору освітньої статистики ДНУ «Інститут освітньої аналітики», Київ, Україна, gaiduk94ivan@gmail.com
ORCID ID: https://orcid.org/0000-0003-3144-1469

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА УПРАВЛІННЯ ІНКЛЮЗИВНОЮ ОСВІТОЮ В УМОВАХ ВОЄННОГО СТАНУ З УРАХУВАННЯМ ДОСВІДУ ЄС

Анотація. *Метою статті є дослідження сучасних шляхів удосконалення інформаційно-аналітичної підтримки управління інклюзивною освітою в кризових умовах з урахуванням досвіду ЄС. Наведено перелік компонентів, які входять до складу центрального програмно-технічного комплексу АС «ІРЦ». Проаналізовано типи сучасних загроз інформаційній безпеці в АС «ІРЦ», які впливають на інформацію, що обробляється та зберігається в АС «ІРЦ», й технологічні дані. Розглянуто критерії забезпечення захисту інформації від несанкціонованого доступу засобами криптозахисту, моніторингу системних журналів реєстрації роботи програмних і технічних засобів, аналізу порушень у роботі АС «ІРЦ», налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів, визначення повноважень користувачів цієї системи. Запропоновано впровадження для потреб АС «ІРЦ» організаційних і технічних заходів із кіберзахисту, які вживаються для об'єктів критичної інформаційної інфраструктури. Описано дії із забезпечення доступності й відмовостійкості компонентів та інформаційних ресурсів АС «ІРЦ». Зроблено висновок, що для збереження інформації за аварійних режимів роботи під час збройної агресії рф в АС «ІРЦ» повинні бути передбачені засоби безперебійного живлення та резервного копіювання (архівування) інформації з баз даних із використанням спеціального програмного забезпечення.*

Ключові слова: *інклюзивна освіта, освітні інформаційні системи, інклюзивно-ресурсний центр, автоматизована система інклюзивно-ресурсних центрів, загрози інформаційній безпеці.*

JEL classification: I22, I28.

DOI: 10.32987/2617-8532-2022-4-17-30.

Україна обрала своє майбутнє в ЄС із набуттям незалежності в 1991 р. Ці наміри вкотре підтвердились у 2013–2014 рр., під час Революції гідності, й відтоді український народ невтомно продовжує боротися за свій вибір. Зараз триває повномасштабна збройна агресія російської федерації проти України. І однією з основних причин вторгнення є проєвропейський рух нашої держави. На сьогодні Україна вже здійснила кілька структурних реформ, щоб наблизитися до Копенгагенських критеріїв, та робитиме це й надалі.

Ключові завдання в процесі становлення української державності визначалися трансформаційними процесами орієнтації на повноцінну демократично-правову державу, становлення ефективної економіки, необхідність подолання відставання від світових тенденцій соціально-економічного розвитку. Варто підкреслити, що прискорення глобалізації та формування освічених постіндустріальних суспільств у Європейському Союзі, членом якого прагне стати Україна, безпосередньо пов'язане з якісними змінами в освітній сфері, зокрема в системному розвитку й підтримці суб'єктів освітньої діяльності.

Для наближення й гармонізації з передовими світовими стандартами соціально-економічного устрою Україна має враховувати основні глобальні тенденції в освітній сфері в частині становлення та вдосконалення навчального процесу закладів освіти. Варто наголосити, що освіта є одним із найважливіших факторів формування нової якості економіки й суспільства в цілому, а системне подолання економічних та інституційних проблем, додатково загострених воєнним станом, безпосередньо залежить від спрямованості й ефективності освітнього процесу. На окрему увагу наукової спільноти в контексті розвитку освіти заслуговує дослідження інформаційно-аналітичної підтримки управління інклюзивною освітою, яка, за замовчуванням, передбачає імплементацію принципів недискримінації, урахування багатоманітності людини, ефективного залучення та включення до освітнього процесу всіх його учасників [1].

ЄС в особі Європейської комісії, вищого органу виконавчої влади, на соціальному саміті в Гетеборзі виклав своє бачення європейського освітнього простору. Ця ініціатива підкреслила цінність високоякісної інклюзивної освіти з дитинства для закладення основ соціальної єдності, мобільності та справедливого суспільства [2].

У рекомендаціях Ради щодо загальних цінностей, інклюзивної освіти та європейського виміру зазначено, що інклюзивна і якісна освіта на всіх рівнях, а також європейський вимір викладання є найважливішими для створення й підтримки згуртованого європейського суспільства, передаючи спільні цінності, практикуючи інклюзивну освіту та навчаючи про Європу та її держави-члени [3].

Також варто зауважити, що помітних успіхів в інклюзивній освіті держави-члени ЄС досягли завдяки:

– створенню робочої групи зі сприяння загальним цінностям та інклюзивній освіті;

– ініціативам із залучення позитивних прикладів для сприяння соціальній інтеграції та запобігання

відчуженню й насильницькій радикалізації серед молоді;

– набору інструментів для роботи з молодими людьми, яким загрожує дискримінація в частині їхніх освітніх потреб та ін.

Серед сучасних вітчизняних науковців, чиї дослідження присвячено інклюзивній освіті, – С. Лондар, І. Гевко, Г. Кравченко, А. Колупаєва, О. Мартинчук, Н. Матвеєва, Г. Сіліна, О. Таранченко, І. Ярмощук [4–10]; серед зарубіжних – Дж. Деппелер, Е. Ервін, Т. Лореман, Д. Кугельмас, У. Шарма, Л. Фелпс, К. Хенлі-Максвелл, А. Шварц, Б. Хопкінс, Л. Штіфель, Г. Хорнбі [11–16]. Попри вагомий доробок науковців і практиків з окресленої проблематики, залишається актуальним питання вдосконалення інформаційного забезпечення функціонування системи інклюзивної освіти та забезпечення його стікості в кризових умовах.

Метою статті є дослідження сучасних шляхів удосконалення інформаційно-аналітичної підтримки управління інклюзивною освітою в кризових умовах з урахуванням досвіду ЄС.

Завдання дослідження та його наукова новизна полягають у розкритті критеріїв забезпечення захисту інформації від несанкціонованого доступу засобами криптозахисту, моніторингу системних журналів реєстрації роботи програмних і технічних засобів, аналізу порушень у роботі АС «ІРЦ»; упровадженні для потреб АС «ІРЦ» організаційних і технічних заходів із кіберзахисту, які вживаються для об'єктів критичної інформаційної інфраструктури; обґрунтуванні переліку дій для забезпечення доступності й відмовостійкості компонентів та інформаційних ресурсів АС «ІРЦ».

На сьогодні автоматизована система «Інклюзивно-ресурсний центр» (*далі* – АС «ІРЦ») працює відповідно до наказу Міністерства освіти і науки України «Про затвердження Положення про систему автоматизації роботи інклюзивно-ресурсних центрів» від 02.11.2020 № 1353 [17]. На АС «ІРЦ» покладено функції із забезпечення комплексної оцінки дітей з особливими освітніми потребами, надання їм необхідної підтримки тощо. У ДНУ «ІОА» забезпечується безперебійна робота мобільних додатків зазначеної системи на платформах IOS та Android у середовищах Play Market і App Store.

Захист інформації в АС «ІРЦ» забезпечується шляхом функціонування комплексної системи захисту інформації (*далі* – КСЗІ) з атестованою відповідністю вимогам технічного захисту інформації. КСЗІ АС «ІРЦ» забезпечує захист від порушень цілісності даних, різні види доступності (блокування) відкритої інформації та інформації з обмеженим доступом, вимогу щодо захисту якої встановлено законодавством України. Обробка й захист даних здійснюються в АС «ІРЦ» відповідно до вимог законодавства у сфері захисту інформації, що перебуває у власності держави [17].

В умовах воєнного стану важливо забезпечити продовження навчання осіб з особливими освітніми потребами (*далі* – осіб з ООП) за місцем їх тимчасового перебування, максимально можливе збереження кадрового потенціалу педагогічних працівників закладів освіти, які забезпечували навчання дітей з ООП,

та інклюзивно-ресурсних центрів (*далі* – ІРЦ).

У зв'язку з російською військовою агресією, бойовими діями на території України та виникненням обставин, що становлять загрозу життю й здоров'ю мирних громадян, рекомендується організовувати роботу ІРЦ залежно від конкретної ситуації на території їх розміщення.

З метою збереження кадрового потенціалу фахівців ІРЦ по всій території України місцевим управлінням (відділам) освіти рекомендується використовувати ресурс педагогічних працівників ІРЦ та допомагати (в межах своїх можливостей) у забезпеченні умов їх роботи, повідомляти заклади освіти про наявні людські ресурси, інформувати батьків осіб з ООП про можливість одержання кваліфікованої підтримки й допомоги [18].

Зважаючи на виклики, що наразі постали перед Україною, варто звернути увагу на сучасні ІТ-загрози. Зокрема, розглянемо та згрупуємо за типами загрози, які мають вплив на інформаційно-телекомунікаційні системи, а саме на АС «ІРЦ». Зокрема, під терміном «інформація, що обробляється або зберігається в АС "ІРЦ"», розуміється відкрита й конфіденційна інформація.

1. У межах конфіденційності інформації, що обробляється та зберігається в АС «ІРЦ», розрізняють отримання несанкціонованого доступу сторонніх осіб унаслідок:

– несанкціонованого фізичного доступу до обладнання;

– навмисного під'єднання до обладнання, помилок при налаштуванні комутаційного обладнання або апаратних збоїв;

– навмисного під'єднання до каналів зв'язку чи обладнання, а потім використання для несанкціонованого доступу до відомих уразливостей програмного забезпечення та системних технічних заходів;

– умисного під'єднання до каналів або пристроїв зв'язку з подальшим використанням для несанкціонованого доступу перехоплених атрибутів доступу авторизованих користувачів;

– фізичного доступу до носіїв інформації (змінних і пошкоджених носіїв; носіїв, які підлягають утилізації).

У частині порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) сторонніми особами виокремлюють загрози внаслідок:

– необережного поводження авторизованих користувачів з атрибутами доступу;

– ескалації прав доступу до ресурсів АС «ІРЦ» та виконання несанкціонованих дій від імені іншого користувача;

– порушення конфіденційності технологічної інформації (атрибутів доступу користувача системи) авторизованими користувачами системи з використанням відомих уразливостей програмного забезпечення й технічних засобів АС «ІРЦ»;

– фізичного доступу до носіїв інформації (змінних, пошкоджених, утилізаційних носіїв).

2. У межах визначення цілісності інформації, що обробляється та зберігається в АС «ІРЦ», розрізняють загрози внаслідок:

– апаратного чи програмного збою;

– отримання фізичного доступу до обладнання (навмисне або в результаті необережного поводження з облад-

нанням і системами, що забезпечують його роботу);

– навмисних дій авторизованого користувача будь-якого рівня в межах його прав;

– ненавмисних (помилкових) дій авторизованого користувача будь-якого рівня;

– ураження комп'ютерним вірусом.

У частині порушення цілісності технологічної інформації (конфігураційні файли) сторонніми особами або авторизованими користувачами із застосуванням відомих уразливостей програмно-технічних засобів АС «ІРЦ» чи перехоплених атрибутів доступу співробітників з адміністративними правами виокремлюють загрози з метою:

– приховування несанкціонованих дій у системі в межах реалізації інших загроз, спрямованих на порушення надійності або конфіденційності інформації;

– створення умов для подальшого несанкціонованого доступу до інших компонентів системи;

– ураження системи комп'ютерним вірусом.

3. У межах доступності інформації, що обробляється та зберігається в АС «ІРЦ», розрізняють загрози внаслідок:

– виходу з ладу комутаційного чи серверного обладнання або забезпечуючих елементів (найімовірнішим вважається вихід із ладу системи електроживлення);

– ураження системи комп'ютерним вірусом (перевантаження каналів зв'язку віддалених користувачів інтенсивним трафіком, створюваним вірусами-«хробаками» під час розповсюдження, вичерпання дискового простору чи процесорного часу на серверах, уражених певними типами вірусів, що призводить до неможливості обробки запитів та збоїв у роботі) [12; 19–21].

У наведеному переліку загрози розглядаються тільки із середнім і високим ефективним рівнем, що позначається як «високий» та повинен забезпечуватися потужностями щонайменше двох різних програмних чи програмно-технічних засобів або сукупністю організаційно-технічних заходів.

Ключовим припущенням у ході аналізу потенційних ризиків для АС «ІРЦ» є те, що працівники, які мають повний адміністративний доступ до компонентів системи та фізичний доступ до комутаційних і серверних пристроїв, не вважаються порушниками. Додатковими вважаються технічні заходи захисту від зловмисних дій співробітників із правами адміністратора. Основним засобом захисту від таких загроз є організаційна діяльність (кадрова політика, взаємоконтроль адміністраторів під час виконання важливих технологічних операцій).

У зв'язку з неможливістю одержання достатньо об'єктивних даних про ймовірність реалізації більшості з наведених загроз, таку ймовірність визначено експертним методом та, для окремих випадків, що є типовими для інформаційно-телекомунікаційних систем на зразок АС «ІРЦ», емпіричним шляхом, на підставі досвіду експлуатації подібних систем [14–16].

В АС «ІРЦ» функціонує КСЗІ, що забезпечує:

– розмежування доступу користувачів і програм користувачів до інформації;

– виявлення та реєстрацію спроб порушення розмежування доступу;

– автоматизовану ідентифікацію користувачів і експлуатаційного персоналу при зверненні до ресурсів АС «ІРЦ»;

– реєстрацію фактів порушення доступу;

– протоколювання дій користувачів, включаючи доступ із зовнішніх систем;

– заборону на несанкціоновану зміну конфігурації АС «ІРЦ»;

– виявлення, ідентифікацію та видалення комп'ютерних вірусів на серверах системи;

– захист бази даних, звітної, архівної інформації від несанкціонованого доступу й фізичного руйнування;

– захист інформації від спотворення та несанкціонованого використання при взаємодії структурних складових АС «ІРЦ» через канали зв'язку;

– захист цілісності даних від руйнувань за аварійних режимів і збоїв в електроживленні АС «ІРЦ» [22].

В АС «ІРЦ» також передбачено захист інформації від несанкціонованого доступу засобами криптозахисту, для чого забезпечено:

– шифрування з гарантованою стійкістю та імітозахистом інформації, яка передається через канали зв'язку між об'єктами автоматизації;

– криптографічне перетворення інформації, що передається через відкриті IP-мережі загального користування;

– авторизацію електронних документів засобами формування й перевірки кваліфікованого електронного підпису;

– керування та розподіл ключової й ідентифікуючої інформації;

– відповідність законодавству України в частині захисту інформації.

Варто також звернути увагу на постанову Кабінету Міністрів України «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» від 12.03.2022 № 263, яка містить окремі положення щодо інформаційно-телекомунікаційних систем, а саме:

1) розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України, та реєструвати доменні імена у домені gov.ua для такого розміщення;

2) створювати додаткові резервні копії державних інформаційних ресурсів та публічних електронних реєстрів з дотриманням установлених для таких ресурсів вимог щодо цілісності, конфіденційності та доступності;

3) зберігати резервні копії державних інформаційних ресурсів та публічних електронних реєстрів у зашифрованому вигляді, зокрема за межами України, на хмарних ресурсах та/або окремих фізичних носіях, та/або в ізольованому сегменті центрів обробки даних з дотриманням установлених для таких ресурсів вимог щодо цілісності, конфіденційності та доступності;

4) зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів [23–25].

Зокрема, перелік базових вимог із забезпечення кіберзахисту АС «ІРЦ»

може бути доповнено відповідно до технології обробки інформації, особливостей функціонування та програмно-апаратного складу, складу інформаційних ресурсів і компонентів, які підлягають захисту.

Пропонуємо впровадити та вдосконалити для потреб АС «ІРЦ» організаційні й технічні заходи з кіберзахисту, що вживаються для об'єктів критичної інформаційної інфраструктури (рис. 1).

У разі неможливості фізичного розділення зовнішньої мережі та АС «ІРЦ» на межі між зовнішніми мережами, іншими інформаційно-телекомунікаційними системами повинні бути встановлені засоби мережевого захисту (рис. 2).

Для забезпечення доступності й відмовостійкості компонентів та інформаційних ресурсів АС «ІРЦ» повинне здійснюватися:

– періодичне створення резервних копій інформаційних ресурсів, включаючи технологічну інформацію компонентів об'єкта та образів серверів, а також їх відновлення у випадку втрати або пошкодження;

– резервування критичних для функціонування об'єкта програмних і апаратних компонентів для забезпечення його сталого функціонування у випадку виходу з ладу одного із критичних компонентів (у разі використання віртуальних серверів необхідно забезпечити їх резервування);

– дублювання (кластеризація) критичних для функціонування програмних і апаратних компонентів об'єкта для забезпечення його сталого функціонування, зниження навантаження та підвищення продуктивності;

– використання джерел безперебійного живлення для критичних компонентів об'єкта;

– зв'язок з Інтернетом із використанням двох і більше каналів передачі даних, які надаються різними провайдерами [26].

Отже, для забезпечення збереження інформації за аварійних режимів під час збройної агресії рф в АС «ІРЦ» повинні бути передбачені засоби

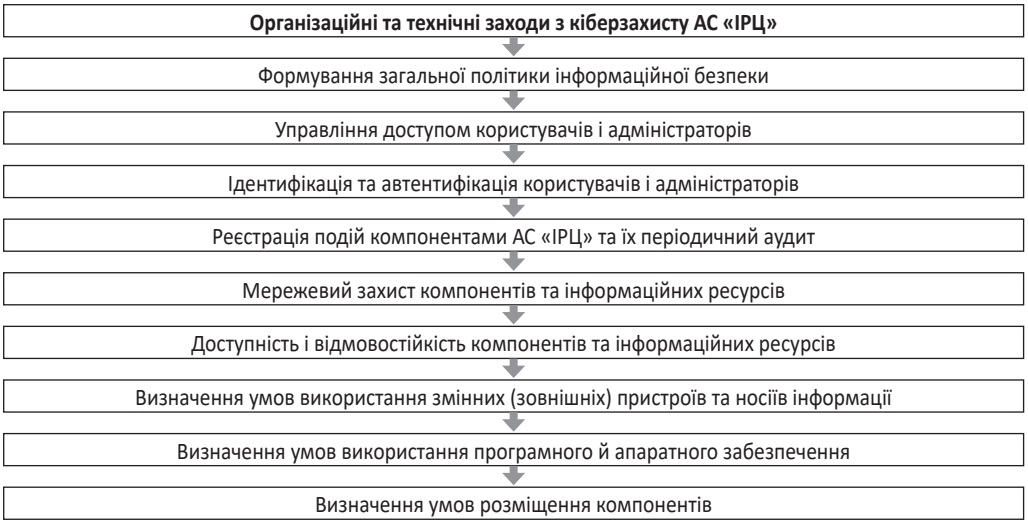

Рис. 1. **Організаційні та технічні заходи з кіберзахисту АС «ІРЦ»**

Побудовано авторами за: [26].

Рис. 2. **Засоби мережевого захисту АС «ІРЦ»**

Побудовано авторами за: [26].

безперебійного живлення та дублювання інформації. Обов'язковою умовою також має стати резервне копіювання (архівування) інформації з баз даних із використанням спеціального програмного забезпечення.

Контроль, збереження, відновлення даних повинні бути регламентовані, а зберігання резервних даних – здійснюватися в місцях, що не допускають їх пошкодження у випадку знищення основних даних АС «ІРЦ».

АС «ІРЦ» повинна забезпечувати відновлення даних у разі виходу з ладу апаратного комплексу, за аварійних режимів і збоїв в електроживленні. АС «ІРЦ» покликана реалізовувати (засобами системи управління базами даних, апаратними засобами серверного обладнання, прикладними засобами резервного копіювання) збереження інформації в разі відмови основного накопичувача. Для цього мають бути передбачені резервні пристрої й носії, що архівуватимуть інформацію.

Пропоновані локальні освітні реєстри, бази даних та копії державних реєстрів потрібно перемістити в безпечне місце/середовище на вільних територіях. Програмне забезпечення, що функціонує на робочих комп'ютерах освітян, може автоматично зберігати документи й дані на цих пристроях. У разі ризику потрапляння до рук ворога освітні персональні дані / програмне забезпечення мають бути заздалегідь видалені.

Необхідно забезпечити застосування з боку технічних адміністраторів, власників, операторів національних і локальних, державних та приватних освітніх інформаційних систем і освітніх інформаційних ре-

сурсів механізму превентивного відключення доступу для користувачів на окупованих територіях до «чутливої» інформації [27].

В оперативному режимі для АС «ІРЦ» було вжито заходів для забезпечення розміщення, розгортання й початку функціонування в хмарних системах (Amazon Web Services), що забезпечило, крім захисту програмно-апаратної частини системи від зловмисних дій країни-агресора, гнучкість, маштабованість та інтероперабельність [28].

Список використаних джерел

1. Інклюзивне навчання / М-во освіти і науки України. URL: https://mon.gov.ua/ua/tag/inklyuzivne-navchannya.

2. Council recommendation on common values, inclusive education and the European dimension of teaching. URL: https://education.ec.europa.eu/focus-topics/improving-quality/inclusive-education/common-values.

3. European Commission (2018). On promoting common values, inclusive education, and the European dimension of teaching (Council recommendation, May 22). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0607%2801%29.

4. *Гевко І. В.* Значення інноваційних технологій при здійсненні інклюзивної освіти. *Педагогічний альманах*. 2018. Вип. 37. С. 236–240. URL: http://dspace.tnpu.edu.ua/handle/123456789/13376.

5. *Колупаєва А. А., Таранченко О. М.* Інклюзивна освіта: від основ до практики : монографія. Київ : ТОВ «АТОПОЛ», 2016. 152 с. URL: https://lib.iitta.gov.ua/id/eprint/708170.

6. *Кравченко Г. Ю., Сіліна Г. О.* Інклюзивна освіта. Харків : Ранок, 2014. 144 с. URL: https://sf4b2e8052c76e462.jimcontent.com/download/version/1623755029/module/10272453385/name/%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0%20%D0%86%D0%BD%D0%BA%D0%BB%D1%8E%D0%B7%D0%B8%D0%B2%D0%BD%D0%B0%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%B0%20%D0%B2%20%D0%94%D0%9D%D0%97.pdf.

7. *Мартинчук О. В.* Інклюзивна освіта: освітологічний контекст. *Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського*. *Сер. : педагогічні науки*. 2016. № 3 (54). С. 146–150. URL: https://science.iea.gov.ua/wp-content/uploads/2021/07/7_Litvinchuk_Ko_213_2021_82_92.pdf.

8. *Лондар С. Л.* Міжнародний досвід розвитку сучасних освітніх інформаційних систем. *Освітня аналітика України*. 2019. № 1 (5). С. 5–19. URL: https://science.iea.gov.ua/wp-content/uploads/2019/05/1_Londar_15_2019_5_19-1.pdf.

9. *Матвеєва Н.* Інклюзивна освіта в Україні: соціально-педагогічний аспект. *Освітній простір України*. 2017. № 11. С. 180–187. URL: https://journals.pnu.edu.ua/index.php/esu/article/view/3080.

10. *Ярмощук І.* Інклюзивне навчання в системі освіти. *Шлях освіти*. 2009. № 2. С. 24–28. URL: http://www.irbis-nbuv.gov.ua/publ/REF-0000411380.

11. *Deppeler J., Loreman T., Sharma U.* Reconceptualising specialist support services in inclusive classrooms. *Australasian Journal of Special Education*. 2005. No. 29 (2). P. 117-127. URL: https://www.researchgate.net/publication/236029286_Reconceptualising_specialist_support_services_in_inclusive_classrooms.

12. *Ервін Е., Кугельмас Д.* Підготовка вчителів і вихователів до роботи в інклюзивних класах та групах. Київ : ВФ «Крок за кроком», 2000. 203 с.

13. *Loreman T. A.* Canadian collaboration on inclusive education: reflections on a six-year partnership. URL: http://revistas.unilasalle.edu.br/index.php/desenvolve/article/view/1884.

14. *Phelps L. A., Hanley-Maxwell C. H.* School to work transitions for youth with disabilities: a review of outcomes and practices. *Review of Educational Research*. 1997. Vol. 67 (2). P. 197-226. URL: https://journals.sagepub.com/doi/10.3102/00346543067002197.

15. *Schwartz A. E.; Hopkins B. G.; Stiefel L.* The Effects of Special Education on the Academic Performance of Students with Learning Disabilities. *Journal of Policy Analysis and Management*. 2021. Vol. 40. P. 480-520. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/pam.22282.

16. *Hornby G.* Inclusive special education: Development of a new theory for the education of children with special educational needs and disabilities. *The British Journal of Special Education*. 2015. Vol. 42(3). P. 234-256. URL: https://nasenjournals.onlinelibrary.wiley.com/doi/abs/10.1111/1467-8578.12101.

17. Про затвердження Положення про систему автоматизації роботи інклюзивно-ресурсних центрів : наказ Міністерства освіти і науки України від 02.11.2020 № 1353. URL: https://zakon.rada.gov.ua/laws/show/z0024-21#Text.

18. Конвенція про права осіб з інвалідністю (Конвенція про права інвалідів) : ООН; Конвенція від 13.12.2006. URL: https://zakon.rada.gov.ua/laws/show/995_g71#Text.

19. Про затвердження Порядку організації інклюзивного навчання в закладах дошкільної освіти : постанова Кабінету Міністрів України від 10.04.2019 № 530. URL: https://zakon.rada.gov.ua/laws/show/530-2019-%D0%BF#Text.

20. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації : наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93. URL: https://zakon.rada.gov.ua/laws/show/z0820-07#Text.

21. Перелік документів системи технічного захисту інформації (НД ТЗІ). URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi.

22. *Литвинчук А. О., Кир'янов А. В., Гайдук І. С.* Методичні підходи до розширення функціоналу інформаційної системи АС «ІРЦ» та оптимізації е-збору даних форми звітності в сегменті інклюзивної освіти. *Освітня аналітика України*. 2021. № 3 (14). С. 33–41. URL: https://science.iea.gov.ua/wp-content/uploads/2022/01/3_Litvinchuk_Kiryanov_Gayduk_314_2021_33_41.pdf.

23. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану : постанова Кабінету Міністрів України від 12.03.2022 № 263. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263.

24. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

25. Захист інформації / Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/statics/zakhist-informaciyi.

26. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

27. Офіційний сайт інформаційно-телекомунікаційної системи «Державна інформаційна система освіти» (ІТС «ДІСО»). URL: https://diso.gov.ua.

28. Організація функціонування АС «ІРЦ» для забезпечення потреб освітнього процесу осіб з ООП в умовах збройної агресії рф. URL: https://iea.gov.ua/wp-content/uploads/2022/08/3_az_litvinchuk_-organizacziya-funkczionuvannya-as-ircz-v-umovah-zbrojno%D1%97-agresi%D1%97-rf.pdf.

Andrii Lytvynchuk
Ph. D. (Economics), SSI «Institute of Educational Analytics», Kyiv, Ukraine, a.litvinchuk@iea.gov.ua
ORCID ID: https://orcid.org/0000-0002-7523-558X

Andrii Kyrianov
SSI «Institute of Educational Analytics», Kyiv, Ukraine, a.kiryanoff@iea.gov.ua
ORCID ID: https://orcid.org/0000-0003-0452-7689

Julia Irynevich
Ph. D. (Economics), SSI «Institute of Educational Analytics», Kyiv, Ukraine, nnaru1@ukr.net
ORCID ID: https://orcid.org/0000-0003-1755-5240

Ivan Gaiduk
SSI «Institute of Educational Analytics», Kyiv, Ukraine, gaiduk94ivan@gmail.com
ORCID ID: https://orcid.org/0000-0003-3144-1469

INFORMATION AND ANALYTICAL SUPPORT FOR THE MANAGEMENT OF INCLUSIVE EDUCATION UNDER MARTIAL CONDITIONS AND TAKING INTO ACCOUNT THE EU EXPERIENCE

Abstract. *The purpose of the article is to study modern ways of improving information and analytical support for the management of inclusive education in crisis conditions, taking into account the experience of the EU. The list of components that compose the central software and technical complex of the automated system of inclusive resource centers (AS "IRC") was described. The types of modern threats to the information security of the AS "IRC", which influence the information processed and stored in this system, as well as technological information, were analyzed. Criteria for providing information protection from unauthorized access through crypto protection, monitoring of system logs of software and technical means, and analysis of violations in the functioning of the AS "IRC" were described. Implementation of organizational and technical measures on cyber protection, used for objects of critical information infrastructure, for AS "IRC" needs was proposed. The list of actions to ensure the availability and fault tolerance of components and information resources of the AS "IRC" was shown. It was concluded that for the storage of information in emergency modes of operation during the armed aggression of the russian federation, the means of uninterruptible power supply and backup (archiving) of information from databases using special software should be provided in the AS "IRC". Data monitoring and recovery should be managed and backup data must be stored in locations that do not allow them to be damaged in the event of the destruction of the AS "IRC" main components. The proposed local education registries, databases and copies of state registries should be moved to a safe place/environment in free territories. Educational personal data/software at risk of falling into enemy hands should be deleted in*

advance. It is necessary to ensure the application of the mechanism of preventive disconnection by technical administrators, owners, operators of national and local, public and private educational information systems and educational information resources for users in the occupied territories to "sensitive" information.

Keywords: *inclusive education, educational information systems, inclusive resource center, automated system of inclusive resource centers, threats to information security.*

References

1. Ministry of Education and Science of Ukraine. (n. d.). *Inclusive education.* Retrieved from https://mon.gov.ua/ua/tag/inklyuzivne-navchannya [in Ukrainian].

2. European Commission. (n. d.). *Council recommendation on common values, inclusive education and the European dimension of teaching*. Retrieved from https://education.ec.europa.eu/focus-topics/improving-quality/inclusive-education/common-values.

3. European Commission. (2018). *On promoting common values, inclusive education, and the European dimension of teaching* (Council recommendation, May 22). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0607%2801%29.

4. Hevko, I. V. (2018). The importance of innovative technologies in the implementation of inclusive education. *Pedagogical almanac*, *37,* 236–240. Retrieved from http://dspace.tnpu.edu.ua/handle/123456789/13376 [in Ukrainian].

5. Kolupaieva, A. A., & Taranchenko, O. M. (2016). *Inclusive education: from basics to practice*. Kyiv: TOV "ATOPOL". Retrieved from https://lib.iitta.gov.ua/id/eprint/708170 [in Ukrainian].

6. Kravchenko, H. Yu., & Silina, H. O. (2014). *Inclusive education*. Kharkiv: Ranok. Retrieved from https://sf4b2e8052c76e462.jimcontent.com/download/version/1623755029/module/10272453385/name/%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0%20%D0%86%D0%BD%D0%BA%D0%BB%D1%8E%D0%B7%D0%B8%D0%B2%D0%BD%D0%B0%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%B0%20%D0%B2%20%D0%94%D0%9D%D0%97.pdf [in Ukrainian].

7. Martynchuk, O. V. (2016). Inclusive education: educational context. *Scientific Bulletin of Mykolaiv National University named after V. O. Sukhomlynskyi*. *Pedagogical sciences*, *3(54),* 146–150. Retrieved from https://science.iea.gov.ua/wp-content/uploads/2021/07/7_Litvinchuk_Ko_213_2021_82_92.pdf [in Ukrainian].

8. Londar, S. L. (2019). International experience in the development of modern educational information systems. *Educational analytics of Ukraine, 1(5),* 5–19. Retrieved from https://science.iea.gov.ua/wp-content/uploads/2019/05/1_Londar_15_2019_5_19-1.pdf [in Ukrainian].

9. Matveieva, N. (2017). Inclusive education in Ukraine: socio-pedagogical aspect. *Educational space of Ukraine, 11,* 180–187. Retrieved from https://journals.pnu.edu.ua/index.php/esu/article/view/3080 [in Ukrainian].

10. Yarmoshchuk, I. (2009). Inclusive learning in the education system. *The way of education, 2,* 24–28. Retrieved from http://www.irbis-nbuv.gov.ua/publ/REF-0000411380 [in Ukrainian].

11. Deppeler, J., Loreman, T., & Sharma, U. (2005). Reconceptualising specialist support services in inclusive classrooms. *Australasian Journal of Special Education, 29(2),* 117-127. Retrieved from https://www.researchgate.net/publication/236029286_Reconceptualising_specialist_support_services_in_inclusive_classrooms.

12. Ervin, E., & Kuhelmas, D. (2000). *Training of teachers and educators to work in inclusive classes and groups*. Kyiv: VF "Krok za krokom" [in Ukrainian].

13. Loreman, T. A. (n. d.). *Canadian collaboration on inclusive education: reflections on a six-year partnership*. Retrieved from http://revistas.unilasalle.edu.br/index.php/desenvolve/article/view/1884.

14. Phelps, L. A., & Hanley-Maxwell, C. H. (1997). School to work transitions for youth with disabilities: A review of outcomes and practices. *Review of Educational Research, 67(2),* 197-226. Retrieved from https://journals.sagepub.com/doi/10.3102/00346543067002197.

15. Schwartz, A. E., Hopkins, B. G., & Stiefel, L. (2021). The Effects of Special Education on the Academic Performance of Students with Learning Disabilities. *Journal of Policy Analysis and Management, 40,* 480-520. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1002/pam.22282.

16. Hornby, G. (2015). Inclusive special education: Development of a new theory for the education of children with special educational needs and disabilities. *The British Journal of Special Education, 42(3),* 234-256. Retrieved from https://nasenjournals.onlinelibrary.wiley.com/doi/abs/10.1111/1467-8578.12101.

17. Ministry of Education and Science of Ukraine. (2020). *On the approval of the Regulation on the system of automation of work of inclusive resource centers* (Order No. 1353, November 2). Retrieved from https://zakon.rada.gov.ua/laws/show/z0024-21#Text [in Ukrainian].

18. United Nations. (2006). *Convention on the Rights of Persons with Disabilities (CRPD).* Retrieved from https://zakon.rada.gov.ua/laws/show/995_g71#Text [in Ukrainian].

19. Cabinet of Ministers of Ukraine. (2019). *About the statement of the Order of preparation of organizing inclusive education in preschool education institutions* (Decree No. 530, April 10). Retrieved from https://zakon.rada.gov.ua/laws/show/530-2019-%D0%BF#Text [in Ukrainian].

20. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2007). *About the statement of Regulations on state expertise in the field of technical information protection* (Decree No. 93, May 16). Retrieved from https://zakon.rada.gov.ua/laws/show/z0820-07#Text [in Ukrainian].

21. State Service of Special Communications and Information Protection of Ukraine. (2021). *The list of documents of the technical information protection system (ND TPI).* Retrieved from https://cip.gov.ua/ua/news/perelik-dokumentiv-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi [in Ukrainian].

22. Lytvynchuk, A. O., Kyrianov, A. V., & Gaiduk, I. S. (2021). Methodical approaches to custom programming of the information system of AS "IRC" and optimization of e-collection of data reporting forms in the inclusive education segment. *Educational analytics of Ukraine, 3(14),* 33–41. Retrieved from https://science.iea.gov.ua/wp-content/uploads/2022/01/3_Litvinchuk_Kiryanov_Gayduk_314_2021_33_41.pdf [in Ukrainian].

23. Cabinet of Ministers of Ukraine. (2022). *Some issues of ensuring the functioning of information and communication systems, electronic communication systems, public electronic registers in the conditions of martial law* (Resolution No. 263, March 12). Retrieved from https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263 [in Ukrainian].

24. Verkhovna Rada of Ukraine. (2006). *On the State Service of Special Communications and Information Protection of Ukraine* (Act No. 3475-IV, February 23). Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text [in Ukrainian].

25. State Service of Special Communications and Information Protection of Ukraine. (n. d.). *Protection of information*. Retrieved from https://cip.gov.ua/ua/statics/zakhist-informaciyi [in Ukrainian].

26. Cabinet of Ministers of Ukraine. (2019). *On the approval of the General requirements for cyber protection of critical infrastructure objects* (Decree No. 518, June 19). Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [in Ukrainian].

27. Information and telecommunication system "State Information System of Education" (ITS "DISO"). (n. d.). Retrieved from https://diso.gov.ua [in Ukrainian].

28. SSI "Institute of Educational Analytics". (2022). *The organization of the operation of the AS "IRC" to ensure the needs of the educational process of persons with special educational needs in the conditions of armed aggression of the russian federation*. Retrieved from https://iea.gov.ua/wp-content/uploads/2022/08/3_az_litvinchuk_-organizacziya-funkczionuvannya-as-ircz-v-umovah-zbrojno%D1%97-agresi%D1%97-rf.pdf [in Ukrainian].