КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.5370
УДК 004.056

Кива Владислав Юрійович
доктор філософії,
слухач інституту забезпечення військ (сил) та інформаційних технологій
Національний університет оборони України імені Івана Черняховського, м. Київ, Україна
ORCID ID: 0000-0002-6689-7530
kyvavlad30101991@gmail.com

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА КІБЕРБЕЗПЕКУ ВИЩОГО ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Анотація. У статті розглянуто вплив розвитку та поширення інформаційно-комунікаційних технологій (ІКТ) у вищому військовому навчальному закладі (ВВНЗ), оскільки з одного боку – підвищує ефективність його функціонування та сприяє підготовці висококваліфікованих кадрів (тактичного, оперативного та стратегічного рівня військової освіти) для Сектору безпеки і оборони України, що є вкрай необхідним в умовах протистояння збройній агресії Російської Федерації, а з іншого – робить вразливим його інформаційний простір до кібератак, що актуалізує проблемне питання забезпечення кібербезпеки ВВНЗ. При цьому, автор зосереджує увагу на аналізі кібератак на заклади освіти останніх років, які обумовлені розвитком методів (засобів) їх виконання та широким доступом до них різних користувачів, зокрема зловмисників. До того ж визначено, що розподілена кібератака на відмову в обслуговуванні (*Distributed Denial of Service – DDoS*) є найпоширенішою кіберзагрозою міжнародних освітніх закладів, що відображено в аналітичному звіті компанії *Netscout* (компанія розробник ІКТ рішень для протидії *DDoS* кібератакам – США). Проаналізовано, що останнім часом зловмисники використовують *DDoS* кібератаки з метою вимагання грошей. При чому *DDoS* кібератаки були спрямовані, як на банки, фондові біржі, туристичні агентства, валютні біржі, так і на заклади освіти. Тому, кібербезпека ВВНЗ потребує постійної уваги з боку учасників її забезпечення. Окрім того, проведений аналіз свідчить, що на кібербезпеку будь-якого ВВНЗ впливають зовнішні та внутрішні чинники, що підтверджує актуальність обраного напряму дослідження. У зв'язку з цим кібербезпека ВВНЗ вимагає аналізу чинників, які на неї впливають, з метою вибору кращого варіанту її реалізації. Відповідно у статті визначено сутність та основні особливості впливу чинників на кібербезпеку ВВНЗ та наведено їх характеристику. Зроблено декомпозицію впливу чинників на кібербезпеку ВВНЗ, зокрема за взаємозалежністю та критичністю їх впливу. Обґрунтовано необхідність врахування та постійного моніторингу впливу зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ, що дає змогу отримати ситуаційну обізнаність сучасного стану кібербезпеки та прийняти керівництву відповідні рішення.

Ключові слова: вищий військовий навчальний заклад; інформаційно-комунікаційні технології; чинники; кібербезпека; кібератаки.

ВСТУП

Постановка проблеми. Нині в Україні спостерігається активне впровадження ІКТ в освітньо-наукову діяльність закладів вищої освіти (ЗВО), зокрема і ВВНЗ. Відповідно, впровадження ІКТ у ВВНЗ є передумовою для великого потенціалу змін консервативних підходів стосовно щоденного навчання військовослужбовців, що обумовлено його доступністю, мобільністю та ефективністю [7].

Разом з тим є і проблемні питання щодо впровадження і застосування ІКТ у ВВНЗ, а саме:

– недостатнє фінансування для закупівлі ІКТ;

– відсутність стратегічного бачення з боку керівництва ВВНЗ щодо впровадження та застосування сучасних ІКТ;

– недостатня обізнаність викладачів та навчаємих (студентів, солдатів, курсантів та слухачів) щодо застосування ІКТ під час навчання;

– відсутність або наявність невеликої кількісті фахівців (безпосередньо у ВВНЗ) яка б забезпечувала функціонування та кібербезпеку ІКТ.

У випадку з трьома першими пунктами щодо проблемних питань впровадження ІКТ у ВВНЗ, можна стверджувати про активну діяльність керівників ВВНЗ щодо їх вирішення. Тоді як четверте проблемне питання є вкрай проблематичним і спостерігається не тільки у ВВНЗ але й на державному рівні.

Зокрема, 27 червня 2017 року відбулася кібератака з використанням шкідливого програмного забезпечення *Petya*, що спричинило порушення функціонування українських державних підприємств, установ, банків та медіа. Окрім того, в наслідок кібератаки було заблоковано діяльність таких критичних установ, як Ощадбанк, Укрзалізниця та аеропорт «Бориспіль». Завдяки цьому, вище керівництво держави звернуло увагу на проблемне питання пов'язане з забезпечення кібербезпеки в Україні, що і актуалізувало прийняття закону та рішень Ради національної безпеки і оборони України, а саме: Закону України «Про основні засади забезпечення кібербезпеки України» [11]; Рішення Ради національної безпеки і оборони України «Про невідкладні заходи з кібероборони держави» [12]; «Про Стратегію кібербезпеки України» [13] та «Про Стратегічний оборонний бюлетень України» [14]. Однак, прийнятті рішення та задекларовані наміри не реалізувалися на практиці. Так, у ніч з 13 на 14 січня 2022 року в чергове була здійснена кібератака на урядові сайти та портал «Дія» [3].

Аналогічно погіршила стан кібербезпеки в державі – пандемія *COVID*-19. Так, ЗВО, зокрема і ВВНЗ вимушені були перейти на дистанційне навчання. З одного боку, це прискорило впровадження ІКТ, а з другого – підвищило загрози щодо кібератак з боку зловмисників, що опубліковано у відповідних дослідженнях науковців [33], [38]. Обумовлено це неготовністю та відсутністю в ЗВО практики щодо забезпечення кібербезпеки освітньо-наукової діяльності в умовах віддаленої роботи.

При чому, аналіз наукових публікацій свідчить, що найбільш поширеною кібератакою на освітні ресурси закладів освіти є *DDoS* атака, яка створювала труднощі доступу до них [40], [23]. Очевидно, що кібервплив став реальною загрозою і є однією з пріоритетних проблем, як у повсякденному житті громадян, так і в освітньо-науковій діяльності ЗВО. Тому актуальною є проблема забезпечення кібербезпеки ЗВО, зокрема ВВНЗ, які щоденно здійснюють підготовку висококваліфікованих офіцерських кадрів та є системоутворюючим елементом формування і розвитку боєздатних та боєготовних Збройних Сил України.

Аналіз останніх досліджень і публікацій. Аналіз наукових джерел щодо кібербезпеки ЗВО свідчить, що наукові дослідження ведуться за такими проблемними напрямами, а саме:

– проблеми забезпечення кібербезпеки ЗВО (Ю. С. Антонов, П. В. Римар та О. Г. Антонова [1]; О. О. Ільїн, С. О. Сєрих та В. В. Вишнівський [5]; Н. М. Кириленко [9]; О. Ю. Чубукова та І. В. Пономаренко [17]; A. Ghazvini, Z. Shukur та Z. Hood [24]; S. Hina та P. D. D. Dominic [28]; IBM [22]; C. Joshi та U. K. Singh [31]);

– теоретичне обґрунтування системи управління кібербезпекою ЗВО (А. Ю. Нашинець-Наумова, В. Л. Бурячок, Н. В. Коршун, О. Б. Жильцов, П. М. Складанний та Л. В. Кузьменко [10]; I. S. Bianchi та R. D. Sousa [21]; X. H. He, Z. Z. Chun та Z. Z. Zhao [27]; H. Rehman, A. Masood та A. R. Cheema [37]; Y. Zeng, H. Zhang, X. Liu, Y. Fu, Q. Deng та R. Ye [43]);

– оцінювання кібербезпеки ЗВО (M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann та K. Sakurai [39]; W. Yustanti, A. Qoiriah, R. Bisma та A. Prihanto [42]);

– проблеми кібербезпеки учасників освітньо-наукової діяльності ЗВО (В. Ю. Биков, О. Ю. Буров та Н. П. Дементієвська [2]; M. Anwar, W. He, I. Ash, X. Yuan, L. Li та L. Xu [20]; M. Gratian, S. Bandi, M. Cukier, J. Dykstra та A. Ginther [26]; J. Jang-Jaccard та S. Nepal [29]; D. Jeske та P. V. Schaik [30]; W. D. Kearney та H. A. Kruger [32]; J. G. Mohebzada, A. E. Zarka, A. H. Bhojani та A. Darwish [34]; G. Ogutcu, O. M. Testik та O. Chouseinoglou [35]; M. Rajab [36]; Z. Yan, T. Robertson, R. Yan, S. Y. Park, S. Bordoff, Q. Chen та E. Sprissler [41]; J. Zhang, B. J. Reithel та H. Li [44]).

Проте, незважаючи на вагомі результати досліджень щодо кібербезпеки ЗВО, доводиться констатувати, що в жодному з них не було чітко визначено та проаналізовано чинники, які впливають на кібербезпеку ЗВО, зокрема ВВНЗ.

Крім того, дослідження науковців здебільшого фокусувалися на кіберзагрозах, а саме їх впливі та класифікації, які не дозволяють системно врахувати всю причинно-наслідкову систему зв’язків стосовно впливу на кібербезпеку ВВНЗ, що обумовлює актуальність статті.

Метою статті є аналіз зовнішніх та внутрішніх чинників, які впливають на кібербезпеку вищого військового навчального закладу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Дедалі ширше впровадження ІКТ є сьогодні загальносвітовим явищем. Воно спостерігається практично у всіх сферах людської діяльності, у тому числі і військовій [4], [15], [25]. Окрім того, сучасні процеси інформатизації призводять як до підвищення ролі інформаційних технологій, так і до залежності від них, зокрема в освітньо-науковій діяльності ВВНЗ.

Варто зазначити, що переважно всі ВВНЗ пройшли шлях від консервативно-традиційного (навчально-наукового) процесу до сучасної інформаційної (освітньо-наукової) діяльності. При цьому, будівництво власного інформаційного простору ВВНЗ включало, як правило такі кроки, а саме:

– оновлення та модернізація ІКТ обладнання;
– розроблення офіційного веб-сайту ВВНЗ та його структурних підрозділів;
– підключення ВВНЗ до мережі Інтернет та створення власної мережі Інтранет;
– впровадження електронного документообігу;
– впровадження системи дистанційного навчання;
– розроблення електронних освітніх ресурсів;
– розроблення електронної бібліотеки;
– впровадження системи електронних журналів для публікації наукових результатів дослідників;
– впровадження системи відеоконференцзв’язку;
– впровадження системи відеоспостереження;
– автоматизація фінансово-економічної діяльності ВВНЗ;
– автоматизація господарської діяльності ВВНЗ;
– автоматизація кадрової діяльність ВВНЗ;
– автоматизація медичної діяльності;
– впровадження системи контролю доступу до ВВНЗ.

Слід зазначити, що з одного боку, за рахунок інформатизації у ВВНЗ підвищується якість та ефективність освітньо-наукової діяльності, а з іншого – створюється

багаторівнева інформаційно-просторова система ВВНЗ, яка стає критичним об'єктом його надійного функціонування та кібербезпеки.

Відповідно, під **інформаційним простором ВВНЗ** будемо розуміти – інформаційне середовище (систему), яка утворюється та функціонує в результаті з'єднання різноманітних за призначенням ІКТ, з метою забезпечення суб'єкт-суб'єктної взаємодії того, хто вчить, і того, хто навчається. При цьому, під **кібербезпекою ВВНЗ** будемо розуміти – стан кіберзахищеності інформаційного простору ВВНЗ, при якому забезпечено конфіденційність, цілісність та доступність інформації яка в ній циркулює.

Разом з тим, критичність інформаційного простору ВВНЗ полягає в тому, що в ній накопичується та циркулює надзвичайно багато конфіденційної інформації, а саме:

– персональна (дані постійного та зміну складу ВВНЗ);

– службова (директиви, накази, розпорядження та документи з відповідним грифом обмеження доступу);

– фінансова (фінансові звіти та облік ресурсів);

– юридична (судові позови та службові розслідування);

– освітньо-наукова (інтелектуальна власність, патенти, перспективні наукові винаходи, науково-дослідні роботи, освітньо-наукові програми, фахові електронні журнали, електронні навчальні курси, електронна бібліотека та електронні ресурси).

У зв'язку з цим, інформаційний простір ВВНЗ є потенційною ціллю для реалізації різноманітних кібератак з боку зловмисників. Крім того, успішна реалізація кібератаки на інформаційний простір ВВНЗ може завдати таку шкоду:

– технічну (вихід з ладу технологічного обладнання; блокування доступу до інформаційного простору закладу, зокрема до освітніх ресурсів; знищення освітньо-наукової (інтелектуальної) власності);

– матеріальну (фінансові витрати на відновлення технологічного обладнання; проведення аудиту кібербезпеки експертами приватних фірм);

– репутаційну (припинення співробітництва з іншими ЗВО; зниження авторитету закладу; відтік вступників на навчання);

– моральну (шантаж керівництва або співробітників; завдання стресу особистості чиї дані було видалені, викрадені або розповсюдженні).

Таким чином, питання забезпечення кібербезпеки ВВНЗ, набуває особливої важливості та вимагає виконання таких завдань, а саме:

1. Аналізу чинників, які впливають на кібербезпеку ВВНЗ.
2. Розроблення та впровадження моделі кіберзахисту ВВНЗ.
3. Оцінювання ефективність функціонування моделі кіберзахисту ВВНЗ.
4. Розроблення рекомендацій щодо підвищення ефективності функціонування моделі кіберзахисту ВВНЗ.

З врахуванням мети дослідження, зупинимося саме на першому завданні, а саме аналізі чинників, які впливають на кібербезпеку ВВНЗ.

Варто зазначити, що кібербезпека ВВНЗ взаємозалежна від кіберзахисту, який можна представити як комплекс взаємопов'язаних заходів, які утворюють єдине ціле і мають спільну мету щодо забезпечення кібербезпеки ВВНЗ від впливу багатьох різноманітних чинників (умов). При цьому, по відношенню до об'єкта впливу, чинники можна розділити на внутрішні та зовнішні (рис. 1).

Слід наголосити, що вони можуть по-різному впливати на кібербезпеку ВВНЗ, зокрема одні з них можуть мати позитивний вплив, інші ж негативний. Відповідно, домінуючий вплив негативних чинників здатний знизити позитивну дію інших.

ISSN 2663 - 4023

Внутрішні чинники залежать від наших дій, тому ми можемо впливати на їх ефективність, як позитивно так і негативно. Тобто внутрішні чинники можуть як підвищити кібербезпеку ВВНЗ, так і знизити її через навмисні або ненавмисні наші дії.

Зовнішні чинники не залежать від нас, створюються зовнішніми умовами або зловмисником та є неконтрольованими. Проте опосередковано ми можемо впливати на їх ефективність шляхом посилення (удосконалення) своїх внутрішніх чинників, які спрямовані на забезпечення кібербезпеки ВВНЗ.

Рис. 1. Вплив зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ

Відповідно, вплив зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ визначає необхідність проведення постійного моніторингу його стану кіберзахищеності. Безумовно, що стан кіберзахищеності ВВНЗ буде залежати від правильно змодельованої та реалізованої моделі кіберзахисту, яка має ґрунтуватися на результатах аналізу впливу зовнішніх та внутрішніх чинників кібербезпеки ВВНЗ.

Тому, аналіз зовнішніх та внутрішніх чинників допомагає прийняти обґрунтовані управлінські рішення, які забезпечать взаємодію ВВНЗ із зовнішнім інформаційним простором в короткостроковій та довгостроковій перспективі. До того ж постійний моніторинг та прогнозування напряму впливу (дії) зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ, дає змогу керівництву розробляти відповідні стратегії реагування, які будуть максимально адекватними ситуації, що може гіпотетично відбутися.

Отже, проведений аналіз кібербезпеки ВВНЗ дає змогу визначити такі **основні зовнішні чинники**, які впливають на неї, а саме:

1. Надзвичайні ситуації.
2. Розроблення та виробництво апаратно-програмного забезпечення.
3. Кібератаки.
4. Вербування або шантаж особового складу.

Відповідно, розглянемо зовнішні чинники більш детально.

1. Надзвичайні ситуації. ВВНЗ має визначене місце розташування на окремій території, яка може піддаватися впливу природньої або техногенної небезпеки. При цьому вони можуть виникати в комплексі, що значно посилює їх вплив. Виникнення одного небезпечного явища може спричинити низку інших.

Природня небезпека. Будь-яка діяльність або функціонування окремого предмета, об'єкта або системи відбувається у взаємодії з природнім (навколишнім) середовищем, зокрема це повітря, вода, ґрунт. Так само і інформаційний простір ВВНЗ взаємодіє із природнім середовищем своїми окремими елементами, а саме: інформаційно-телекомунікаційними системами, лініями зв'язку, супутниковими та Wi-Fi антенами і т.д. Відповідно, всі вони прямо або опосередковано взаємодіють з природнім середовищем, яке може вплинути на їх функціонування та стан кібербезпеки ВВНЗ в цілому, шляхом небезпечних природніх явищ, зокрема це:

– геологічні (землетруси, зсуви, сель, карстове провалля, абразія);

– гідрологічні (повені, паводки, підтоплення, снігові лавини, дощ);

– метеорологічні (град, спека, вітер, смерч, снігопад, мороз, блискавка).

Техногенна небезпека. Масштаб техногенної небезпеки в ВВНЗ може сягати критичного рівня, що пов'язано з використанням електроенергії, горючих, вибухонебезпечних речовин та матеріалів. Аналіз техногенних ситуацій свідчить, що пожежа або вибух здатні завдати значні руйнівні втрати, як для критичної інформаційної інфраструктури, так і для особового складу ВВНЗ в цілому. Тому, питанню забезпечення техногенної безпеки слід приділяти достатньо уваги, зокрема усунути умови їх виникнення.

2. Розроблення та виробництво апаратно-програмного забезпечення.

Нині ІКТ з одного боку забезпечують підвищення ефективності вирішення багатьох науково-прикладних завдань, а з іншого – втягують у нескінчену залежність від них всі державні інститути країни, зокрема ВВНЗ. Слід наголосити, що основними складовими ІКТ є апаратна та програмна частини.

Відповідно, апаратна складова є техніко-технологічною основою (материнська плата, процесор, оперативний запам'ятовуючий пристрій, графічний адаптер, жорсткий диск і т.д.), за допомогою якої реалізується виконання (функціонування) програмної складової (операційні системи, різноманітне прикладне та системне програмне забезпечення і т.д.). У зв'язку з цим, вони взаємозалежні та доповнюють одна одну.

Слід наголосити, що аналіз застосування апаратно-програмно забезпечення ВВНЗ свідчить, що воно іноземного розроблення та виробництва. Окрім того, така ситуація спостерігається у всіх державних інститутах України. Необхідно зазначити, що пов'язано це зі спроможностями нашої країни щодо розроблення та виробництва відповідних зразків апаратно-програмного забезпечення, зокрема систематичним браком коштів на фінансування відповідних науково-технічних розробок. До того ж Україні буде важко ввійти в коло розробників (монополістів) апаратно-програмного забезпечення, а з врахуванням необхідно часу та фінансових ресурсів – фантастичні мрії.

Варто зазначити, що нині ринок апаратно-програмного забезпечення представлений такими учасниками:

– *Intel Corporation* (виробляє процесори для різних цифрових систем та пристроїв – США);

– *Advanced Micro Devices* (виробник інтегрованої електроніки та другий найбільший постачальник процесорів – США);

– *Nvidia Corporation* (виробник графічних процесорів, відеоадаптерів, мультимедійних та комунікаційних пристроїв для комп'ютерів – США);

ISSN 2663 - 4023

– *Radeon Technologies Group* (є підрозділом *Advanced Micro Devices*, виробляє графічні процесори – США);

– *Microsoft Corporation* (домінуюча корпорація з розробки програмного забезпечення, її продуктами користуються і домашні користувачі, і міжнародні корпорації – США);

– *Oracle Corporation* (розробник програмного забезпечення та баз даних для організацій – США);

– *Red Hat* (компанія випускає програмні рішення на базі вільної операційної системи *GNU/Linux* – США);

– *The Debian Project* (проект розробника програмного забезпечення Іана Ешлі Мердока – США);

– *Cisco Systems, Inc Cisco Systems* (світовий лідер у галузі мережевих технологій – США);

– *Dell* (американська корпорація, одна з найбільших компаній в області виробництва комп'ютерів – США);

– *Hewlett-Packard* (постачальник апаратно-програмного забезпечення для організацій та індивідуальних споживачів – США);

– *International Business Machines* (один з найбільших в усьому світі виробників та постачальників апаратно-програмного забезпечення – США);

– *Western Digital* (виробник комп'ютерної електроніки – США);

– *Toshiba* (міжнародний концерн, що працює в області електротехніки та електроніки – Японія);

– *D-Link* (поставляє мережеві та комунікаційні рішення підприємствам, малому та середнього бізнесу, провайдерам Інтернет та компаніям, що надають послуги зв'язку – Тайвань).

З врахуванням вищесказаного, виникає необхідність визначення ключових особливостей впливу іноземного програмного забезпечення на кібербезпеку ВВНЗ, які полягають в наступному:

– по-перше, помилки при розробленні та виробництві апаратно-програмного забезпечення (відсутність можливості контролю виробництва та тестування апаратно-програмного забезпечення, що може призвести до нештатних ситуацій під час його функціонування, зокрема до повного або часткового виводу з ладу);

– по-друге, відсутність юридичної відповідальності за відсутність кіберзахисту при розробленні та виробництві апаратно-програмного забезпечення (відповідальність за потенційно можливі реалізовані кібератаки або збої лежить виключно на користувачі, який його обслуговує);

– по-третє, гіпотетична ймовірність наявності навмисно вбудованих вразливостей в апаратно-програмному забезпеченні (перехід від класичних бойових дій до інформаційного протиборство, де питання своїх національних інтересів завжди буде стояти вище інтересів інших країн);

– по-четверте, неможливість створення єдиної системи кіберзахисту ВВНЗ у відповідності до запропонованих рішень з боку іноземного виробника апаратно-програмного забезпечення (наявність бажання створення комплексної системи кіберзахисту ВВНЗ та відсутність фінансових можливостей для її реалізації, зокрема висока ціна – високий рівень кіберзахищеності, низька ціна – низький рівень кіберзахищеності ВВНЗ).

А отже, без сумніву можна сказати, що все апаратно-програмне забезпечення яке використовується в ВВНЗ є іноземного виробництва, а це збільшує ймовірність його впливу на кібербезпеку ВВНЗ.

ISSN 2663 - 4023

3. Кібератаки. Слід наголосити, що одним з головних чинників, який впливає на кібербезпеку ВВНЗ є кібератака. Під **кібератакою** будемо розуміти – цілеспрямовані дії на складові елементи інформаційного простору, які виконуються шляхом застосування апаратно-програмних засобів з метою порушення їх конфіденційності, цілісності та доступності.

До того ж кібератака може виконуватися віддалено (знаходження атакуючого за межами операційної зони впливу по відношенню до об'єкта) або локально (безпосередня фізична присутність атакуючого по відношенню до об'єкта впливу).

Здебільшого найпоширенішими типами кібератак, які спостерігаються є:

– шкідливе програмне забезпечення (в залежності від його функціоналу може отримати повний доступ до операційної системи, зокрема: контролювання дій об'єкта впливу та натискання клавіш; відправка, знищення або модифікація конфіденційної інформації і т.д.);

– фішинг (використання зацікавленості або імпульсивності об'єкта впливу з метою виконання їм заздалегідь спланованих небезпечних дій, зокрема: відкриття в електронному листі посилання або файлу, що призведе до зараження або перенаправлення на шкідливий сайт; використання коротких текстових повідомлень (смішінг) або голосових дзвінків (вішинг) з метою виконання наведених вище дій по відношенню до об'єкта впливу);

– *SQL Injection* (застосування мови структурованих запитів для впливу на базу даних сайту (сервера) об'єкта впливу, що дозволяє виконувати шкідливий код);

– *XSS* (міжсайтовий скриптинг, що дозволяє використовувати вразливий сайт (сервер) для кібератаки на об'єкт впливу, зокрема шкідливий код інтегрується у сайт, який буде відвідувати об'єкт впливу, що надалі дозволяє атакуючому отримати його авторизаційні куки);

– *DoS* (відмова в обслуговуванні, яка полягає в неможливості отримати доступ до інформаційного ресурсу (об'єкта атаки) у зв'язку з одночасним підключенням до нього мережі ботів, що призводить до повної витрати пам'яті та процесорного ресурсу сервера);

– атака нульового дня (використання вразливості апаратно-програмного забезпечення, яка невідома його користувачам чи розробникам, що дозволяє атакуючому використати її в своїх намірах, з метою порушення конфіденційності, цілісності та доступності інформаційного ресурсу).

При цьому, кібератаки постійно вдосконалюються, а їх масштабність стає критичною. З цієї причини керівник ВВНЗ має чітко усвідомити ефект впливу кібератак на функціонування його інформаційного простору та прийняти відповідні рішення щодо кіберзахисту.

4. Вербування або шантаж особового складу. Останніми роками дуже багато говориться про діяльність російської агентури в Україні, зокрема резонанс був із затриманням високопосадовців Станіслава Єжова [18] та генерал-майора Валерія Шайтанова [16]. Ці випадки свідчать, що активно відбувається вербування або шантаж відповідних суб'єктів з метою заподіяння шкоди національній безпеці України.

Крім того, гіпотетично це може відбутися і у ВВНЗ, який виконує важливе завдання щодо підготовки висококваліфікованих офіцерських кадрів та є системоутворюючим елементом формування і розвитку боєздатних та боєготовних Збройних Сил України.

У зв'язку з цим постає дуже складне завдання щодо недопущення вербування посадових осіб (відповідають за функціонування інформаційної інфраструктури) та постійного особового складу (професорсько-викладацький склад) ВВНЗ, які потенційно

можуть бути завербовані або під впливом шантажу виконати кібератаку на критичні елементи інформаційного простору ВВНЗ.

Отже, проаналізувавши зовнішні чинники, які впливають на кібербезпеку ВВНЗ можемо зробити висновок, що вони є неконтрольованими з боку ВВНЗ, а також під їх впливом постає необхідність змінювати та посилювати свої внутрішні чинники, які з одного боку, зменшують ефективність впливу зовнішніх чинників, а з іншого – забезпечують кібербезпеку ВВНЗ. Водночас є необхідність аналізу внутрішніх чинників, які впливають на кібербезпеку ВВНЗ.

Проведений аналіз кібербезпеки ВВНЗ дає змогу визначити такі **основні внутрішні чинники**, які впливають на неї, а саме:

1. Підготовленість (навченість) особового складу.
2. Політика кіберзахисту.
3. Топологія (архітектура) інформаційного простору.
4. Апаратне забезпечення.
5. Програмне забезпечення.

Відповідно, розглянемо внутрішні чинники більш детально.

1. Підготовленість (навченість) особового складу. У зв'язку з геометричним зростання кібератак в усьому світі перед різноманітними суб'єктами державних інститутів, зокрема і ВВНЗ постає завдання, щодо пошуку раціональних рішень щодо підвищення ефективності їх кіберзахищеності.

До того ж проведений аналіз свідчить, що неусвідомлені дії (необережність та неуважність) різної категорії особового складу, які прямо або опосередковано впливають на кібербезпеку ВВНЗ є однією з головних причин зниження її рівня. При цьому аналіз неусвідомлених дій особового складу по відношенню до кіберзахисту ВВНЗ свідчить, що передумовою їх прояву були такі причини:

– відсутність цінностей та мотивації щодо дотримання правил кіберзахисту (відсутність з боку керівництва дій щодо формування у особового складу ВВНЗ цінностей та мотивації до виконання правил кіберзахисту при застосуванні ІКТ у науко-педагогічній діяльності, а також відсутність розуміння важливості діагностування їх рівня сформованості [6], [8], [19]);

– низький рівень освітнього, наукового та методичного забезпечення кібербезпеки освітньо-наукової діяльності (фрагментований підхід до формування у особового складу ВВНЗ компетентності з кіберзахисту або його відсутність взагалі; відсутність досліджень щодо проблемних питань пов'язаних із забезпеченням кібербезпеки особового складу в їх освітньо-науковій діяльності; відсутність методичної літератури з практичними прикладами щодо кіберзахисту).

Розглянувши причини неусвідомлених дій особового складу по відношенню до кіберзахисту ВВНЗ, необхідно зазначити, що без забезпечення ціннісно-мотиваційної підготовки особового складу досягнути кіберзахищеності не вдасться. Крім того, питання підготовки з кіберзахисту є системоутворюючим елементом забезпечення кібербезпеки ВВНЗ. Зокрема це пов'язано з тим, що:

– по-перше, за впровадження ІКТ в освітньо-наукову діяльність та забезпечення кіберзахисту ВВНЗ відповідає окремий технічний підрозділ, від рівня підготовленості (компетентності) якого залежить якість виконання завдання щодо розроблення політики кіберзахисту ВВНЗ, яка має враховувати організаційно-правові та інженерно-технічні заходи, зокрема: затвердження настанов, правил, обмежень, рекомендацій та інструкцій на основі якої будується кіберзахист ВВНЗ; покладання відповідальності за розгортання та функціонування інформаційного простору ВВНЗ; визначення топології (архітектури)

ISSN 2663 - 4023

інформаційного простору ВВНЗ та апаратно-програмного забезпечення яке буде встановлено);

– по-друге, від рівня підготовленості (компетентності) особового складу залежить кібербезпека інформаційного простору ВВНЗ, а саме усвідомлення або не усвідомлення дій стосовно використання ІКТ в освітньо-науковій діяльності, що може призвести до кіберзагроз.

Звідси можна зробити висновок, що проблема підготовки (навченості), як особового складу, так і фахівців у сфері кіберзахисту ВВНЗ, актуальна як ніколи і цьому питанню необхідно приділяти першочергову увагу.

2. Політика кіберзахисту. Варто зазначити, що політика кіберзахисту визначає сукупність настанов, правил, обмежень, рекомендацій та інструкцій, на основі якої будується кіберзахист ВВНЗ, зокрема вона має враховувати організаційно-правові та інженерно-технічні заходи, а саме:

– юридичну відповідальність визначеного кола фахівців за розгортання та функціонування інформаційного простору ВВНЗ;

– топологію (архітектури) інформаційного простору ВВНЗ та апаратно-програмного забезпечення яке буде встановлено;

– модель кіберзахисту ВВНЗ;

– порядок використання інформаційного простору ВВНЗ користувачами та дотримання вимог (правил) з кіберзахисту;

– порядок надання та використання прав доступу користувачів в системі інформаційного простору ВВНЗ;

– вимоги звітності користувачів інформаційного простору ВВНЗ щодо виникнення кіберінцидентів;

– план реагування (заходів) користувачів інформаційного простору ВВНЗ на випадок кіберінцидентів і т.д.

Відтак, система кіберзахисту ВВНЗ буде ефективною, якщо будуть виконуватися вимоги (правила) політики кіберзахисту. Крім того, перш за все необхідно визначити головну мету побудови системи кіберзахисту ВВНЗ, що має виражатися через вплив сукупності зовнішніх та внутрішніх чинників, які впливають на неї. Сукупність зовнішніх та внутрішніх чинників є базисом (основою) для визначення вимог до системи кіберзахисту ВВНЗ.

Без сумніву, розробка політики кіберзахисту ВВНЗ є нетривіальним завданням. Експерти (фахівці) з кіберзахисту мають не тільки знати відповідні стандарти, мати високий рівень підготовленості (компетентності) і добре розбиратися в комплексних підходах до забезпечення кіберзахисту інформаційного простору, але й, наприклад, проявляти детективні здібності при виявленні особливостей його побудови.

Крім того, необхідним є постійний аналіз відповідності політики кіберзахисту ВВНЗ реальному стану речей, що вкрай важливо. З цієї причини необхідно за сукупністю показників кіберзахисту визначити відповідні критерії (відібрати свого роду «контрольні точки») та провести оцінювання стану кібербезпеки, за результатами якого встановити відповідність (невідповідність) політики кіберзахисту заданим вимогам кіберзахищеності та зробити відповідні зміни до неї.

3. Топологія (архітектура) інформаційного простору. Побудова інформаційного простору ВВНЗ неможлива без визначення її топології (архітектури), яка буде визначати спосіб розміщення та з’єднання елементів ІКТ.

При цьому, побудова тієї або іншої топології (архітектури) інформаційного простору ВВНЗ впливає на:

ISSN 2663 - 4023

– кількість необхідного апаратного (мережевого обладнання) та програмного забезпечення для організації ліній (каналів) зв'язку;

– спосіб з'єднання апаратних (мережевого обладнання) та різних за призначення елементів ІКТ;

– функціональні можливості апаратного (мережевого обладнання) та програмного забезпечення;

– можливість розширення інформаційного простору;

– сегментацію (зони) інформаційного простору;

– спосіб управління інформаційним простором;

– модель кіберзахисту інформаційного простору;

– фінансові витрати щодо закупівлі апаратного (мережевого обладнання) та програмного забезпечення.

Виходячи з вищесказаного, можна зробити висновок, що чим складніша топологія (архітектура) інформаційного простору ВВНЗ, тим складнішим є завдання забезпечення її кіберзахищеності, що в свою чергу впливає на кібербезпеку ВВНЗ в цілому.

4. Апаратне забезпечення. Нині інформатизація освітньо-наукової діяльності ВВНЗ потребує сучасного апаратного забезпечення. Під апаратним забезпеченням будемо розуміти – спеціалізовані обчислювальні засоби (пристрої) або електронні (механічні) його складові. Крім того, сучасні тенденції свідчать про необхідність мати продуктивне апаратне забезпечення, яке буде спроможне виконувати складні навантаження в умовах створення, оброблення, передачі, зберігання та кіберзахисту циркулюючої інформації (даних) в інформаційному просторі ВВНЗ.

Проведений аналіз апаратного забезпечення дає змогу визначити такі основні характеристики (показники) його впливу на кібербезпеку ВВНЗ, а саме:

– встановлення (наявність) апаратного забезпечення;

– актуальність (сучасність) апаратного забезпечення;

– справність апаратного забезпечення;

– налаштованість апаратного забезпечення.

При цьому невідповідність хоча б одній з характеристик впливу апаратного забезпечення на кібербезпеку ВВНЗ створює передумови для зниження кіберзахищеності ВВНЗ, тобто створенню вразливості в інформаційному просторі. Тому, при оцінюванні кібербезпеки ВВНЗ необхідно враховувати всі перераховані вище характеристики впливу апаратного забезпечення на кібербезпеку ВВНЗ.

5. Програмне забезпечення. Слід наголосити, що без використання програмного забезпечення неможливо реалізувати кінцеву мету – інформатизацію освітньо-наукової діяльності ВВНЗ. При цьому кожен ВВНЗ використовує в своїй освітньо-науковій діяльності таке програмне забезпечення, як: операційні системи *Microsoft Windows*; редактор документів *Microsoft Office*; модульне об'єктно-орієнтоване динамічне навчальне середовище *Moodle*; антивірусні програми *ESET* і т.д.

Разом з тим, роль програмного забезпечення полягає в керуванні апаратними складовими різноманітного обладнання (пристроїв), створенні, обробленні, передачі, зберіганні та кіберзахисті циркулюючої інформації (даних) в інформаційному просторі ВВНЗ. До того ж апаратне та програмне забезпечення, взаємозалежні та доповнюють одна одну.

Проведений аналіз програмного забезпечення дає змогу визначити такі основні характеристики (показники) його впливу на кібербезпеку ВВНЗ, а саме:

– встановлення (наявність) програмного забезпечення;

– актуальність (сучасність) програмного забезпечення;

– справність програмного забезпечення;

ISSN 2663 - 4023

– налаштованість програмного забезпечення.

Так само, як і з апаратним забезпечення, невідповідність хоча б одній з характеристик впливу програмного забезпечення на кібербезпеку ВВНЗ створює передумови для зниження кіберзахищеності ВВНЗ, тобто створенню вразливості в інформаційному просторі. Тому, при оцінюванні кібербезпеки ВВНЗ необхідно враховувати всі перераховані вище характеристики впливу програмного забезпечення на кібербезпеку ВВНЗ.

Врешті, проведений аналіз зовнішніх та внутрішніх чинників дає можливість зробити декомпозицію їх впливу на кібербезпеку ВВНЗ, що важливо для системного розуміння причинно-наслідкових зв'язків (рис. 2).

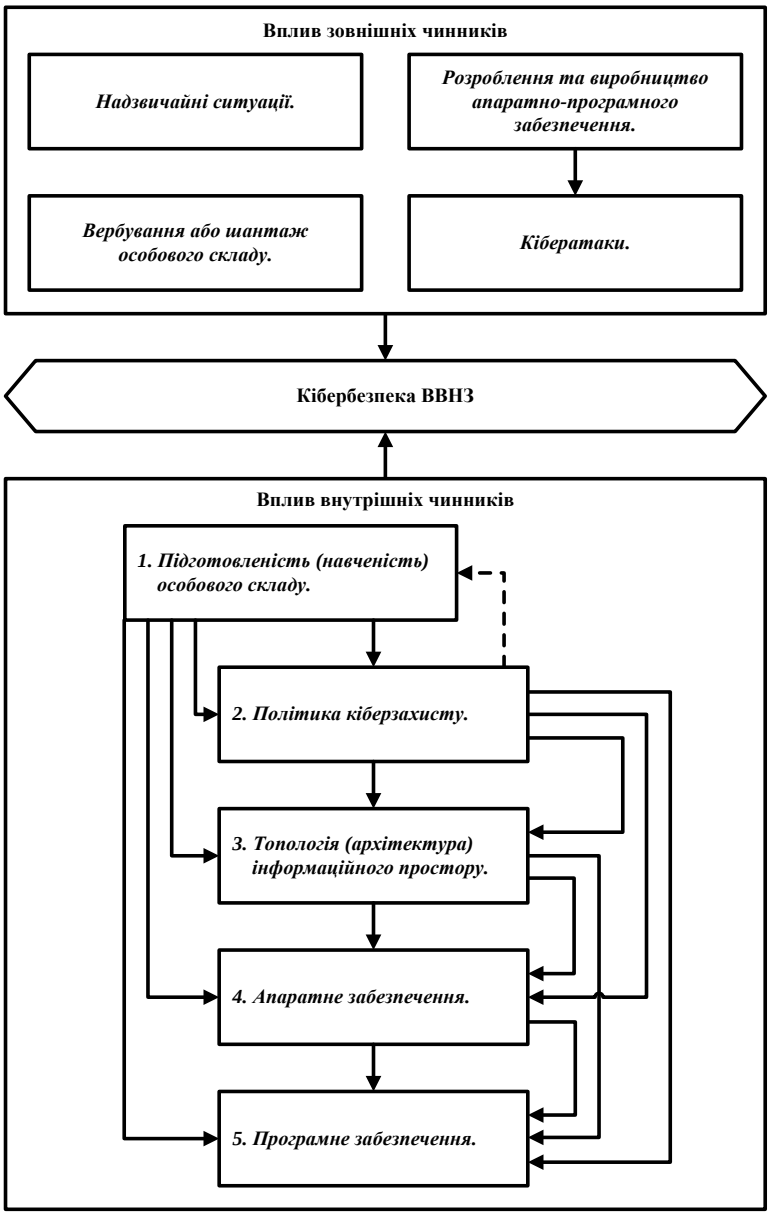

Рис. 2. Декомпозиція впливу зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ

Завдяки зробленій декомпозиції можна визначити ключові особливості впливу зовнішніх та внутрішніх чинників, які випливають з рис. 2, зокрема:

1. Вплив зовнішніх чинників на кібербезпеку ВВНЗ:

– спостерігається залежність реалізації різних типів кібератак від якості розроблення та виробництва апаратно-програмного забезпечення відповідного іноземного виробника, а саме наявність вразливостей (навмисних або ненавмисних);

– за критичністю впливу зовнішніх чинників на кібербезпеку ВВНЗ, надзвичайні ситуації (природня небезпека) є найбільш небезпечними (знизити ефективність їх впливу майже нереально) у порівнянні з іншими зовнішніми чинниками.

2. Вплив внутрішніх чинників на кібербезпеку ВВНЗ:

– спостерігається залежність всіх внутрішніх чинників від підготовки (навченості) особового складу, зокрема від компетентності фахівців залежить якість політики кібербезпеки, топології (архітектури) інформаційного простору, апаратного та програмного забезпечення ВВНЗ. При цьому, політика кібербезпеки ВВНЗ в майбутньому також опосередковано може впливати на підготовку (навченість) особового складу, шляхом закріплення в ній юридичної вимоги щодо постійного формування/розвитку знань, умінь та навичок з питань кіберзахисту.

– за критичністю впливу внутрішніх чинників на кібербезпеку ВВНЗ, підготовка (навченість) особового складу також займає вирішальне значення, зокрема вона є системоутворюючим елементом (без знань неможливо вирішити будь-які наявні проблеми, тим паче питання забезпечення кібербезпеки ВВНЗ).

Таким чином, аналіз зовнішніх та внутрішніх чинників, має стати передумовою для розуміння поточного рівня кібербезпеки вашого ВВНЗ та прийняття відповідних управлінських рішень щодо його підвищення.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, проведений аналіз свідчить, що на кібербезпеку будь-якого ВВНЗ впливають зовнішні та внутрішні чинники. На основі декомпозиції встановлена взаємозалежність (критичність) впливу зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ, що дає змогу системно врахувати всю причинно-наслідкову систему їх зв’язків. Обґрунтовано, що завчасний аналіз впливу зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ дасть змогу отримати ситуаційну обізнаність сучасного стану кібербезпеки та прийняти керівництву відповідні управлінські рішення.

Перспективні напрями подальших досліджень: теоретичне обґрунтування моделі кіберзахисту ВВНЗ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Антонов, Ю. С., Римар, П. В., Антонова, О. Г. (2019). Проблема DoS/DDoS атак навчальних ресурсів студентами. *Сучасний захист інформації*, *4*(40), 52–62.

2 Биков, В. Ю., Буров, О. Ю., Дементієвська, Н. П. (2019). Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання*, *2*(70), 313–331.

3 *Вказана Microsoft програма для знищення даних з високою ймовірністю є складовою кібератаки на державні органи.* Державна служба спеціального зв’язку та захисту інформації України. https://cip.gov.ua/ua/news/vkazana-microsoft-programa-dlya-znishennya-danikh-z-visokoyu-imovirnistyu-ye-chastinoyu-kiberataki-na-derzhavni-organi.

4 Головченко, О., Іщенко, О., Линок, Н. (2021). ЗДОБУТІ УРОКИ ВЕДЕННЯ БОЙОВИХ ДІЙ АРТИЛЕРІЙСЬКИМИ ПІДРОЗДІЛАМИ В ХОДІ ЗБРОЙНОГО КОНФЛІКТУ НА СХОДІ УКРАЇНИ ЗА АСПЕКТОМ ЖИВУЧОСТІ В 2014–2015 РОКАХ. *Воєнно-історичний вісник*, *39*(1), 82–96. https://doi.org/10.33099/2707-1383-2021-39-1-82-96.

5 Ільїн, О. О., Сєрих, С. О., Вишнівський, В. В. (2017). Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки. *Сучасний захист інформації*, (1), 66–72.

6 Кива, В. Ю. (2019). Інформаційно-комунікаційна компетентність викладачів системи військової освіти: поняття, зміст і структура. *Вісник Черкаського університету. Серія «Педагогічні науки»*, (1), 287–293.

7 Кива, В. Ю. (2020). *Розвиток інформаційно-комунікаційної компетентності викладачів системи військової освіти у процесі дистанційного навчання* [Дис. д-ра філософії в галузі педагогіки].

8 Кива, В. Ю. (2018). Розвиток інформаційно-комунікаційної компетентності викладачів системи військової освіти як методологічна проблема. *Адаптивне управління: теорія і практика. Педагогіка*, *5*(9), 1–20.

9 Кириленко, Н. М. (2012). Проблеми інформаційної безпеки освітнього середовища вищого навчального закладу. *Інформаційно-телекомунікаційні технології в сучасній освіті*, 149–151.

10 Нашинець-Наумова, А. Ю., Бурячок, В. Л., Коршун, Н. В., Жильцов, О. Б., Складанний, П. М., Кузьменко, Л. В. (2020). Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання*, *77*(3), 337–354.

11 Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2017) (Україна).

12 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави", Указ Президента України № 446/2021 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/446/2021#Text.

13 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", Указ Президента України № 447/2021 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/447/2021#Text.

14 Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України", Указ Президента України № 473/2021 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/473/2021#Text.

15 Репіло, Ю., Головченко, О., Іщенко, О. (2021). КОНТЕНТ-АНАЛІЗ УРОКІВ ЗБРОЙНОГО КОНФЛІКТУ В НАГІРНОМУ КАРАБАСІ ЩОДО ВОГНЕВОЇ ПІДТРИМКИ ВІЙСЬКОВИХ ФОРМУВАНЬ АЗЕРБАЙДЖАНУ В НАСТУПАЛЬНИХ ДІЯХ. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*, *84*(1), 86–99. https://doi.org/10.32453/3.v84i1.805.

16 СБУ викрила генерал-майора, який працював на ФСБ РФ. https://ssu.gov.ua/novyny/7448.

17 Чубукова, О. Ю., Пономаренко, І. В. (2018). Інформаційна безпека у навчальних закладах України. *Вісник Київського національного університету технологій та дизайну*, *Спец. Випуск*, 388–395.

18 Шпигунські ігри. https://www.radiosvoboda.org/a/ezgov-derzgzrada-sud-hpygun/30038712.html.

19 Ягупов, В. В., Кива, В. Ю. (2019). Критерії та показники діагностування розвиненості інформаційно-комунікаційної компетентності викладачів системи військової освіт. *Інформаційні технології і засоби навчання*, 71(3), 248–266.

20 Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L. (2016). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

21 Bianchi, I. S., Sousa, R. D. (2016). IT Governance Mechanisms in Higher Education. *Procedia Computer Science*, *100*, 941–946. https://doi.org/10.1016/j.procs.2016.09.253.

22 (2020). Cost of a Data Breach Report. *Ponemon Institute and IBM*. www.ibm.com/downloads/cas/RZAX14GX.

23 DDoS Attacks Are Already Creating Chaos While Schools and Universities Are Reopening During the Pandemic. https://www.netscout.com/sites/default/files/2020-09/NETSCOUT_DDoS_Attacks_Are_Already_Creating_Chaos_While_Schools.pdf.

24 Ghazvini, A., Shukur, Z., & Hood, Z. (2018). Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. *International Journal of Advanced Computer Science and Applications*, *9*(8), 410–423. https://doi.org/10.14569/ijacsa.2018.090853.

25 Golovchenko, O. (2020).Content-analysis of trends of waging warfare by the army of the armed forces of the Russian Federation. *Sciences of Europe*, *2*(58), 54–61.

26 Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015.

27 He, X. H., Chun, Z. Z., Zhao, Z. Z. (2011). Discussion on security protection framework of classified protection construction. *Communications Technology*, *44*(12), 98–100.
28 Hina, S., Dominic, P. D. (2020). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201–211.
29 Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.
30 Jeske, D., Schaik, P. V. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, (66), 129–141.
31 Joshi, C., Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, (35), 128–137.
32 Kearney, W. D., Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, (61), 46–58.
33 Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248.
34 Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. У *2012 International Conference on Innovations in Information Technology (IIT)*. IEEE. https://doi.org/10.1109/innovations.2012.6207742.
35 Ogutcu, G., Testik, O. M. , Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, (56), 83–93.
36 Rajab, M. (2019). *The relevance of social and behavioral models in determining intention to comply with information security policy in higher education environments*. Eastern Michigan University.
37 Rehman, H., Masood, A., Cheema, A. R. (2013). Information Security Management in academic institutes of Pakistan. У *2013 2nd National Conference on Information Assurance (NCIA)*. IEEE. https://doi.org/10.1109/ncia.2013.6725323.
38 Saeed, N., Bader, A., Al-Naffouri, T. Y., Alouini, M.-S. (2020). When Wireless Communication Responds to COVID-19: Combating the Pandemic and Saving the Economy. *Frontiers in Communications and Networks*, *1*. https://doi.org/10.3389/frcmn.2020.566853.
39 Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis of IT Assessment Security Maturity in Higher Education Institution. *Information Science and Applications*, 701–713.
40 Ulven, J. B., Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039.
41 Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019.
42 Yustanti, W., Qoiriah, A., Bisma, R., Prihanto, A. (2018). An analysis of Indonesia's information security index: a case study in a public university. *IOP Conference Series: Materials Science and Engineering*, *296*, 012038. https://doi.org/10.1088/1757-899x/296/1/012038.
43 Zeng, Y., Zhang, H., Liu, X., Fu, Y., Deng, Q., Ye, R. (2019). Information system and management for campus safety. У *SIGSPATIAL '19: 27th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM. https://doi.org/10.1145/3356998.3365760.
44 Zhang, J., Reithel, B. J., Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340. https://doi.org/10.1108/09685220910993980.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

Vladyslav Yu. Kyva
PhD of Pedagogical Sciences,
Student of the Institute of Troops and (Forces) Support and Information Technologies
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID: 0000-0002-6689-7530
kyvavlad30101991@gmail.com

ANALYSIS OF FACTORS AFFECTING CYBER SECURITY OF A HIGHER MILITARY EDUCATIONAL INSTITUTION

Abstract. The impact of the development and dissemination of information and communication technologies (ICT) in higher military educational institutions (HMEI) is considered in the article, as on the one hand, it increases its efficiency and promotes the training of highly qualified personnel (tactical, operational and strategic level of military education) for the Security Sector and defense of Ukraine, which is extremely necessary in the case of armed aggression by the Russian Federation, and on the other hand, it makes its information space vulnerable to cyberattacks, which the issue of cybersecurity of HMEI raises. At the same time, the author focuses on the analysis of cyber-attacks on educational institutions in recent years, which are due to the development of methods (means) of their implementation and wide access to them by various users, including attackers. In addition, Distributed Denial of Service (DDoS) cyber-attack is the most common cyber threat to international educational institutions, according to an analytical report by Netscout (a developer of ICT solutions to combat DDoS cyberattacks in the United States). It has been analyzed that criminals have recently used DDoS cyberattacks to extort money. Moreover, DDoS cyberattacks were aimed at banks, stock exchanges, travel agencies, currency exchanges and educational institutions. Therefore, the cybersecurity of HMEI needs constant attention from the participants of its provision. In addition, the analysis shows that the cybersecurity of any university is influenced by external and internal factors, which confirm the relevance of the chosen area of research. Therefore, the cybersecurity of HMEI requires an analysis of the factors that affect it, in order to choose the best option for its implementation. Accordingly, the essence and main features of the impact of factors on the cybersecurity of HMEI are identified and their characteristics are presented. The influence of factors on the cybersecurity of HMEI has been decomposed, in particular on the interdependence and criticality of their impact. The necessity of taking into account and constant monitoring of the influence of external and internal factors on the cybersecurity of HMEI is substantiated, which allows to get situational awareness of the current state of cybersecurity and to make appropriate decisions to the management.

Keywords: higher military educational institution; information and communication technologies; factors; cybersecurity; cyberattacks.

REFERENCES (TRANSLATEDAND TRANSLITERATED)

1 Antonov, Yu. S., Rymar, P. V., Antonova, O. H. (2019). Problema DoS/DDoS atak navchalnykh resursiv studentamy. Suchasnyi zakhyst informatsii, 4(40), 52–62.
2 Bykov, V. Yu., Burov, O. Yu., Dementiievska, N. P. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi. Informatsiini tekhnolohii i zasoby navchannia, 2(70), 313–331.
3 Vkazana Microsoft prohrama dlia znyshchennia danykh z vysokoiu ymovirnistiu ye skladovoiu kiberataky na derzhavni orhany. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. https://cip.gov.ua/ua/news/vkazana-microsoft-programa-dlya-znishennya-danikh-z-visokoyu-imovirnistyu-ye-chastinoyu-kiberataki-na-derzhavni-organi.
4 Holovchenko, O., Ishchenko, O., Lynok, N. (2021). ZDOBUTI UROKY VEDENNIa BOIOVYKh DII ARTYLERIISKYMY PIDROZDILAMY V KhODI ZBROINOHO KONFLIKTU NA SKhODI UKRAINY ZA ASPEKTOM ZhYVUChOSTI V 2014–2015 ROKAKh. Voienno-istorychnyi visnyk, 39(1), 82–96. https://doi.org/10.33099/2707-1383-2021-39-1-82-96.

5 Ilin, O. O., Sierykh, S. O., Vyshnivskyi, V. V. (2017). Analiz urazlyvosti informatsiinoho resursu vyshchoho navchalnoho zakladu ta klasyfikatsiia zahroz informatsiinoi bezpeky. Suchasnyi zakhyst informatsii, (1), 66–72.
6 Kyva, V. Yu. (2019). Informatsiino-komunikatsiina kompetentnist vykladachiv systemy viiskovoi osvity: poniattia, zmist i struktura. Visnyk Cherkaskoho universytetu. Seriia «Pedahohichni nauky», (1), 287–293.
7 Kyva, V. Yu. (2020). Rozvytok informatsiino-komunikatsiinoi kompetentnosti vykladachiv systemy viiskovoi osvity u protsesi dystantsiinoho navchannia [Dys. d-ra filosofii v haluzi pedahohiky].
8 Kyva, V. Yu. (2018). Rozvytok informatsiino-komunikatsiinoi kompetentnosti vykladachiv systemy viiskovoi osvity yak metodolohichna problema. Adaptyvne upravlinnia: teoriia i praktyka. Pedahohika, 5(9), 1–20.
9 Kyrylenko, N. M. (2012). Problemy informatsiinoi bezpeky osvitnoho seredovyshcha vyshchoho navchalnoho zakladu. Informatsiino-telekomunikatsiini tekhnolohii v suchasnii osviti, 149–151.
10 Nashynets-Naumova, A. Yu., Buriachok, V. L., Korshun, N. V., Zhyltsov, O. B., Skladannyi, P. M., Kuzmenko, L. V. (2020). Tekhnolohiia zabezpechennia informatsiinoi i kiberbezpeky v zakladakh vyshchoi osvity Ukrainy. Informatsiini tekhnolohii i zasoby navchannia, 77(3), 337–354.
11 Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, Zakon Ukrainy № 2163-VIII (2017) (Ukraina).
12 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro nevidkladni zakhody z kiberoborony derzhavy", Ukaz Prezydenta Ukrainy № 446/2021 (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/446/2021#Text.
13 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy", Ukaz Prezydenta Ukrainy № 447/2021 (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/447/2021#Text.
14 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku "Pro Stratehichnyi oboronnyi biuleten Ukrainy", Ukaz Prezydenta Ukrainy № 473/2021 (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/473/2021#Text.
15 Repilo, Yu., Holovchenko, O., Ishchenko, O. (2021). KONTENT-ANALIZ UROKIV ZBROINOHO KONFLIKTU V NAHIRNOMU KARABASI ShchODO VOHNEVOI PIDTRYMKY VIISKOVYKh FORMUVAN AZERBAIDZhANU V NASTUPALNYKh DIIaKh. Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia: viiskovi ta tekhnichni nauky, 84(1), 86–99. https://doi.org/10.32453/3.v84i1.805.
16 SBU vykryla heneral-maiora, yakyi pratsiuvav na FSB RF. https://ssu.gov.ua/novyny/7448.
17 Chubukova, O. Yu., Ponomarenko, I. V. (2018). Informatsiina bezpeka u navchalnykh zakladakh Ukrainy. Visnyk Kyivskoho natsionalnoho universytetu tekhnolohii ta dyzainu, Spets. Vypusk, 388–395.
18 Shpyhunski ihry. https://www.radiosvoboda.org/a/ezgov-derzgzrada-sud-hpygun/30038712.html.
19 Iahupov, V. V., Kyva, V. Yu. (2019). Kryterii ta pokaznyky diahnostuvannia rozvynenosti informatsiino-komunikatsiinoi kompetentnosti vykladachiv systemy viiskovoi osvit. Informatsiini tekhnolohii i zasoby navchannia, 71(3), 248–266.Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L. (2016). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040
20 Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L. (2016). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040
21 Bianchi, I. S., Sousa, R. D. (2016). IT Governance Mechanisms in Higher Education. *Procedia Computer Science*, *100*, 941–946. https://doi.org/10.1016/j.procs.2016.09.253.
22 (2020). Cost of a Data Breach Report. *Ponemon Institute and IBM*. www.ibm.com/downloads/cas/RZAX14GX.
23 DDoS Attacks Are Already Creating Chaos While Schools and Universities Are Reopening During the Pandemic. https://www.netscout.com/sites/default/files/2020-09/NETSCOUT_DDoS_Attacks_Are_Already_Creating_Chaos_While_Schools.pdf.
24 Ghazvini, A., Shukur, Z., & Hood, Z. (2018). Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. *International Journal of Advanced Computer Science and Applications*, *9*(8), 410–423. https://doi.org/10.14569/ijacsa.2018.090853.
25 Golovchenko, O. (2020).Content-analysis of trends of waging warfare by the army of the armed forces of the Russian Federation. *Sciences of Europe*, *2*(58), 54–61.
26 Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015.

27 He, X. H., Chun, Z. Z., Zhao, Z. Z. (2011). Discussion on security protection framework of classified protection construction. *Communications Technology*, *44*(12), 98–100.
28 Hina, S., Dominic, P. D. (2020). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201–211.
29 Jang-Jaccard, J., Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993.
30 Jeske, D., Schaik, P. V. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security*, (66), 129–141.
31 Joshi, C., Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, (35), 128–137.
32 Kearney, W. D., Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, (61), 46–58.
33 Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248.
34 Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. У *2012 International Conference on Innovations in Information Technology (IIT)*. IEEE. https://doi.org/10.1109/innovations.2012.6207742.
35 Ogutcu, G., Testik, O. M. , Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, (56), 83–93.
36 Rajab, M. (2019). *The relevance of social and behavioral models in determining intention to comply with information security policy in higher education environments*. Eastern Michigan University.
37 Rehman, H., Masood, A., Cheema, A. R. (2013). Information Security Management in academic institutes of Pakistan. У *2013 2nd National Conference on Information Assurance (NCIA)*. IEEE. https://doi.org/10.1109/ncia.2013.6725323.
38 Saeed, N., Bader, A., Al-Naffouri, T. Y., Alouini, M.-S. (2020). When Wireless Communication Responds to COVID-19: Combating the Pandemic and Saving the Economy. *Frontiers in Communications and Networks*, *1*. https://doi.org/10.3389/frcmn.2020.566853.
39 Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis of IT Assessment Security Maturity in Higher Education Institution. *Information Science and Applications*, 701–713.
40 Ulven, J. B., Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039.
41 Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019.
42 Yustanti, W., Qoiriah, A., Bisma, R., Prihanto, A. (2018). An analysis of Indonesia's information security index: a case study in a public university. *IOP Conference Series: Materials Science and Engineering*, *296*, 012038. https://doi.org/10.1088/1757-899x/296/1/012038.
43 Zeng, Y., Zhang, H., Liu, X., Fu, Y., Deng, Q., Ye, R. (2019). Information system and management for campus safety. У *SIGSPATIAL '19: 27th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM. https://doi.org/10.1145/3356998.3365760.
44 Zhang, J., Reithel, B. J., Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, *17*(4), 330–340. https://doi.org/10.1108/09685220910993980.