DOI: https://doi.org/10.32782/2524-0072/2024-60-24

УДК 378:004

КІБЕРБЕЗПЕКА ЯК ФАКТОР ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

CYBER SECURITY AS A FACTOR OF THE EFFICIENCY OF THE FUNCTIONING OF HIGHER EDUCATION'S INSTITUTIONS

Савченко Володимир
доктор економічних наук, професор,
Уманський державний педагогічний університет імені Павла Тичини
ORCID: https://orcid.org/0000-0001-7637-2124

Маклюк Олег Володимирович
старший викладач,
Північноукраїнський інститут імені Героїв Крут
Приватного акціонерного товариства «Вищий навчальний заклад
«Міжрегіональна Академія управління персоналом»
ORCID: https://orcid.org/0000-0002-7429-692X

Savchenko Volodymyr
PavloTychynaUman State Pedagogical University

Makliuk Oleh
North Ukrainian Institute named after Heroes of Kruty
PJSC Private Joint-Stock Company «Higher education institution
«Interregional Academy of Personnel Management»

У статті досліджені проблеми кібербезпеки у світі і у нашій країні, вплив кіберзлочинності на роботу закладів вищої освіти і шляхи попередження та подолання кібератак. Обґрунтовано, що використання комп'ютерних технологій разом з перевагами несе певні загрози відносно складності захисту даних. З'ясовано, що на сьогоднішній день світові тенденції протистояння кіберзагрозам поступаються нападникам, що призводить до проведення останніми агресивних і успішних кібератак. Доведено, що атаки на мережі навчання останній час значно посилилися. Запропоновані організаційні заходи відносно вирішення проблем кібербезпеки. На основі дослідженого матеріалу робиться висновок, що від рівня підготовленості, компетентності і відповідальності учасників залежить ефективність протидії кібератакам і, як наслідок, успішне та стабільне функціонування закладів вищої освіти України.

Ключові слова: кібербезпека, кіберзлочинність, заклади вищої освіти, комп'ютерні технології, кіберзагрози, деструктивні процеси, мережі навчання, навчальний процес.

The article examines the problems of cyber security in the countries of the world and specifically in our country, the impact of cybercrime on the work of higher education institutions and ways to prevent and overcome cyber attacks. It is substantiated that the use of computer technologies together with numerous advantages regarding the availability and efficiency of obtaining information carries certain threats regarding the complexity of data protection of individuals and legal entities, the state as a whole. It has been found that today the global trends in countering cyber threats are inferior to the attackers, which leads to the latter conducting aggressive and successful cyber attacks. It has been established that a similar situation fully applies to Ukraine. The main problems of the state, regional and local levels are highlighted: insufficient awareness and responsibility of users; unclear determination of priorities; lack of specificity of planned activities; lack of a development program for the main subjects of the national cyber security system; limited budget funding; weakness of public-private partnership; unsystematic nature of e-learning. It has been proven that an important stage in the strengthening of cyber security was the initiation of training in the specialty "cyber security" by domestic institutions of higher education. It is shown that the war intensified the destructive processes that began as a result of the COVID-19

pandemic and fully relate to institutions of higher education. It has been proven that attacks on learning networks have increased significantly recently. Proposed organizational measures for solving cyber security problems: training and informing students and teachers; formation of students' critical thinking when using the Internet. It was determined that the special attention of cybercrime to the field of education is explained by a significant array of personal data of participants in the educational process. The classification of cyber threats in the field of higher education has been carried out. Based on the researched material, it is concluded that the effectiveness of combating cyberattacks and, as a result, the successful and stable functioning of higher education institutions of Ukraine depends on the level of preparedness, competence and responsibility of the participants.

Keywords: cyber security, cyber crime, higher education institutions, computer technologies, cyber threats, destructive processes, learning networks, educational process.

Постановка проблеми і її зв'язок з важливими науковими та практичними завданнями. Кібератаки на всі ланки народногосподарського комплексу країни і особисте життя її громадян посилюються і урізноманітнюються. Особливо небезпечними в останній час стали активні дії кіберзлочинців, пов'язані з війною росії, проти закладів вищої освіти щодо викладачів, студентів, технічних спеціалістів, інфраструктури навчальних закладів. Це пояснюється значним масивом персональних даних учасників навчального процесу, а також тим, що навчальні заклади проводять сучасні дослідження, володіють інноваціями та інтелектуальною власністю. Завдання злочинців полегшуються через відкритість та вільний обмін інформацією під час співпраці. Зазначене ставить перед органами кібербезпеки завдання теоретичного обґрунтування шляхів захисту кіберпростору та практичної реалізації запланованих заходів.

Аналіз останніх досліджень, у яких започатковано вирішення проблеми. Проблеми, пов'язані з кібербезпекою в умовах війни, стали предметом дослідження вітчизняних науковців. І. Білоус, Т. Вдовичин, І. Гальона, О. Захарова, М. Кириченко, У. Когут, О. Кричківська, Н. Муранова, О. Сікора, З. Шацька, І. Шемелинець аналізують певні проблеми кібербезпеки освітнього процесу в умовах воєнного часу. Проте, виходячи з важливості, дослідження потребують подальших теоретичних напрацювань і їх практичної реалізації.

Цілі статті. Головною метою дослідження є вивчення складових кібербезпеки в Україні, досвіду провідних країн світу, особливостей кібератак на всі ланки вищої освіти, надання пропозицій щодо заходів боротьби з кіберзлочинцями.

Методологія та методи дослідження. При написанні статті були використані наукові та спеціальні методи дослідження, зокрема аналіз і синтез, узагальнення, статистичний аналіз, політичний та геополітичний методи.

Викладення основного матеріалу дослідження. Використання комп'ютерних технологій в останні роки і десятиріччя різко активізувалося практично в усіх країнах світу, охопило всі сфери діяльності та особисте життя людей. Разом з чисельними перевагами подібної ситуації доступність і оперативність отримання інформації несе в собі певні загрози щодо складності захисту даних як особи, так і фірм, органів влади, суспільства в цілому.

Щоб зберегти інформацію від небажаного втручання, здійснюються заходи з кібербезпеки, під якими розуміються комплексні дії технологічного, економічного, організаційного, правового і юридичного характеру, покликані цілеспрямовано проводитися з метою виявлення і ліквідації загроз законним інтересам держави, юридичних та фізичних осіб, приватного життя усіх верств населення [1, с. 12].

На даний час світові тенденції щодо протистояння кіберзагрозам на випередження по основних своїх складових поступаються у підготовці операційних можливостей політично та економічно мотивованим нападникам, що призводить до їх успішних кібератак. Це стосується і ситуації в Україні.

За кібербезпеку в нашій державі відповідає Міністерство цифрової інформації, створене відповідно до Постанови Кабінету Міністрів України від 02 вересня 2019 року [2], на яке, серед інших, були покладені завдання формування державної політики щодо кіберзахисту, протидії розвідкам, функціонування системи зв'язку тощо.

На сьогодні головні проблеми, які стоять перед вказаним вище міністерством і всіма задіяними структурами: недостатня визначеність пріоритетів; неконкретність запланованих заходів; відсутність програми розвитку основних суб'єктів національної системи кібербезпеки; обмеженість інституційного,

а особливо бюджетного, забезпечення; відсутня модель державно-приватного партнерства; несистемність кібернавчання [3; 4].

Водночас розвиток міжнародного співробітництва з питань кібербезпеки, поглиблення співпраці з країнами Європейського Союзу і Північноатлантичного пакту покращують наші позиції у боротьбі з кіберзлочинністю, поліпшують ситуацію у кіберпросторі.

Важливим етапом у подальшому зміцненні кібербезпеки та її кадровому забезпеченні стало започаткування вітчизняними закладами вищої освіти навчання зі спеціальності 125 «Кібербезпека». При цьому кількість студентів та змістова градація у цьому напрямку щорічно збільшуються. Для прикладу надамо дані по м. Києву за 2018–2022 роки (рисунок 1; таблиця 1).

Наведені дані засвідчують, що з 2018 року протягом останніх п'яти років кількість університетів даного профілю поступово зростає. До 2022 року зростала і кількість поданих заяв за спеціальністю «Кібербезпека». Військова агресія росії істотно зменшила чисельність як загальної кількості поданих заяв, так і бажаючих вчитися за цією спеціальністю. Причини загальновідомі: військові дії росії і, як наслідок, масовий виїзд школярів випускних класів за кордон; ситуація з молоддю на тимчасово окупованих територіях; служба молодих людей у збройних силах України, де вони дають відсіч ворогу, та інше.

Проте наявність вибору значної кількості програм у межах вказаної спеціальності, відкриття нових кафедр в університетах засвідчують подальші перспективи навчального процесу та його інноваційну спрямованість. До того ж випускники цих та інших навчальних закладів мають високу репутацію за кордоном, запрошуються і ефективно працюють там у престижних IT-компаніях [6, с. 175–185].

Забезпечення кібербезпеки потребує комплексного підходу та скоординованих дій на державному, регіональному і особистісному рівнях, а також міжнародного сприяння як відповіді на агресію у кібепросторі, особливо пов'язану з російськими військовими потугами [7; 8].

Доцільно назвати основні ознаки кібератак: зовнішнє проявлення; специфіка порушення базових характеристик; інструменти; дистанційність; автоматизація; передбачуваний кінцевий результат; міра складності.

Запобіжними заходами мають стати: обізнаність співробітників; розроблення та періодичне коригування плану боротьби; оцінювання ступеню ризику та вразливості; аналіз змін у середовищі; створення груп експертів і сприяння їхній праці [9].

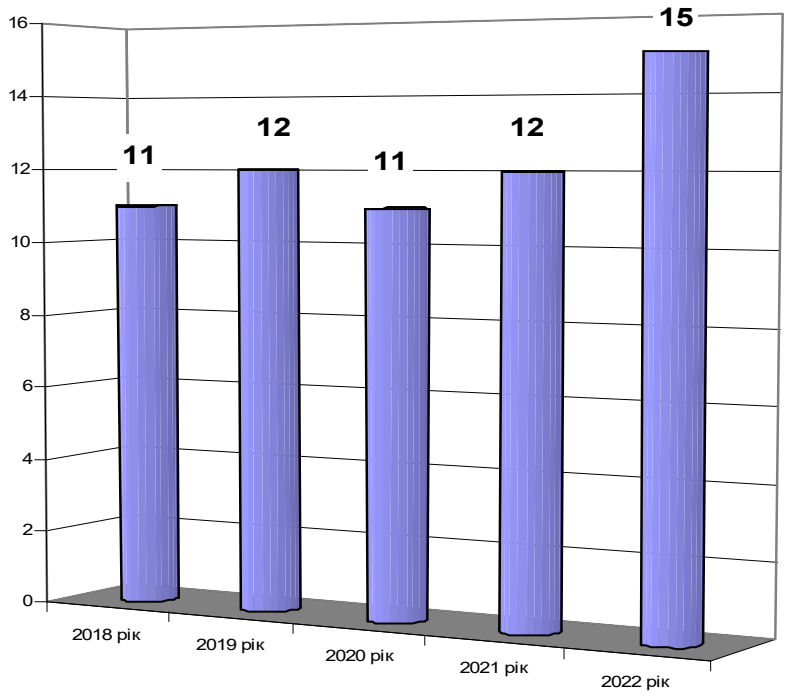

Рис. 1. Кількість закладів вищої освіти (м. Київ) із пропозиціями щодо спеціальності «Кібербезпека»

Джерело: [5]

Таблиця 1

Показники вступної кампанії за спеціальністю «Кібербезпека» (за даними закладів вищої освіти м. Києва) у 2018–2022 роках

Назва університету	Кількість поданих заяв				
	2018	2019	2020	2021	2022
Державний вищий навчальний заклад «Київський національний економічний університет імені Вадима Гетьмана»	417	453	529	1083	521
Державний університет телекомунікацій	762	912	904	1706	934
Київський національний торговельно-економічний університет	288	468	794	1108	502
Київський національний університет будівництва і архітектури	259	253	338	638	289
Київський національний університет імені Тараса Шевченка	703	856	751	1376	820
Київський університет імені Бориса Грінченка	245	347	399	689	361
Маріупольський державний університет	83	88	100	134	33
Національний авіаційний університет	1665	1370	1529	3885	2133
Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського»	1655	1787	1864	2856	1628
Національний університет біоресурсів і природокористування України	-	278	343	604	338
Приватний вищий навчальний заклад «Європейський університет»	49	42	113	290	227

Джерело: [5]

Темпи кібератак проти нашої держави постійно посилюються. Спершу окупанти найбільше атакували уряд та державні органи на місцевому рівні, сектори безпеки і оборони, фінансові структури, енергетичні об'єкти.

З часом все більше загроз виникає для секторів послуг населенню, інформаційних ресурсів та закладів вищої освіти і їх контингенту (викладачів, технічних працівників, студентів) [10, с. 3–4].

Розглянемо світовий досвід боротьби з кіберзлочинністю. В провідних країнах вважають за головне розробку інформаційних систем і методів, націлених на кібербезпечне середовище. В них впроваджуються і постійно вдосконалюються національні стратегії, які включають в себе пріоритети і довгострокові завдання для державних органів та їх бюджетне фінансування.

У липні 2009 року Франція створила агентство мережевої та інформаційної безпеки, основними напрямками якого визначено: боротьбу з кіберзлочинністю; промислові питання; кіберзахист у рамках Спільної політики і оборони ЄС; міжнародна політика у кібепросторі.

В Японії Рада з політики інформаційної безпеки у 2013 році прийняла Стратегію кібербезпеки, де передбачені взаємодія з іншими державами; створення ефективних відповідей на нові ризики; забезпечення обміну інформацією з урахуванням її безпечності.

В Республіці Корея була створена школа з вивчення кібервійн для збільшення спеціалістів з безпеки. Визначені перспективні напрямки захисту кіберпростору: профілактика вторгнень; подолання стійких загроз; шифрування для доступу до мережі.

Великобританія особливо прискіпливо зберігає свої кіберсекрети. Розроблена детальна система підбору кадрів з кібербезпеки, коли в конкурсі можуть брати участь тільки фахівці з прикладних технологій і математики [11]. В роботі держави та її громадян використовуються власні одиниці виміру в милях і ярдах, специфічна конструкція розеток та інші питання життєзабезпечення, що викликає зацікавленість і повагу [13–15, с. 6–11].

Війна посилює деструктивні процеси в економіці і взагалі в житті країни, що розпочалися в результаті пандемії COVID-19. Вони стосуються інфляції, збоїв у постачанні та енергетичній безпеці, захоплення територій ворожою державою. В повній мірі зазначене відноситься і до закладів вищої освіти. Так, з початку бойових дій на Донбасі було евакуйовано 18 вищих навчальних закладів, які в значній мірі втратили своїх викладачів та сту-

дентів, інфраструктуру, напрацьовані зв'язки, матеріально-технічну базу та інше. 43 заклади вищої освіти потрапили під обстріли, п'ять з них повністю зруйновано [16].

Згідно зі звітом, затвердженим Міжнародною науковою радою, щодо ситуації в Україні надаються рекомендації в таких напрямках: середньо- і довгострокова підтримка її наукової системи; передбачуваність; людяність; відкритість та міжнародна солідарність.

Військова агресія росії і пов'язані з нею кіберзагрози в усіх сферах життя, включаючи освітню, призвела до нагальної необхідності переорієнтації в підготовці кадрів, реформування та подолання недоліків в інституційному, освітньому, матеріало-технічному, законодавчо-нормативному забезпеченні [19, с. 142–144].

Організація освітніми закладами у 2020–2021 роках дистанційного навчання студентів допомогла адаптуватися до умов воєнного стану. Проте з'явилися практично нездоланні перешкоди щодо використання такого навчання на підконтрольних ворогу територіях та у місцях проведення бойових дій через неможливість використання мережі Інтернет. Посилилися і кібератаки на навчальні мережі.

Розроблена у 2022 році «Стратегія розвитку вищої освіти в Україні на 2022–2032 роки» [18], визначила основні пріоритети та характеристики, шляхи зменшення наслідків російської агресії. Складовою стратегії є і забезпечення кібербезпеки закладів вищої освіти [19].

Проблема впровадження інформаційно-комунікаційних технологій в освіті набуває особливої гостроти якраз через кібератаки у цій сфері. Так, на Міжнародних форумах в Давосі у 2018–2019 роках акцентувалася особлива увага на кібербезпеці освітніх процесів при їх повній інформатизації [20, с. 191].

Законом України «Про основні засади забезпечення кібербезпеки» [4] кібербезпека (в тому числі освітнього процесу – автори) визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України [4].

Число небезпек від відкритого кіберпростору весь час зростає. Найбільш активні приховані загрози: кіберзлочинність, вірусна небезпека, розголошення приватної інформації, платні послуги.

У широкому розумінні цілями впливу, крім об'єктів критичної інфраструктури, виступають: освіта і професійна підготовка, засоби масової інформації, соціальні мережі, бази даних, персональні дані, фінансова звітність, підручники.

Організаційні заходи щодо вирішення проблем кібербезпеки: навчання; інформування. Необхідно враховувати, що хакерські атаки в останній час переорієнтовуються з ураження техніки на людину. Тому основним засобом захисту є навчання студентів, педагогів та організаторів навчального процесу. Вони мають бути попереджені про недопустимість розкриття персональної та конфіденційної інформації, навчені способам запобігання витоку даних. Всі повинні бути забезпечені інструкцією на які теми дозволяється спілкуватися із сторонніми особами, яку інформацію можна надавати.

Викладачам вищої освіти необхідно не тільки вміти надавати відповідну інформацію, а і володіти педагогічними технологіями формування таких навиків у студентів.

При вивченні методики викладання навчальних дисциплін важливим є формування критичного мислення студентів при використанні можливостей мережі Інтернет.

Ефективним засобом формування в учасників освітнього процесу відповідної поведінки при користуванні мережею Інтернет є проведення спеціальних тренінгів з критичного оцінювання джерел і достовірності даних на їх сторінках. При цьому важливе тренування стійкості користувачів до дії кіберзагроз [21, с. 313–325].

Освітній процес найбільше страждає від шкідливого програмного забезпечення. При цьому під дію хакерів потрапляють всі його учасники – студенти, аспіранти, професорсько-викладацький склад, партнери і працівники філій [22].

Особлива увага кіберзлочинності до галузі освіти пояснюється значним масивом персональних даних учасників навчального процесу. До того ж ряд навчальних закладів проводять сучасні дослідження, володіють інноваціями та інтелектуальною власністю, що також є об'єктом пильної уваги зловмисників, злочинні завдання яких полегшуються в силу академічної відкритості установ та вільного обміну інформацією під час творчої співпраці.

Сектор вищої освіти потребує втручання технічних спеціалістів з кіберзахисту, яких не завжди може дозволити собі конкретний навчальний заклад, маючи проблеми з бюджетними фінансуванням.

Вільний потік робочої сили, щорічна ротація студентів, наявність численних комп'ютерних лабораторій, перехід до віддаленої роботи, електронного навчання та онлайн-викладання роблять дані всередині мереж набагато більш відкритими, а в ряді випадків незахищені пристрої стають більш вразливими для атак [23, с. 698–700].

Не всі заклади вищої освіти навіть після злому їх систем змінюють свою стратегію щодо кібербезпеки [24].

Наведемо класифікацію кіберзагроз у секторі вищої освіти.

Коротко охарактеризуємо деякі з кіберзагроз:

1. Людський фактор або помилки в силу необізнаності та неврахування вимог кібербезпеки. Ця загроза є найбільш типовою, при кібератаках її використовують найчастіше.
2. Крадіжка персональних даних (імена, адреси, методичні показники тощо).
3. Програми-вимагачі (зловмисне програмне забезпечення) – пристрої заражаються за допомогою вірусу або замаскованого вкладення.
4. Фінансова вигода – навчання оплачується здебільшого через онлайн-портали і в разі недостатнього захисту перехоплюється кіберзлочинцями.
5. Шпигунство – поширене, якщо заклад вищої освіти є центром досліджень і володіє унікальною інтелектуальною власністю.
6. Фішинг – найбільш популярний під час віддаленого навчання та роботи в домашніх умовах [25, с. 76–81].

В сучасній ситуації освіта у сфері кібербезпеки тісно переплетена з цифровими технологіями. У багатьох викладачів є свої інструменти, які вони використовують в процесі навчання. При цьому цифрові інструменти постійно оновлюються. До них додаються нові функції, розширюється сфера застосування. Сучасна наука ставить підвищені вимоги до кібервикладачів (кібертренерів), що мають вільно володіти сучасними цифровими технологіями та використовувати їх у своїй викладацькій діяльності [21, с. 93–106; 27, с. 64].

Від рівня підготовленості, компетентності і відповідальності учасників процесу навчання залежить і кібербезпека вищих військових навчальних закладів, для яких вона особливо важлива. Зупинимось на окремих її складових в частині організаційно-правових та інженерно-технічних заходів, які мають бути відображені у інструкціях, правилах та рекомендаціях: план заходів користувачів інформаційного простору на випадок кібератаки; звітність у випадку небезпечної ситуації; модель кіберзахисту; програмне забезпечення; порядок надання доступу; порядок дотримання вимог з кібербезпеки; юридична відповідальність за порушення правил.

Фахівці з кіберзахисту навчальних закладів даного профілю повинні бути добре обізнаними з правилами та інструкціями, ґрунтовно розбиратися в інженерно-технічних питаннях, юридично обізнані із основними видами кіберзлочинності та методами їх пошуку і знешкодження [28, с. 61–62].

Висновки. На сьогодні світові тенденції щодо протистояння кіберзагрозам поступаються у підготовці політично та економічно мотивованим нападникам, що в ряді випадків призводить до їх небезпечних кібератак.

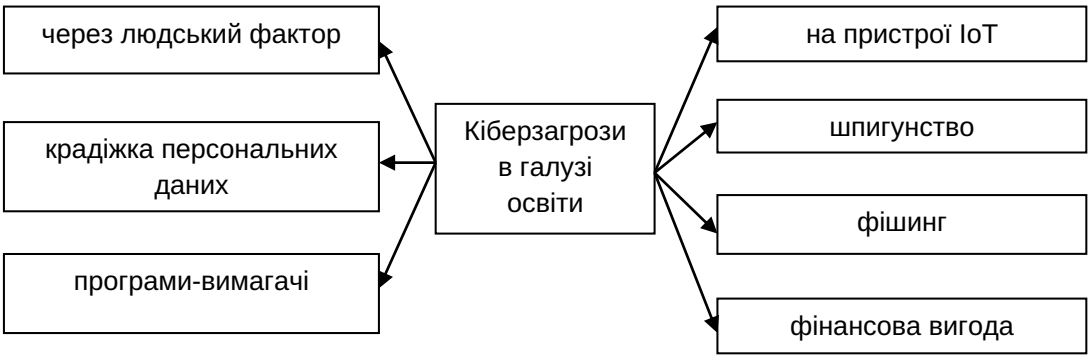

Рис. 2. Класифікація кіберзагроз у секторі вищої освіти

Джерело: [25], доопрацьовано авторами

В значній мірі зазначене стосується і ситуації в Україні.

Головні проблеми, які стоять перед фахівцями та структурами з даного питання: недостатня визначеність пріоритетів; неконкретність програмних заходів; відсутність плану розвитку основних суб'єктів національної системи кібербезпеки; обмеженість бюджетного фінансування; відсутність державно-приватного партнерства; несистемність кіберн навчання.

Важливим етапом у подальшому зміцненні кібербезпеки та її кадровому забезпеченні стало започаткування вітчизняними закладами вищої освіти навчання зі спеціальності «кібербезпека». При цьому кількість студентів та змістова градація у цьому напрямку щорічно зростають.

З часом все більше загроз виникає для закладів вищої освіти і їх контингенту – викладачів, студентів, технічних працівників. Військова агресія росії і пов'язані з нею кіберзагрози призвели до необхідності переорієнтації в підготовці кадрів, особливо що стосується дистанційного навчання.

Основним засобом захисту є навчання студентів, викладачів та організаторів навчального процесу. Від рівня підготовленості, компетентності і відповідальності учасників залежить кібербезпека і, як наслідок, успішне та стабільне функціонування закладів вищої освіти України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с.

2. Деякі питання оптимізації системи центральних органів виконавчої влади : Постанова Кабінету Міністрів України від 2 верес. 2019 р. № 829. Урядовий портал. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-optimizaciyi-sistem-829

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. № 447/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

4. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовт. 2017 р. № 2163-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Вступна кампанія 2022. Єдина державна електронна база з питань освіти. URL: https://vstup.edbo.gov.ua/offers/

6. Свердлик З. (2022). Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*, (10), 175–188. DOI: https://doi.org/10.31866/2616-7654.10.2022.269495

7. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.

8. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: науково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально-наукового інституту захисту інформації. Київ, 2022. С. 31–33.

9. Кузьменко О., Маклюк О., Чернишова О. (2022). Кібербезпека бізнесу під час війни. *Економіка та суспільство*, (44). DOI: https://doi.org/10.32782/2524-0072/2022-44-21

10. 10. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. Київ, 2023. № 7 (липень). 270 с.

11. Welcome to GCHQ.Pioneering a new kind of security for an ever more complex world. URL: www.gchq.gov.uk

12. Equities process Publication of the UK's process for how we handle vulnerabilities. URL: www.ncsc.gov.uk/blog-post/equities-process

13. Tencent Xuanwu Lab Security URL: http://blogstechnet.microsoft.com/msrc/2018/04/20/recognizing-q3-top-5

14. A new approach for cyber security in the UK (2016). URL: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk

15. Khlaponin Y. I., Kondakova S. V., Shabala Y. Y., Yurchuk L. P., Demianchuk P. S. (2019) Аналіз стану кібербезпеки в провідних країнах світу. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 4(4), 6–13. DOI: https://doi.org/10.28925/2663-4023.2019.4.613

16. New tank йducation&recherche URL: https://education.newstank.fr/article/view/257099/40-chercheurs-ukrainiens-refugier-endroits-plus-surs-berezko-eurodoc.html

17. Жила Г. Вища освіта в умовах війни: виклики, проблеми, перспективи для студентів та науковців. *Молодь і ринок*. 2023. № 2 (210). С. 141–145. DOI: https://doi.org/10.24919/2308-4634.2023.276118

18. Розпорядження КМУ «Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 роки» від 23 лютого 2022 р. № 286-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-strategiyi-rozvitku-vishchoyi-osviti-v-ukrayini-na-20222032-roki-286-

19. Маклюк О. В., Кононенко С. В. Вища освіта в умовах воєнного стану. Збірник матеріалів І Всеукраїнської науково-практичної конференції Соціально-економічна та правова політика України: виклики сьогодення (6 грудня 2023 року). Чернігів : Північноукраїнський інститут ім. Героїв Крут ПрАТ «ВНЗ «МАУП», 2023. 226 с. С.110–117. URL: http://maupchern.pp.ua/wp-content/uploads/2023/12/sbornik_2023_fall.pdf#page=110

20. Биков В. Ю., Спірін О. М., Пінчук О. П. «Загальна середня освіта як базова ланка в системі безперервної освіти». Наукове забезпечення розвитку освіти в Україні: актуальні проблеми теорії і практики (до 25-річчя НАПН України) [Текст] : збірник наукових праць, Київ : Видавничий дім «Сам», 175–245, 2017.

21. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. Т. 70. № 2. С. 313–331. URL: http://nbuv.gov.ua/UJRN/ITZN_2019_70_2_25

22. Кіберризики: як розуміти та управляти. URL: https://10guards.com/ua/articles/cyber-risks/

23. Трофименко О. Г. Кібербезпека освітнього сектора. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 698–700. URL: https://hdl.handle.net/11300/19765

24. Geer D., Jardine E., Leverett E. (2020). On market concentration and cybersecurity risk. Journal of Cyber Policy, 5, 1–21. DOI: https://doi.org/10.1080/23738871.2020.1728355. URL: https://www.researchgate.net/publication/339459416_On_market_concentration_and_cybersecurity_risk

25. Trofymenko O., Loginova N., Serhii M., Dubovoi1 Y. (2022). Кіберзагрози в освітньому секторі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 4(16). 76–84. DOI: https://doi.org/10.28925/2663-4023.2022.16.7684

26. Arsenovych, L. (2022) Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,* 3(15), 93–109. DOI: https://doi.org/10.28925/2663-4023.2022.15.93109

27. Татомир І. Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний дискурс*. 2020. Випуск 1. С. 59–67. DOI: https://doi.org/10.36742/2410-0919-2020-1-7

28. Kyva V. (2022) Аналіз чинників, які впливають на кібербезпеку вищого військового навчального закладу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 53–70. DOI: https://doi.org/10.28925/2663-4023.2022.15.5370

REFERENCES:

1. Lisovska, Yu. (2019) Kiberbezpeka: ryzyky ta zakhody [Cyber security: risks and measures]. Kyiv: Condor, 272 p. [in Ukrainian].

2. Cabinet of Ministers of Ukraine. Deiaki pytannia optymizatsii systemy tsentralnykh orhaniv vykonavchoi vlady [Some issues of optimization of the system of central executive bodies]. Resolution № 829 (2019, September 2). *Government portal*. Available at: https://cutt.ly/CwMC2ptv [in Ukrainian].

3. Verkhovna Rada of Ukraine. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy» [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine»]: Decree of the President of Ukraine N 447/2021 (2021, August 26). Available at: https://cutt.ly/GwMC2Fw5 [in Ukrainian].

4. Verkhovna Rada of Ukraine. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the main principles of ensuring cyber security of Ukraine] Law of Ukraine N 2163-VIII (2017, October 5). Available at: https://cutt.ly/xwMC293o [in Ukrainian].

5. Unified state electronic database on education. Vstupna kampaniia 2022 [Admission campaign 2022]. Available at: https://vstup.edbo.gov.ua/offers/ [in Ukrainian].

6. Sverdlyk Z. (2022) Kiberbezpeka ta kiberzakhyst: pytannia poriadku dennoho v ukrainskomu suspilstvi [Cyber security and cyber protection: issues on the agenda in Ukrainian society]. *Ukrainskyi zhurnal z bibliotekoznavstva ta informatsiinykh nauk – Ukrainian Journal of Library Science and Information Sciences*, vol. 10, pp. 175–188. Available at: https://cutt.ly/xwMC9v6X [in Ukrainian].

7. Bilyavska Yu., Shestak Ya. (2022) Kiberbezpeka ta kiberhihiiena: nova era tsyfrovykh tekhnolohii [Cyber security and cyber hygiene: a new era of digital technologies]. *Tovary i rynky – Goods and markets,* vol. 3, pp. 47–59 [in Ukrainian].

8. Vyshnivskyi V. V., Pampukha A. I. (2022) Kiberbezpeka v Ukraini [Cybersecurity in Ukraine]. *Digital transformation of cyber security: a scientific and practical online conference* (pp. 31–33), Kyiv: State University of Telecommunications of the Educational and Scientific Institute of Information Protection [in Ukrainian].

9. Kuzmenko O., Makliuk O., Chernyshova O. (2022) Kiberbezpeka biznesu pid chas viiny [Business Cybersecurity in a Time of War]. *Ekonomika ta suspilstvo – Economy and society*, vol. 44. Available at: https://cutt.ly/SwMC9Ckm [in Ukrainian].

10. Dovgan O. (Eds.). (2023). Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest [Cybersecurity in the information society: Informational and analytical digest]. Kyiv: State scientific institution «Institute of Information, Security and Law of the National Academy of Sciences of Ukraine»; National Library of Ukraine named after V. I. Vernadskyi, vol. 7 [in Ukrainian].

11. Welcome to GCHQ. Pioneering a new kind of security for an ever more complex world. Available at: https://www.gchq.gov.uk [in English].

12. Equities process Publication of the UK's process for how we handle vulnerabilities. Available at: https://cutt.ly/ZwMC3rsE [in English].

13. Tencent Xuanwu Lab Security. Available at: https://cutt.ly/DwMC0HON [in English].

14. A new approach for cyber security in the UK (2016). Available at: https://cutt.ly/nwMC3x1E [in English].

15. Khlaponin Y. I., Kondakova S. V., Shabala Y. Y., Yurchuk L. P., Demianchuk P. S. (2019). Analiz stanu kiberbezpeky v providnykh krainakh svitu [Analysis of the state of cyber security in the world's leading countries]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» – Electronic professional scientific publication* «*Cybersecurity: education, science, technology*», vol. 4(4), pp. 6–13. Available at: https://cutt.ly/xwMC3G2M [in Ukrainian].

16. New tank education&recherche Available at: https://cutt.ly/AwMC0qxB [in in French].

17. Zhyla G. (2023). [Vyshcha osvita v umovakh viiny: vyklyky, problemy, perspektyvy dlia studentiv ta naukovtsiv] Higher education in the conditions of war: challenges, problems, prospects for students and scientists. *Molod i rynok – Youth and the market,* vol. 2 (210), pp. 141–145. Available at: https://cutt.ly/WwMC1TrH [in Ukrainian].

18. Cabinet of Ministers of Ukraine. Rozporiadzhennia Kabinetu Ministriv Ukrainy «Pro skhvalennia Stratehii rozvytku vyshchoi osvity v Ukraini na 2022–2032 roky» № 286 [Decree of the Cabinet of Ministers of Ukraine «On the Approval of the Strategy for the Development of Higher Education in Ukraine for 2022–2032» № 286] (2022, February 23). Available at: https://cutt.ly/pwMCM40o [in Ukrainian].

19. Makliuk O.V., Kononenko S.V. (2023) Vyshcha osvita v umovakh voiennoho stanu [Higher education under martial law]. *Collection of materials of the 1st All-Ukrainian scientific and practical conference Socio-economic and legal policy of Ukraine: today's challenges*. Chernihiv: North Ukrainian Institute named after Heroiv Krut PJSC «MAUP University», pp. 110–117. Available at: https://cutt.ly/RwMCMW1O [in Ukrainian].

20. Bykov V., Spirin O., Pinchuk O. (2017). Zahalna serednia osvita yak bazova lanka v systemi bezperervnoi osvity [General secondary education as a basic link in the system of continuous education]. *Scientific support for the development of education in Ukraine: topical problems of theory and practice (to the 25th anniversary of the National Academy of Sciences of Ukraine)*: *collection of scientific works,* Kyiv: Sam Publishing House, pp. 175–245 [in Ukrainian].

21. Bykov V., Burov O., Dementievska N. (2019) Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cyber security in a digital educational environment]. *Informatsiini tekhnolohii i zasoby navchannia – Information technologies and teaching aids,* vol. 2 (70), pp. 313–331. Available at: https://cutt.ly/0wMC8sZM [in Ukrainian].

22. 10Guards. Kiberryzyky: yak rozumity ta upravliaty [Cyber risks: how to understand and manage]. Available at: https://cutt.ly/bwMC8Uhv [in Ukrainian].

23. Trofymenko O.G. (2022) Kiberbezpeka osvitnoho sektora [Cybersecurity of the educational sector]. *The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century (to the 25th anniversary of the National University* «*Odesa Law Academy*» *and the 175th anniversary of the Odessa School of Law)*: *materials of International science and practice conference*. (Vol. 1). Odesa: «Helvetyka» Publishing House, pp. 698–700. Available at: https://hdl.handle.net/11300/19765 [in Ukrainian].

24. Geer, D., Jardine, E., Leverett, E. (2020). On market concentration and cybersecurity risk*. Journal of Cyber Policy*, vol. 5, pp. 1–21. Available at: https://cutt.ly/rwMCB9wP [in English].

25. Trofymenko O., Loginova N., Serhii M., Dubovoi1 Y. (2022). Kiberzahrozy v osvitnomu sektori [Cyber threats in the education sector]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» –*

Electronic professional scientific publication «Cybersecurity: education, science, technology», vol. 4(16), pp. 76–84. Available at: https://cutt.ly/BwMCN8oj [in Ukrainian].

26. Arsenovych L. (2022). Instrumentarii pidvyshchennia rivnia tsyfrovoi kompetentnosti fakhivtsiv iz kiberbezpeky v osvitnomu protsesi [Toolkit for increasing the level of digital competence of cyber security specialists in the educational process]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» – Electronic professional scientific publication «Cybersecurity: education, science, technology»*, vol. 3(15), pp. 93–109. Available at: https://cutt.ly/UwMCNYrE [in Ukrainian].

27. Tatomyr I. (2020) [Kiberbezpeka universytetiv yak sposib protydii fishynhovomu shakhraistvu] Cyber security of universities as a way to counter phishing scams. *Ekonomichnyi dyskurs – Economic discourse,* vol. 1, pp. 59–67. Available at: https://cutt.ly/YwMC86NU [in Ukrainian].

28. Kyva V. (2022) Analiz chynnykiv, yaki vplyvaiut na kiberbezpeku vyshchoho viiskovoho navchalnoho zakladu [Analysis of factors affecting the cyber security of a higher military educational institution]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» – Electronic professional scientific publication «Cybersecurity: education, science, technology»,* vol. 3(15), pp. 53–70. Available at: https://cutt.ly/gwMC4TuQ [in Ukrainian].