УДК 37:004:316.772.5

Биков Валерій Юхимович
доктор технічних наук, професор, академік НАПН України, директор
Інститут інформаційних технологій і засобів навчання НАПН України, м. Київ, Україна
ORCID ID 0000-0002-5890-6783
valbykov@gmail.com

Буров Олександр Юрійович
доктор технічних наук, провідний науковий співробітник
Інститут інформаційних технологій і засобів навчання НАПН України, м. Київ, Україна
ORCID ID 0000-0003-0733-1120
ayb@iitlt.gov.ua

Дементієвська Ніна Петрівна
науковий співробітник
Інститут інформаційних технологій і засобів навчання НАПН України, м. Київ, Україна
ORCID ID 0000-0002-5450-6635
dementievska@iitlt.gov.ua

КІБЕРБЕЗПЕКА В ЦИФРОВОМУ НАВЧАЛЬНОМУ СЕРЕДОВИЩІ

Анотація. У статті розглянуто проблеми кібербезпеки учасників освітнього процесу, акцентується увага на тому, що ці проблеми не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони мають охоплювати такі види захисту, як правові, технічні, інформаційні, організаційні та психологічні, оскільки в останні роки населення в цілому та особливо діти й молодь усе частіше стають об'єктами кібератак, найбільш уразливою (слабкою) ланкою мережі. У людино центричних мережах, що становлять постійно зростаючу частку серед загальних мереж, сама мережа набуває нових властивостей, діючи як самостійний складник (на додаток до таких факторів, як вузол мережі, інтерфейс і зв'язки між вузлами). Загрози учасникам навчального процесу з боку кіберпростору доцільно розглядати як пасивні та активні, розробляючи адекватні засоби захисту та життєстійкості системи "суб'єкт освітнього процесу-засоби навчання-середовище". Найбільш значущими серед кіберзагроз для учасників навчально-виховного процесу відзначаються методи соціальної інженерії, знання яких та протидія яким можуть бути найбільш ефективними для забезпечення кібербезпеки. Як складником підготовки учасників навчального процесу з питань кібербезпеки пропонується використовувати "кібер-вакцинацію", тобто формування усвідомленого чуттєвого досвіду перебування під дією кіберзагрози та протидія їй системою заходів, які охоплюють, крім традиційних методів, тренувальні "кібератаки", а також формування знань і вмінь стійкості (відновлення) стосовно кіберзагроз. Учасникам освітнього процесу пропонується подальші дослідження проблеми зосередити на детальному розробленні видів загроз, а також методам протидії. Особливе місце має зайняти проблематика стійкості до кібер-небезпек, яка може використовувати досвід підготовки операторів емерджентних галузей, у тому числі діагностування поточного стану людини та необхідне коригування з метою оптимізації її діяльності.

Ключові слова: кібербезпека; цифрове середовище; навчальна діяльність; людський чинник; когнітивна небезпека; соціальна інженерія.

1. ВСТУП

Люди живуть та діють у цифровому просторі (ЦП). Діти народжуються, зростають, навчаються і працюватимуть з гаджетами, що під'єднані до мереж і стають природним середовищем. Їх життя знаходиться під впливом і дією ЦП зі старими та новими небезпеками, залежить все більше від когнітивних факторів (інтерфейсу, вмісту, моделей поведінки) і може характеризуватися з позицій безпеки, ефективності

© В. Ю. Биков, О. Ю. Буров, Н. П. Дементієвська, 2019.

та комфортності (зокрема здоров'я), тобто знаходиться в полі діяльності ергономістів [1]. Виникають нові проблеми, викликані життям і діяльністю в ЦП, відповідними факторами впливу, способами їх уникнення та відповідними новими засобами та інструментами. Відповідно потребують вирішення проблеми розвитку та впровадження інформаційно-комунікаційних технологій (ІКТ) в освіті, на чому акцентується увага як на міжнародному [2], так і національному рівнях [3]. Проте слід враховувати, що «під впливом новітніх інформаційних технологій відбуваються процеси трансформації суспільного розвитку настільки фундаментальні й глобальні, що, крім позитивного впливу, закономірно несуть з собою серйозні проблеми, загрози і ризики в разі недооцінки нових факторів і умов» [4, с. 191]. Як відзначалось у матеріалах Міжнародних Форумів у Давосі (2018–2019 рр.), особливої гостроти набуває проблема кібербезпеки (КБ), яка стосується практично всіх сфер життя та діяльності людини, особливо в умовах повної інформатизації освіти. Через кібератаки людство зазнає збитків більше ніж на 400 млрд. доларів США за рік.

Постановка проблеми. Ключові проблеми інформатизації освіти в Україні визначені в Національній доповіді 2016 р.: «Про стан і перспективи розвитку освіти в Україні» [3, с.159]: формування і широке впровадження єдиного освітнього інформаційного простору України та забезпечення належного наукового супроводу цих процесів; розгортання та удосконалення необхідних елементів інфраструктури регіональних інформаційних і телекомунікаційних мереж, взаємопов’язаних як між собою, так і з глобальною мережею Інтернет; низький рівень ІКТ та інформатичних компетентностей населення; фактична несформованість цілісної національної політики застосування ІКТ в освіті, недостатня правова база. Нові виклики часу та нові напрями розвитку суспільства – Суспільство 4.0, Освіта 4.0 [5], проникнення найновіших технологій у всі сфери життя, «гібридна» війна – вимагають зрозуміти ключові проблеми та питання безпеки освітнього процесу в цифровому просторі, зокрема безпеку всіх безпосередніх учасників, організаторів освіти, держави, а також безпеку змісту навчання.

Законом України "Про основні засади забезпечення кібербезпеки України" визначаються основні поняття зазначеної проблемної галузі [6]. Зокрема, Стаття 1 Закону визначає кібербезпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Водночас Стаття 2 Закону пояснює: «1. Цей Закон не поширюється на: 1) відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; ... 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів; …». Інакше кажучи, чинний Закон не передбачає будь-які дії з безпеки стосовно людини, яка не входить до критичної інформаційної інфраструктури держави, а людський складник інтелектуального капіталу (який набуває зростаючого значення в усьому світі) не входить до критичного ресурсу України. І це в той час, коли в усьому світі основна боротьба йде за людські та інтелектуальні ресурси, тобто за тих, хто вже завтра буде забезпечувати конкурентоспроможність країни.

Аналіз останніх досліджень і публікацій. Із охопленням інформатизацією всіх сфер життя людини значення кібербезпеки вийшло на рівень компетентності з питань

безпеки життєдіяльності людини і навіть перевищило його. За даними 2017 Norton Cyber Security Insights Report, 978 млн. громадян країн G-20 у 2017 р. стали жертвами кіберзлочинності. З метою запобігання цьому явищу приймаються національні та регіональні програми [7], створюються міжнародні центри [8], приймаються програми спільної дії [9], затверджуються стандарти [10]. За оцінками світових експертів у 2016 р., світові витрати на кібербезпеку перевищували 70 млрд. дол. США на рік із щорічним зростанням на 10-15%. Зокрема, за даними експертів Gartner, Inc. зростання таких витрат у 2018 р. очікувалися в розмірі до 93 млрд. дол. США [11].

Програмними документами ООН визначалося, що потрібна глобальна культура кібербезпеки, яка буде вимагати від усіх учасників врахування наступних дев'яти взаємодоповнюючих елементів [12]: a) поінформованість; b) відповідальність; c) реагування; d) етика; e) демократія; f) оцінка ризику; g) проектування і впровадження засобів забезпечення безпеки; h) управління забезпеченням безпеки; i) переоцінка. Відповідно, головними напрямами розробки питань з кібербезпеки вважалися інформаційна безпека, безпека мережі, безпека Інтернету та захист критичних інфраструктур [10], а також захист даних різної природи [13], що відбилося в Законі України "Про основні засади забезпечення кібербезпеки України" 2017 р. [6]. Як наслідок, стрімко зросла підготовка фахівців з кібербезпеки, оскільки їх дефіцит у світі до 2020 р. оцінюється в 1.5 млн. працівників.

В Україні на часі підготовка фахівців з кібербезпеки проводиться у 182 вишах. Як правило, майбутні фахівці і в Україні, і в інших країнах отримують теоретичні знання та практичні навички з програмування, розробки та управління базами даних, формування моделей захисту інформації і політик безпеки, технічного та криптографічного захисту інформації, побудови захищених цифрових TCP/IP мереж і обслуговування сертифікатів відкритих ключів, тестування систем захисту на проникнення, адміністрування захищених інформаційних і комунікаційних систем, проведення їх моніторингу та аудиту тощо [14]. Проте за 5 років після прийняття стандарту ISO [10] почало суттєво змінюватись бачення проблеми кібербезпеки, оскільки людина дедалі більше перестає бути лише суб’єктом кіберзлочинів, перетворюючись на об’єкт сама по собі, а не тільки її фінансові та економічні інтереси та можливості [15]. Так, за даними аналітичної компанії RAND Corporation, структура кібер-ризиків змінилася в останні роки [16]. Усе більше аналітиків звертають увагу на те, що основні причини інцидентів в інтернет-ресурсах у 2017 р. пов’язані з дією людського чинника, масовим зламом IoT-пристроїв та хмарних сервісів. Особливо ця проблема загострюється з посиленням цифрового гуманістичного характеру освіти [17], зростанням ролі соціальних мереж у житті людини в цілому та освіті зокрема [18], а також розумінням людства необхідності переходу до освіти протягом життя [19].

За три останніх роки на терені реформування освіти в багатьох економічно розвинених країнах відбулася розробка ключових документів, що стали орієнтирами для освітян, серед яких розроблена та представлена в країнах ЄС Рамка цифрової компетентності для громадян 2.0-2.1 (Digital Competence Framework for Citizens 2.0-2.1). У Законі про освіту інформаційно-комунікаційна компетентність визначена однією з ключових компетентностей. Питання кібербезпеки є важливими складниками цієї компетентності та відображають загальні підходи, сформульовані в Рамках цифрової компетентності для громадян ЄС.

Мета статті – концептуальна оцінка ключових проблем та завдань кібербезпеки учасників освітнього процесу та можливих загроз у цифровому навчальному середовищі.

2. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ПИТАННЯ КІБЕРБЕЗПЕКИ В ОСВІТІ

Питання кібербезпеки гостро стоять з того часу, як комп'ютерна техніка перестала бути лише прерогативою великих наукових центрів. З появою та поширенням локальних і глобальних мереж змінилося розуміння кібербезпеки, відповідних трендів, проблем і задач. Розглянемо їх з урахуванням трансформації освіти в напрямку цифрової освіти, Освіти 4.0.

2.1. Інформаційно-комунікаційні засоби як фундамент виникнення проблематики кібербезпеки

Сучасне життя все більше і більше будується навколо цифрових мереж, а соціальні медіа стають новим соціальним середовищем [20]. Втручання в ці мережі створює реальну загрозу безпеці в галузі освіти та країни в цілому. Складники (чинники) мережі у спрощеному вигляді можна представити як (рис.1):

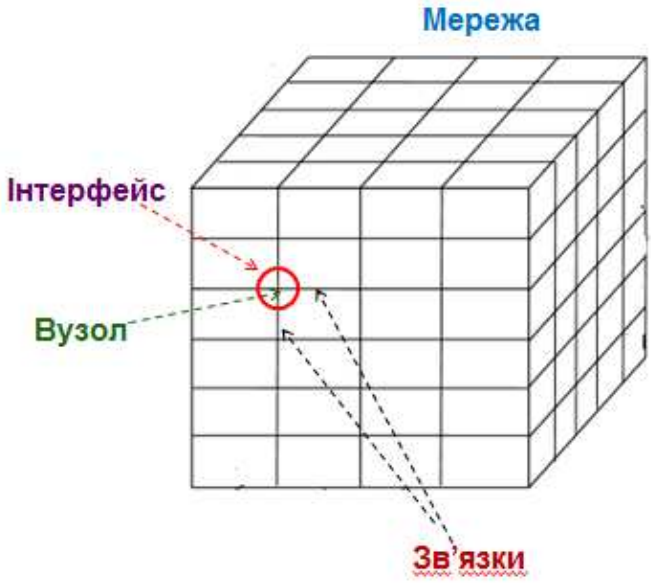

Рис. 1. Фрагмент мережі та її складники (чинники)

У якості вузла можуть виступати «агенти» мережі - *люди* (створювачі ресурсу та його контенту, адміністратори ресурсу, постійні або випадкові користувачі), *технічні* (термінальні станції, комп'ютери, приєднані до мережі гаджети, комунікатори) та *інформаційні* (бази даних, бази знань, керуючі системи тощо) *засоби*.

Усі агенти в залежності від їх природи мають притаманний їм інтерфейс і види зв'язку з іншими агентами. Однак слід зауважити, що одночасно з розвитком технологій побудови мереж, їх ускладненням, використанням штучного інтелекту, появою хмарних і туманних технологій, зростанням потужності баз даних (БД) і баз знань (БЗ) мережа перестала бути просто посередником між користувачами (засобом комунікації). Оскільки інформація в глобальній мережі існує поза окресленим простором і часом, сама мережа стає активним агентом впливу на людину [20], зберігаючи, насамперед, загальнодоступними великі обсяги даних [21]. Будь-який користувач може увійти в мережу (легально або нелегально) та отримати доступ до необхідних вузлів (при використанні хмарних засобів конкретні вузли звичайному користувачу можуть бути невідомими), змінюючи також їх контент (наприклад, Wiki-об'єкт) за дозволеними правилами.

Проте інформація у БД та БЗ за дозволеними правилами може бути змінена або внесена з метою спотворення уявлення користувачів щодо даних, які вони шукають. Певні користувачі мають змогу використовувати це для впливу на широку або цільову аудиторію, «спотворюючи» потрібні вузли (технічної або інформаційної природи) чи впливаючи на них засобами соціальної інженерії (якщо вузол – це людина) [22]. Оскільки мережа є системою зв'язаних вузлів, то пошкоджений («спотворений») вузол може вплинути вже сам по собі на вторинні вузли. Окрім того, спотворена інформація починає існувати в мережі навіть незалежно від людини («агресора»), яка її ввела (рис.2).

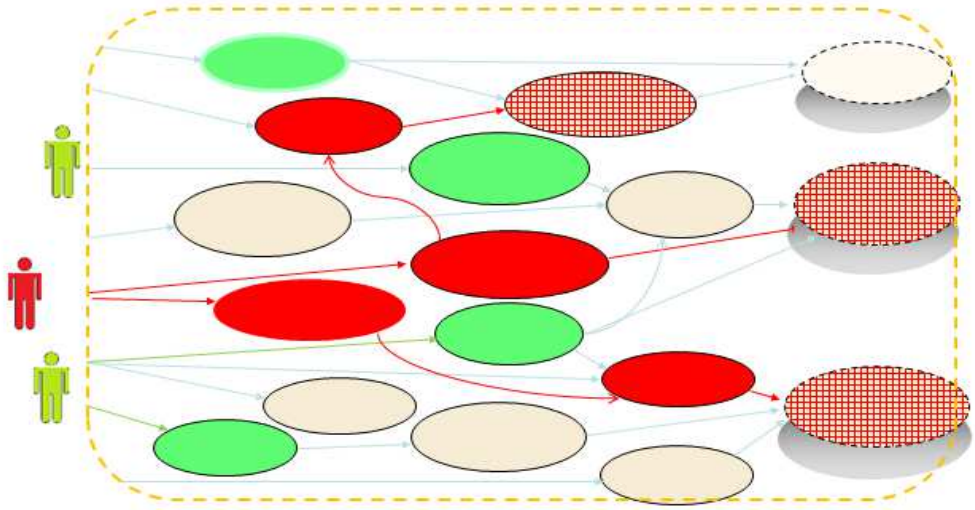

Рис. 2. Приклад активного фрагменту мережі та зовнішніх користувачів (зелений – звичайний, червоний – «агресор»).

У такий спосіб мережа набуває рис самостійного складника (чинника), що впливає на її властивості, функціонування та користувачів, а також систему «людина-техніка-середовище» (СЛТС) в цілому. Усі чотири параметри дії мережі мають певні спільні критичні властивості з точки зору дієвості та впливу на користувача ─ ініціативність, ефективність, стійкість, гнучкість і продуктивність (табл.1). Їх прояв щодо кожного чинника може бути охарактеризований певними показниками, характерними для відповідного параметру, а сукупність показників дозволяє оцінити загальний вплив чинника на мережу як СЛТС.

Таблиця 1

Складники мережі та їх властивості

Властивості	**Вузол**	**Інтерфейс**	**Зв'язок**	**Мережа**
Ініціатива	Усвідомлення інформації	Інформація щодо ситуації	Маршрутизація	Значення/мета
Ефективність	Продуктивність	Юзебіліті	Втрачені пакети	Якість сервісу
Стійкість	Відповідь на стрес	Послідовність	Надійність	Життєздатність
Гнучкість	Здатність до адаптації та змін	Режими відображення	Резервування	Реконфігурація
Продуктивність	Завантаженість	Перешкодостій-кість	Пропускна здатність	Щільність/ Складність

Будь-який розгляд проблем кібербезпеки як самостійного чинника СЛТС є обмеженим і лише частково ефективним, оскільки не враховує зміни, що відбуваються з агентами СЛТС не тільки в часі, але й у просторі, який розширюється з розвитком технологій від локального до глобального. Відповідні зміни відбуваються й стосовно навчального середовища (НС).

2.2. Навчальне середовище та кіберпростір

НС є одним з наріжних каменів освіти. Існує багато різних визначень і класифікацій НС. На наш погляд, «навчальне середовище – це штучно побудована система, структура і складові якої сприяють досягненню цілей навчально-виховного процесу» [23, с.182]. «Доцільно говорити про НС як про оточуюче середовище відносно інтелектуальних складових педагогічної системи - складових, які наділені природним або штучним інтелектом». НС має багатофакторний вплив на суб'єктів навчального процесу, змінюючись як у часі, так і в просторі. Причому це справедливо як для традиційного НС, так і для синтетичного. Відмічається, що «…навчальне середовище у змістовому плані виникає завжди як динамічний процес формування мережі відносин у суб'єкті навчання, до якого (не завжди усвідомлено) вибірково залучаються найрізноманітніші елементи зовнішнього та/або внутрішнього оточення…» [24, с.33], причому такий динамічний процес є характерним для будь-якого НС, але в імерсивному та віртуальному НС набуває ще більшої гостроти через більш глибоке занурення учня в процес навчання.

Різні автори розрізняють природні і штучні, предметні та інформаційно-динамічні, адаптивні та інші НС, використовуючи різні критерії їх типологізації, наприклад, за стилем взаємодії всередині середовища, за характером ставлення до соціального досвіду та його передачі, за ступенем творчої активності, за характером взаємодії із зовнішнім середовищем [24, с.31]. Проте на часі найбільшу увагу привертає цифровий або кіберпростір через загострення проблеми безпеки людини в ньому, насамперед, молодої людини, формування якої тільки відбувається як в особистісному, так і компетентнісному вимірі.

Як визначається Законом "Про основні засади забезпечення кібербезпеки України" [6], «кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних». Звертається увага на те, що кіберпростір визначається різноманіттям з'єднань, що одночасно переводить його в категорію зони ризику. Усі зростаючі розміри, охоплення і функції збільшують можливості як законослухняних громадян, так і ворожих гравців. Супернику необхідно лише атакувати слабку ланку мережі, щоб завоювати новий плацдарм і отримати переваги [25]. Проблеми, що здаються локальними, можуть наростати і швидко поширюватися, створюючи загрози і системні ризики. Уразливість в кіберпросторі є реальною, серйозною і вона швидко розростається. Об'єкти інфраструктури особливої важливості, розвідка, комунікації, командування і контроль, торгівля і фінансові операції, логістика, ліквідація наслідків та готовність до надзвичайних ситуацій повністю залежать від ІТ-систем, об'єднаних у мережі. Порушення кібербезпеки, крадіжка даних та інтелектуальної власності не знають кордонів. Вони впливають на все - від особистої інформації до державних таємниць.

Кіберпростір можна розглядати як тріаду, до якої входять: 1) *інформація* у своєму цифровому представленні: статична (файли, записані на носії інформації) та

динамічна (пакети, потоки, команди, запити тощо); 2) *технічна інфраструктура*: ІКТ, програмне забезпечення, бази даних та бази знань; 3) *інформаційна взаємодія* суб'єктів з використанням отриманої (переданої) інформації та обробки через технічну інфраструктуру.

Як зазначалось вище, це поняття зв'язується Законом з поняттям кібербезпеки як захищеністю «життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору». На міжнародному рівні використовується ряд визначень цього поняття, проте з урахуванням того, що навчання є видом діяльності, можна погодитись з підходом, згідно з яким кібербезпека розглядається як «будь-яка діяльність у мережній, цифровій формі, включаючи зміст інформації та діяльність, що виконується через цифрові мережі» [26]. Ураховуючи, що сьогоднішні школярі народилися в цифрову епоху, зростають, навчаються та розвиваються в значній мірі саме в кіберпросторі, можна стверджувати, що кіберпростір є та залишиться дуже важливою частиною поля битви ідей і цивілізацій. Відповідно перед освітою постають нові завдання, пов'язані не тільки з формуванням у здобувача освіти необхідних знань і соціального самоусвідомлення, але і його розуміння власної інтегрованості у світову спільноту вже на ранніх етапах навчання, практично необмежених можливостей впливу кіберпростору на свою особистість, відповідальності перед собою та суспільством за власну поведінку та її (можливі) глобальні наслідки, знання та розуміння небезпек кіберпростору.

2.3. Загрози учасникам навчального процесу з боку кіберпростору

Спектр небезпек від відкритого кіберпростору постійно розширюється. Якщо десять років тому небезпеки для учнів шкіл можна було звести до відносно невеликої кількості груп – вірусні атаки, кіберзлочинність, небезпеки інтернет-серфінгу [27], – то на часі розмаїття небезпек і загроз зростає постійно, зачіпаючи всі можливі дії людини в мережі. Найбільшу загрозу для школярів мають приховані активні небезпеки [27, с.309].

Мережні загрози.

Активне використання мереж, особливо дітьми та молоддю, супроводжується збільшенням різних видів загроз, що надходять з мережі. Особливо гостро ця проблема виникає при розробці та використанні соціальних мереж. Найбільш активні приховані загрози (для дітей), що походять з комп'ютерної мережі, можуть бути представлені наступною класифікацією [27]:

- вірусні атаки,
- кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо),
- загрози від мережевого серфінгу (кібер-булінг, "дорослий" контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо).

Автори [27] рекомендують розглядати взаємодію школярів та студентів з комп'ютерною мережею як систему "Людина-техніка-середовище". У цій системі комп'ютерна мережа виступає як машина, яка дозволяє нам розглянути вплив мережі на людину як загрозу, що походить від машини. Відповідно, поняття "мережевий ефект" може бути виявлено через поняття "помилка оператора і зниження якості операторської діяльності", "вплив комп'ютерних ігор" та "Інтернет-залежність".

Загрози, що надходять з мереж, можна розділити на наступні *типи:* активні та пасивні, відкриті та приховані, поточні та відкладені.

Використовуючи ергономічний підхід та методологію, можна оцінити активні небезпеки як ієрархічну сукупність показників:

- один інтегрований (комплексний) показник - рівень небезпеки внаслідок дії комп'ютерної мережі; показник - це безрозмірна величина, що входить до оцінок системи верхнього рівня;
- три групових показника - рівень небезпеки, спричинений вірусними нападами; кіберзлочинність й інтернет-серфінг. Показники є безрозмірними величинами і знаходяться на середньому рівні оцінок системи;
- сукупність індивідуальних показників групи однієї чи сукупності загроз; показники також є безрозмірними величинами та відповідають класифікації систем нижчого рівня.

Напрями кібербезпеки.

З огляду на положення Закону України "Про основні засади забезпечення кібербезпеки України" [6] сфера освіти не входить до критичних галузей, на захист яких націлений цей Закон. Проте сьогоднішні учні та студенти в короткий термін можуть працювати в тих галузях. Тому вони вже сьогодні потребують захисту та відповідної підготовки, а також розуміння загальних можливих цільових груп кібербезпеки. Наприклад, за такою класифікацією [15]:

- учні/студенти,
- викладачі,
- діти/молодь,
- населення (в цілому, як соціальне середовище).

У залежності від засобів дії, проблеми (і відповідні засоби) кібербезпеки можна класифікувати за такими групами (або рівнями):

- правові,
- технічні,
- інформаційні,
- організаційні,
- психологічні.

Правовими та технічними питаннями кібербезпеки опікуються спеціалізовані фахівці та організації, тому вони не розглядаються в цій статті.

Інформаційні засоби можуть бути класифіковані залежно від завдань, що вирішуються користувачами:

- захист/засоби захисту,
- інформування,
- зміст,
- навчитися використовувати,
- безпека,
- життєстійкість,
- уникнення загроз.

У широкому розумінні можливими цілями впливу кібербезпеки (крім об'єктів критичної інфраструктури) можуть бути:

- бази даних,
- персональні дані, серед яких фінансові,
- засоби масової інформації,
- соціальні мережі,
- освіта та професійна підготовка,
- підручники, історіографічні видання.

Організаційні засоби вирішення питань кібербезпеки:

- інформування,
- навчання культурі кібербезпеки, професійних працівників КБ і населення в

цілому;
- створення спеціальних засобів КБ,
- розповсюдження засобів КБ,
- контроль використання.

Психологічні засоби можна згрупувати в залежності від особистісного та міжособистісного рівня:
- національний,
- суспільний,
- груповий,
- індивідуальний,
- культурний,
- когнітивний,
- інтелектуальний,
- звички.

Хоча технологічні рішення розробляються у відповідь на кібератаки, зростає поінформованість про те, що роль людської діяльності та прийняття рішень у галузі кібербезпеки має вирішальне значення для підвищення ефективності відповідей на виникаючі загрози. Особливо це важливо з точки зору майбутньої робочої сили, оскільки молодь є особливо чутливою до зовнішнього впливу і є найбільш активною частиною "мережевого населення".

Людський чинник може бути системною слабшою ланкою, але водночас також може бути потужним ресурсом для виявлення та пом'якшення загроз, що виникають. Кілька областей найбільш критичних і невідкладних потреб та прогалин знань, що розглядаються в програмах кібер-досліджень країн НАТО та інших країн, можна визначити як такі: психосоціальні, культурні, концептуальні та організаційні аспекти кібербезпеки.

3. МОЖЛИВОСТІ ТА ШЛЯХИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НАВЧАЛЬНОГО ПРОЦЕСУ

Як свідчать останні дослідження щодо кібербезпеки, інформаційно-технічні засоби в цій сфері постійно вдосконалюються і хакерські атаки переорієнтовуються більше не на техніку, а на людину. Це особливо важливо враховувати через гостроту питання її особистої безпеки та результатів її діяльності. Як показано в [15], «відкриваючись» під час праці в інформаційному середовищі, людина стає не тільки предметом, а об'єктом діяльності інших учасників інформаційного простору. Людська відкритість є результатом цілей діяльності: використовуючи інформацію як інструмент, людина має "доторкнутися" до неї, зв'язатися з нею. У цей момент людина стає відкритою для інформації та вразливою від неї.

3.1. Соціальна інженерія та кібербезпека

Зміщення цілей кіберзлочинності з технічних (інформаційних) об'єктів на людську ланку СЛТС спричинило появу соціальної інженерії (СІ) як методів і технологій отримання необхідного доступу до інформації, заснованих на особливостях психології людей, зокрема - маніпуляція людськими страхами, зацікавленістю або довірою [28].

Основними типами соціальної інженерії на часі можна вважати наступні:

Претекстінг — це набір дій, відпрацьованих за певним, заздалегідь складеним

сценарієм, у результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Для використання цієї техніки зловмисник спочатку збирає певні дані про жертву (ім'я, місце навчання та проживання; дату народження; дані про батьків). Зловмисник спочатку використовує реальні запити з іменами щодо оточення жертви, а після того, як увійде в довіру, отримує необхідну йому інформацію або дії.

Фішинг — техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів авторизаційних даних різних систем. Основним видом фішингових атак є підроблений лист, відправлений жертві електронною поштою, який виглядає як офіційний. У листі міститься форма для введення персональних даних (пін-кодів, логіна і пароля тощо) або посилання на web-сторінку, де розташовується така форма.

Троянський кінь — це техніка ґрунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток, до якого знаходиться «оновлення» антивірусу, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або зміни інформації зловмисником.

Qui pro quo (послуга за послугу) — ця техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці та необхідність їх усунення. У процесі «вирішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко — цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій у загальнодоступних місцях. Для того, щоб виник інтерес до даного носія, зловмисник може нанести на носій логотип відомої популярної компанії.

Байтинг — метод, схожий на попередній, а також фішинг і троянський кінь, проте відрізняється тим, що байтер може запропонувати користувачеві реальну безкоштовну послугу (музику, фільм тощо) в обмін на конфіденційну (приватну) інформацію.

Зворотня соціальна інженерія — даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернутися до зловмисника за «допомогою». Наприклад, створити оборотні неполадки в гаджеті жертви з попереднім інформуванням щодо служби “підтримки”. Користувач у такому випадку зателефонує або зв'яжеться по електронній пошті зі зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

Дружні листи — надсилання електронних листів, у яких особу повідомляють про отримання спадщини, призів, бонусів чи дружнього переказу грошей.

Вішинг — голосова версія фішінгу. Як правило, дії пов'язані з телефонним шахрайством, метою якого є отримання реквізитів банківських карток або будь-якої іншої конфіденційної інформації або змушення жертви перевести гроші на банківський рахунок зловмисника.

Контакти **—** розсилання спаму від імені знайомих. Тобто, заволодівши чиїмось акаунтом, чи то в соціальній мережі, чи в електронній пошті, зловмисники можуть спробувати надсилати від його імені посилання. Психологічна дія, що побудована на схильності людини довіряти своїм знайомим і не дуже вагатися, коли отримують від них пропозицію відкрити посилання.

Засоби СІ широко застосовуються в останні роки для впливу на осіб, що приймають рішення, в політиці та бізнесі. Розроблені та вдосконалюються

рекомендації, методи та засоби протидії їм. Проте практично відсутній розгляд дії та протидії методам СІ стосовно освітньої сфери, незважаючи на те, що діти та підлітки стають все частіше об'єктами атак через Інтернет, а використання засобів протидії для дорослих може бути поширене і на учнів/студентів, але з урахуванням особливостей - вікових та сфери діяльності.

3.2. Суб'єкти навчання та безпечний Інтернет

Основним способом захисту від методів соціальної інженерії є навчання суб'єктів освітнього процесу (СОП). Усі вони (учні, педагоги, організатори навчання) мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації, а також про способи запобігання витоку даних. Крім того, у кожного СОП, в залежності від місця та функції в освітньому процесі, повинні бути інструкції про те, як і на які теми можна спілкуватися із сторонніми особами стосовно персональних особливостей, яку інформацію можна надавати для служби технічної підтримки, як і яку інформацію може повідомити учасник навчального процесу стороннім особам і працівникам мас-медіа. Крім того, можна виділити дев'ять типових правил протидії СІ.

Призначені для користувача облікові дані є власністю навчального закладу. Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали (якщо це має місце), не можна використовувати в інших цілях (на web-сайтах, для особистої пошти тощо), передавати третім особам або іншим співробітникам, які не мають на це права. Наприклад, дуже часто, йдучи у відпустку, співробітник може передати власні авторизовані дані своєму колезі для того, щоб той зміг виконати деяку роботу або подивитися певні дані в момент його відсутності. Персональні дані з результатів тестування та виконання психологічних і медичних обстежень можуть бути застосовані користувачами СІ, тому потребують обережного використання.

Необхідно проводити вступні та регулярні навчання співробітників і учнів, спрямовані на підвищення знань з інформаційної безпеки. Проведення таких інструктажів дозволить СОП мати актуальні дані про існуючі методи соціальної інженерії, а також не забувати основні правила з інформаційної безпеки.

Обов'язковою є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії СОП при виникненні тієї чи іншої ситуації. Наприклад, у регламенті можна прописати, що необхідно робити і куди звертатися при спробі третьої особи запросити конфіденційну інформацію або облікові дані.

На комп'ютерах користувачів завжди має бути актуальне антивірусне програмне забезпечення, а також слід встановити брандмауер.

У корпоративної мережі навчального закладу або об'єднання закладів необхідно використовувати системи виявлення та запобігання атак. Необхідно також використовувати системи запобігання витоку конфіденційної інформації. Усе це дозволить знизити ризик виникнення фішингових атак.

Необхідно максимально обмежити права користувача в системі. Наприклад, можна обмежити доступ до web-сайтів і заборонити використання знімних носіїв, які можуть бути використані за межами навчального закладу.

Необхідно бути пильним щодо джерела, яке запитує конфіденційні дані. Представники Міністерства освіти і науки навряд чи будуть телефонувати до школи, щоб дізнатися дані щодо конкретного учня або студента. Якщо людину просять ввести особисті дані – краще окремо зайти на сайт компанії, наприклад, банку. Ще краще – зателефонувати на офіційний номер установи для уточнення інформації.

Ніколи не слід відкривати вміст додатків або переходити за посиланням, не вивчивши всіх деталей. Часто адреса відправника містить помилки в назвах, а посилання мають неправдоподібний вигляд.

Варто також *критично ставитися до отриманих повідомлень*: наскільки правдоподібною може бути інформація про те, що принц з африканської країни або американський мільярдер міг залишити вам спадщину?

Рекомендується сповіщати про такі небезпеки інших членів сімей, насамперед, літніх людей, які не мають досвіду користування електронними засобами та не обізнані з питань СІ.

Останнім часом в Україні запроваджуються спеціальні навчальні програми і курси для учнів та вчителів, які займаються питаннями безпечного Інтернету [29]. Наприклад, створений і активно використовується вчителями сайт «Онляндія: моя безпечна веб-країна» з матеріалами для дітей, батьків і вчителів; програма Microsoft "Онляндія – безпека в Інтернеті" є популярною серед українських батьків і вчителів. Проте нові кіберзагрози потребують і нових підходів до захисту користувачів, особливо учасників освітнього процесу.

Для викладачів закладів освіти особливого значення набуває не тільки знання критеріїв надійності джерел та достовірності даних і засобів їх оцінювання, а й використання ефективних педагогічних технологій формування відповідних умінь учнів і студентів, а також засоби оцінювання рівня розвитку таких умінь.

3.3. "Когнітивна вакцинація"

20 грудня 2002 р. Генеральною Асамблеєю ООН була прийнята резолюція 57/239 "Елементи для створення глобальної культури кібербезпеки", якою визначені дев'ять основоположних взаємодоповнюючих елементів, що формують глобальну культуру кібербезпеки [30]:

- поінформованість;
- відповідальність;
- реагування;
- етика;
- демократія;
- оцінка ризику;
- проектування та впровадження засобів забезпечення безпеки;
- управління забезпеченням безпеки;
- переоцінка.

Ці елементи стосуються всіх чотирьох зазначених у розділі 2 груп засобів — інформаційних (1, 6 та 9), технічних (3 та 7), організаційних (5, 8) і психологічних (2, 4). Водночас можна зауважити, що психологічні засоби (які безпосередньо стосуються кожної конкретної людини) передбачають лише поведінкові аспекти: відповідальність та етику, тобто прояв соціального ставлення людини до кібербезпеки. Проте на пізнавальному (когнітивному) аспекті, який є формуючим щодо поведінки людини, увага не зосереджується, тобто людина розглядається як відносно пасивний елемент системи забезпечення кібербезпеки. У той же час, оскільки жодні засоби не гарантують 100% захисту людини, доцільно визначити спектр можливостей самої людини до формування особистісного захисту, окрім зазначених вище.

Аналіз програм педагогічних навчальних закладів країни показав, що при вивченні методики викладання навчальних предметів важливим є формування *критичного мислення* учнів у зв'язку з використанням Інтернету [31].

У той же час вирішення питання безпеки учнів в Інтернеті в розвинених країнах

світу, де Інтернет широко використовується в навчальній і науковій діяльності, відзначається комплексним підходом і проблема безпеки тісно пов'язана з питаннями формування власної відповідальності учня за свої дії чи бездіяльність в мережі для уникнення та/або зменшення ризиків. Так, наприклад, у США, Німеччині, Канаді, Фінляндії та інших країнах учні разом з батьками і представниками школи підписують спеціальні угоди про *безпечне* та *відповідальне* використання Інтернету. В таких угодах окремо узгоджені і прописані обов'язки безпечного і відповідального використання соціальних мереж усіма учасниками навчального процесу.

Найбільш дієвий спосіб боротися з проблемами кіберзагроз - зрозуміти їх сутність і змінити поведінку. Правила безпеки прості та відомі, потрібно їх застосовувати. В першу чергу, варто придивитися до дій і зрозуміти, які небезпечні дії робите ви та інші СОП. Наприклад, клікаєте по посиланнях, покладаючись на те, що антивірусний захист забезпечить кібер-недоторканність ? На жаль, жодні технічні засоби з арсеналу кібербезпеки не є гарантією, особливо якщо метою небезпечної дії є людина як така.

У кіберзагрозливому світі важливе місце повинно зайняти *тренування* всіх учасників мережевої діяльності щодо можливого впливу кібер-середовища. Загальна та специфічна інформація щодо кіберзагроз і можливих наслідків їх впливу на життя та діяльність людини необхідно підкріплювати моделюванням тих чи інших ситуацій, що можуть виникати в користувача Інтернету.

Ефективним засобом формування у викладачів і студентів безпечної та відповідальної поведінки при використанні інтернет-ресурсів є проведення спеціальних тренінгових занять з критичного оцінювання надійності джерел і достовірності даних, що публікуються в мережі. Інструменти і засоби такого оцінювання, методичні рекомендації з формування і розвитку таких навичок у користувачів різних вікових категорій розміщені на веб-ресурсі "Критичне оцінювання ресурсів Інтернету для вчителів і учнів" (http://goo.gl/wvoRT3), за матеріалами якого проведено 48 тренінгів для викладачів закладів освіти різного рівня. На цьому постійно обновлюваному ресурсі розміщені приклади уроків і форм оцінювання рівня розвитку вміння критично оцінювати веб-сайти, статті і зображення, які публікуються в Інтернеті.

Найбільш ефективним підходом можна вважати використання комп'ютерного моделювання кіберзагроз у відносно замкнених системах - корпоративних, навчальних. Як рекомендують фахівці, якщо Ви займаєтеся питаннями безпеки - «тренувальні» атаки, насправді є корисним способом. «Але його слід застосовувати правильно. Не просто ділити співробітників на тих, хто відчув підступ, і тих, хто попався. Обов'язково потрібно донести до інших суть їхніх помилок і те, як не робити їх в майбутньому. Ще можна дізнатися, як саме визначили небезпеку ті, хто пройшов перевірку». Прикладами можуть бути: моделювання несанкціонованого розповсюдження приватної інформації щодо конкретної особи в моделюючому середовищі (при використанні реальної інформації з соціальних мереж, яку багато хто необачно розміщує там); моделювання фішингу тощо.

Оскільки забезпечити повний захист практично неможливо, то важливим є тренування *стійкості* користувачів до дії кіберзагроз, тобто навчання "кібер-виживанню", що полягає в умінні розпізнати загрозу або можливу небезпечну дію мережі та раціональній компенсації цієї дії - як психологічної, так і поведінкової (зокрема звернення до відповідних фахівців, за неможливості самостійних відновлюваних дій на початковому етапі навчання). Певною мірою таке навчання подібне до навчання заходам першої невідкладної допомоги при ушкодженні здоров'я.

Інтегровану підготовку за зазначеними напрямами можна вважати "когнітивною вакцинацією", тобто формуванням усвідомленого чуттєвого досвіду перебування під дією кіберзагрози та протидії їй.

Слід зазначити, що ефективно вирішувати питання забезпечення кібербезпеки можливо лише при системному використанні засобів усіх структурних рівнів, враховуючи питому вагу кожного з них для конкретної цільової групи та/або сфери застосування відповідної людиноцентричної системи.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

1. Проблеми кібербезпеки не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони мають включати такі види захисту: правові, технічні, інформаційні, організаційні та психологічні.
2. На часі доцільно виокремити роль психологічних засобів забезпечення кібербезпеки, оскільки населення в цілому та особливо діти і молодь все частіше стають об'єктами кібератак, найбільш уразливою (слабкою) ланкою мережі.
3. У людиноцентричних мережах, що становлять постійно зростаючу частку серед загальних мереж, сама мережа набуває нових властивостей, діючи як самостійний фактор (на додаток до таких факторів, як вузол мережі, інтерфейс і зв'язки між вузлами).
4. Загрози учасникам навчально-виховного процесу з боку кіберпростору доцільно розглядати як пасивні та активні, розробляючи адекватні засоби захисту та життєстійкості системи “суб'єкт освітнього процесу-засоби навчання-середовище”.
5. Найбільш значущими серед кіберзагроз для учасників навчального процесу є методи соціальної інженерії, знання яких та протидія яким можуть бути найбільш ефективними для забезпечення кібербезпеки.
6. Як складником підготовки учасників навчально-виховного процесу з питань кібербезпеки пропонується використовувати “кібер-вакцинацію”, тобто формування усвідомленого відчуттєвого досвіду перебування під дією кіберзагрози та протидії їй як систему тренувальних заходів, які включають, крім традиційних методів, тренувальні “кібератаки”, а також формування знань і вмінь стійкості (відновлення) стосовно кіберзагроз.

Подальші дослідження проблеми доцільно зосередити на детальному вивченні структури кіберзагроз учасниками освітнього процесу, а також методам протидії. Особливе місце має зайняти проблематика стійкості до кібер-небезпек, яка може використовувати досвід підготовки операторів емерджентних галузей, насамперед, діагностування поточного стану людини та необхідне коригування з метою оптимізації її діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] ДСТУ 3899-99. Дизайн та ергономіка. Терміни та визначення. Київ, Держстандарт України, 33, 1999 (in Ukrainian).
[2] «Education and Training 2020 Work programme. Thematic Working Group 'Assessment of Key Competences' Literature review, Glossary and examples». European Commission, Directorate-General for Education and Culture, November, 52, 2012 .
[3] Національна доповідь про стан і перспективи розвитку освіти в Україні. НАПН України, К.: Педагогічна думка, 448 с., 2016.
[4] В. Ю. Биков, О. М. Спірін, та О. П. Пінчук, “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.
[5] В.Ю.Биков, Суспільство знань і освіта. [Електронний ресурс]. Доступно:https://www.youtube.com/watch?v=cDIytlESUz4. Дата звернення: 22.03.2019.

[6] Закон № 2163-VIII “Про основні засади забезпечення кібербезпеки України” (Відомості Верховної Ради), № 45, с. 403, 2017.
[7] European Commission, Digital Single Market News, “EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity — Cybersecurity Strategy and Proposal for a Directive”, February 7, 2013.
[8] NATO Cooperative Cyber Defense Centre of Excellence. [Електронний ресурс]. Доступно: https://ccdcoe.org/ . Дата звернення: 17.08.2018.
[9] B. Lété, and P. Pernik, “EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions”. The German Marshall Fund of the United States. Policy Brief, # 38, 2017.
[10] ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity, 50 pp., 2012
[11] “Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017”. [Електронний ресурс]. Доступно:https://www.gartner.com/en/newsroom/press-releases/2017-08-16-gartner-says-worldwide-information-security-spending-will-grow-7-percent-to-reach-86-billion-in-2017. Дата звернення: 17.08.2018.
[12] “Элементы для создания глобальной культуры кибербезопасности. Документы ООН”. [Електронний ресурс]. Доступно: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml
[13] А. И. Згоба, Д. В. Маркелов, та П. И. Смирнов, «Кибербезопасность: угрозы, вызовы, решения», *Вопросы кибербезопасности*, №5(8), 30-39, 2014.
[14] B. Bystrova, “Comparative analysis of curricula for bachelor’s degree in cyber security in the USA and Ukraine”, *Comparative professional pedagogy*, 7(4), 114–119, 2017.
[15] O. Ju. Burov, «Educational Networking: Human View to Cyber Defense», *Information Technologies and Learning Tools*, 52, 144—156, 2016.
[16] М. Либицки, «Кибербезопасность: проблемы и пути их решения». [Електронний ресурс]. Доступно:http://www.pitsasinsurances.com/ru/article/cyber-risk-problems-solutions-insurance/**.** Дата звернення: 18.08.2018.
[17] В. Ю. Биков, та М. П. Лещенко, «Цифрова гуманістична педагогіка відкритої освіти», *Теорія і практика управління соціальними системами: філософія, психологія, педагогіка, соціологія*, № 4, 115-130, 2016.
[18] Кібербезпека. аспект 1: соціальні мережі. Міністерство оборони України. [Електронний ресурс]. Доступно:http://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-1-soczialni-merezhi.html. Дата звернення: 21.03.2019.
[19] UNESCO, «Partnering for prosperity: education for green and inclusive growth; Global education monitoring report», 2016. [Електронний ресурс]. Доступно:https://unesdoc.unesco.org/ark:/48223/pf0000246918. Дата звернення: 21.03.2019.
[20] O. Burov, "Virtual Life and Activity: New Challenges for Human Factors/Ergonomics", in *Symp. Beyond Time and Space STO-MP-HFM-231*, STO NATO, 2014, pp. 8-1…8-8.
[21] R. F. Mansour, **"**Understanding how big data leads to social networking vulnerability**"**, *Comput.Hum.Behav.*, 57, 348-351, Elsevier Ltd, 2016.
[22] М. Кузнецов, «*Социальная инженерия и социальные хакеры*», Петербург: БХВ-Петербург, 2007.
[23] В. Ю. Биков, "Теоретико-методологічні засади створення і розвитку сучасних засобів та е-технологій навчання". *Розвиток педагогічної і психологічної наук в Україні 1992 – 2002*. Збірник наукових праць до 10–річчя АПН України . Академія педагогічних наук України. Частина 2. Харків: “ОВС”, 2002. С. 182-199.
[24] О. П. Пінчук, С. Г. Литвинова, та О. Ю. Буров, "Синтетичне навчальне середовище – крок до нової освіти", *Інформаційні технології та засоби навчання* , 4(60), 28-45, ISSN 2076-8184. [Електронний ресурс]. Доступно: https://journal.iitta.gov.ua/index.php/itlt/article/view/1831, 2017.
[25] Z.Yan, T. Robertson, R. Yan, Sung Yong Park, S. Bordoff, Q. Chen, and E. Sprissler, “Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?”, *Computers in Human Behavior*, ISSN: 0747-5632, Vol: 84, Page: 375-382, 2018.
[26] A. Klimburg et al., “National cyber security framework manual”. NATO CCD COE Publications (December 2012), [Електронний ресурс]. Доступно: http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manualch-1.pdf, 2012.
[27] О. Ю. Буров, В. В. Камишин, Н. І. Поліхун, та А. Т. Ашеров, *Технології використання мережевих ресурсів для підготовки молоді до дослідницької діяльності* : Монографія, О. Ю. Буров, Ред. К.: ТОВ «Інформаційні системи», 2012.
[28] Т. Савчук, «Соціальна інженерія: як шахраї використовують людську психологію в інтернеті», 30 серпня 2018. [Електронний ресурс]. Доступно:https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html. Дата звернення: 18.08.2018.

[29] Н. П. Дементієвська, "Професійний розвиток вчителів щодо компетентностей, пов'язаних з безпечним і відповідальним використанням електронних соціальних мереж". [Електронний ресурс]. Звітна наукова конференція Інституту інформаційних технологій і засобів навчання НАПН України : матеріали наук. конф., (Київ, 28 бер. 2017 р.). НАПН України, Ін-т інформаційних технологій і засобів навч. К.: ІІТЗН НАПН України, 26-31, [Електронний ресурс]. Доступно: http://lib.iitta.gov.ua/id/eprint/708603, 2017.
[30] Элементы для создания глобальной культуры кибербезопасности.[Електронний ресурс]. Доступно: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml
[31] Н. П. Дементієвська, "Формування навичок критичного оцінювання веб-ресурсів і проблема безпеки учнів в інтернеті", *Комп'ютер у школі та сім'ї* , 7, 46-51, 2015.

Матеріал надійшов до редакції 04.02.2019 р.

КИБЕРБЕЗОПАСНОСТЬ В ЦИФРОВОЙ УЧЕБНОЙ СРЕДЕ

Быков Валерий Ефимович
доктор технических наук, профессор, академик НАПН Украины, директор
Институт информационных технологий и средств обучения НАПН Украины, г. Киев, Украина
ORCID ID 0000-0002-5890-6783
valbykov@gmail.com

Буров Александр Юрьевич
доктор технических наук, ведущий научный сотрудник
Институт информационных технологий и средств обучения НАПН Украины, г. Киев, Украина
ORCID ID 0000-0003-0733-1120
ayb@iitlt.gov.ua

Дементиевская Нина Петровна
научный сотрудник
Институт информационных технологий и средств обучения НАПН Украины, г. Киев, Украина
ORCID ID 0000-0002-5450-6635
dementievska@iitlt.gov.ua

Аннотация. В статье рассмотрены проблемы кибербезопасности участников образовательного процесса, акцентируется внимание на том, что эти проблемы не сводятся только к техническим аспектам защиты информационных ресурсов, в полном объеме они должны включать такие виды защиты: правовые, технические, информационные, организационные и психологические. Среди психологических средств обеспечения кибербезопасности предлагается выделить психологические, поскольку население в целом и особенно дети и молодежь все чаще становятся объектами кибератак, наиболее уязвимым (слабым) звеном сети. В человеко-центрических сетях, которые составляют постоянно растущую долю среди общих сетей, сама сеть приобретает новые свойства, действуя как самостоятельный составляющая (в дополнение к таким факторам, как узел сети, интерфейс и связи между узлами). Угрозы участникам учебно-воспитательного процесса со стороны киберпространства целесообразно рассматривать как пассивные и активные, разрабатывая адекватные средства защиты и жизнестойкости системы "субъект образовательного процесса-средства обучения-среда". Наиболее значимыми среди киберугроз для участников учебно-воспитательного процесса отмечаются методы социальной инженерии, знание которых и противодействие которым могут быть наиболее эффективными для обеспечения кибербезопасности. Как составляющей подготовки участников учебно-воспитательного процесса по вопросам кибербезопасности предлагается использовать "кибер-вакцинацию", то есть формирование осознанного чувственного опыта пребывания под действием киберугрозы и противодействия ей как системв тренировочных мероприятий, включающих, помимо традиционных методов, тренировочные "кибератаки", а также формирование знаний и умений устойчивости (восстановление) по отношению к киберугрозам. Предлагается дальнейшие исследования проблемы сосредоточить на детальной разработке структуры угроз участникам образовательного процесса, а также методам противодействия. Особое место должна занять проблематика устойчивости к киберугрозам, которая может использовать опыт подготовки операторов эмерджентных отраслей, в том числе диагностирования текущего состояния человека и необходимой коррекции с целью

оптимизации деятельности.

Ключевые слова: кибербезопасность; цифровая среда; учебная деятельность; человеческий фактор; когнитивная опасность; социальная инженерия.

CYBER SECURITY IN A DIGITAL LEARNING ENVIRONMENT

Valeriy Yu. Bykov
Doctor of Technical Sciences, Professor, Academician of NAES of Ukraine, Director
Institute of Information Technologies and Learning Tools of NAES of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-5890-6783
valbykov@gmail.com

Oleksandr Yu. Burov
Doctor of Technical Sciences, Leading Researcher
Institute of Information Technologies and Learning Tools of NAES of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0003-0733-1120
ayb@iitlt.gov.ua

Nina P. Dementievska
Researcher
Institute of Information Technologies and Learning Tools of NAES of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-5450-6635
dementievska@iitlt.gov.ua

Abstract. The article discusses the problems of cyber-security of participants of the educational process, emphasizes the fact that these problems are not limited to the technical aspects of the protection of information resources, they must include in their entirety the following types of protection: legal, technical, informational, organizational and psychological. Among the psychological tools for securing cyber-security, it is proposed to distinguish cognitive ones, as the general population, and especially children and youth, increasingly become targets of cyber-attacks, first of all, their cognitive sphere, becoming the most vulnerable (weak) link in the network. In anthropocentric networks, which make up an ever-increasing share among common networks, the network itself acquires new properties, acting as an independent component (in addition to factors such as the network node, interface and links). Threats to participants in the educational process from the cyberspace should be regarded as passive and active, developing adequate means of protection and viability of the system "subject of educational process-learning-environment". The most significant among cyber-threats for the participants of the educational process are the social engineering methods, which knowledge and resistance can be the most effective for providing cyber-security. As part of the training of participants in the educational process on cyber-security, it is proposed to use "cyber vaccination", that is the formation of a conscious cognitive experience of staying under the influence of a cyber threat and counteracting it as a system of training activities that include, in addition to traditional methods, training of "cyber attacks", as well as the formation of knowledge and skills of resilience (recovery) in relation to cyber-threats. Further research is suggested to focus on the detailed development of types of threats to participants in the education process, as well as methods of counteraction. A special place should be a problem of resistance to cyber-threats, which can use the experience of training operators in emergent industries, including assessing the current state of the person and necessary adjustments in order to optimize its performance.

Keywords: cyber security; digital environment; educational activity; human factor; cognitive hazard; social engineering.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] DSTU 3899-99. Design and definirions. Kyiv, Derzhstandart Ukrainy, 33, 1999 (in Ukrainian).
[2] «Education and Training 2020 Work programme. Thematic Working Group 'Assessment of Key Competences' Literature review, Glossary and examples». European Commission, Directorate-General for Education and Culture, November, 52, 2012 . (in English)

[3] National report on the state and prospects of education in Ukraine. NAPN Ukrainy, K.: Pedahohichna dumka, 448 c., 2016. (in Ukrainian).
[4] V. Yu. Bykov, O. M. Spirin, and O. P. Pinchuk, "General secondary education as the basic link in the system of continuous education". Naukove zabezpechennia rozvytku osvity v Ukraini: aktualni problemy teorii i praktyky (do 25-richchia NAPN Ukrainy) [Tekst] : zbirnyk naukovykh prats, Kyiv : Vydavnychyi dim "Sam", 175-245, 2017. (in Ukrainian).
[5] V. Yu. Bykov, Society of knowledge and education. [online]. Available:https://www.youtube.com/watch?v=cDIytlESUz4. Accessed on: 22.03.2019. (in Ukrainian).
[6] Law № 2163-VIII "About the basic principles of providing cyber security of Ukraine" (Vidomosti Verkhovnoi Rady), № 45, c. 403, 2017. (in Ukrainian).
[7] European Commission, Digital Single Market News, "EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity — Cybersecurity Strategy and Proposal for a Directive", February 7, 2013. (in English)
[8] NATO Cooperative Cyber Defense Centre of Excellence. [online]. Available: https://ccdcoe.org/. Accessed on: 17.08.2018. (in English)
[9] B. Lété, and P. Pernik, "EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions". The German Marshall Fund of the United States. Policy Brief, # 38, 2017. (in English)
[10] ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for cybersecurity, 50 pp., 2012. (in English)
[11] "Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017". [online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-08-16-gartner-says-worldwide-information-security-spending-will-grow-7-percent-to-reach-86-billion-in-2017. Accessed on: 17.08.2018. (in English)
[12] "Elements for creating a global culture of cybersecurity. UN documents". [online]. Available: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml. Accessed on: 22.03.2019. (in Russian)
[13] A. Y. Zghoba, D. V. Markelov, and P. Y. Smyrnov, «Cybersecurity: threats, challenges, solutions», Voprosy kyberbezopasnosty, №5(8), 30-39, 2014. (in Russian).
[14] B. Bystrova, "Comparative analysis of curricula for bachelor's degree in cyber security in the USA and Ukraine", Comparative professional pedagogy, 7(4), 114–119, 2017.
[15] O. Ju. Burov, «Educational Networking: Human View to Cyber Defense», Information Technologies and Learning Tools, 52, 144—156, 2016.
[16] M. Lybytsky, «Cybersecurity: problems and solutions to them». [online]. Available: http://www.pitsasinsurances.com/ru/article/cyber-risk-problems-solutions-insurance/. Accessed on: 18.08.2018. (in Russian).
[17] V. Yu. Bykov, ta M. P. Leshchenko, «Digital humanistic pedagogy of open education», Teoriia i praktyka upravlinnia sotsialnymy systemamy: filosofiia, psykholohiia, pedahohika, sotsiolohiia, № 4, 115-130, 2016. (in Ukrainian).
[18] Syber security. Aspect 1: Social Networks. Ministry of ce of Ukraine. [online]. Available: http://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kiberbezpeka-aspekt-1-soczialni-merezhi.html. Accessed on: 21.03.2019. (in Ukrainian).
[19] UNESCO, «Partnering for prosperity: education for green and inclusive growth; Global education monitoring report», 2016. [online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000246918. Accessed on: 21.03.2019. (in English).
[20] O. Burov, "Virtual Life and Activity: New Challenges for Human Factors/Ergonomics", in Symp. Beyond Time and Space STO-MP-HFM-231, STO NATO, 2014, pp. 8-1…8-8. (in English).
[21] R. F. Mansour, "Understanding how big data leads to social networking vulnerability", Comput.Hum.Behav., 57, 348-351, Elsevier Ltd, 2016. (in English).
[22] M. Kuznetsov, « Social engineering and social hackers», Peterburh: BKhV-Peterburh, 2007. (in Russian).
[23] V. Yu. Bykov, "Theoretical and methodological principles of creation and development of modern means and e-technologies of training". Rozvytok pedahohichnoi i psykholohichnoi nauk v Ukraini 1992 – 2002. Zbirnyk naukovykh prats do 10–richchia APN Ukrainy . Akademiia pedahohichnykh nauk Ukrainy. Chastyna 2. Kharkiv: "OVS", 2002. P. 182-199. (in Ukrainian).
[24] O. P. Pinchuk, S. H. Lytvynova, O. Yu. Burov, "Synthetic educational environment – a footpace to new education", Informatsiini tekhnolohii ta zasoby navchannia, 4(60), 28-45. ISSN 2076-8184. [online]. Available:https://journal.iitta.gov.ua/index.php/itlt/article/view/1831. Accessed on: 26.04.2018. (in Ukrainian).
[25] Z.Yan, T. Robertson, R. Yan, Sung Yong Park, S. Bordoff, Q. Chen, and E. Sprissler, "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?",

Computers in Human Behavior, ISSN: 0747-5632, Vol: 84, Page: 375-382, 2018. (in English).
[26] A. Klimburg et al., “National cyber security framework manual”. NATO CCD COE Publications (December 2012), [online]. Available: http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manualch-1.pdf, 2012. (in English).
[27] O. Iu. Burov, V. V. Kamyshin, N. I. Polikhun, A. T. Asherov. “Technologies of network resources’ use for young people training for research activity”: Monograph, O. Iu. Burov (Eds.), K.: TOV «Informatsiini Systemy», 416 p., 2012 (in Ukrainian).
[28] T. Savchuk, «Social engineering: how fraudsters use human psychology on the Internet», 30 serpnia 2018. [online]. Available: https://www.radiosvoboda.org/a/socialna-inzhenerija-shaxrajstvo/29460139.html (in Ukrainian).
[29] N. P. Dementiievska, "Teacher Professional Development on Competences Related to Safe and Responsible Use of Electronic Social Networks". Zvitna naukova konferentsiia Instytutu informatsiinykh tekhnolohii i zasobiv navchannia NAPN Ukrainy : materialy nauk. konf., (Kyiv, 28 ber. 2017 r.). NAPN Ukrainy, In-t informatsiinykh tekhnolohii i zasobiv navch. K.: IITZN NAPN Ukrainy, 26-31. [online]. Available: http://lib.iitta.gov.ua/id/eprint/708603, 2017 (in Ukrainian).
[30] Elements for creating a global culture of cybersecurity. [online]. Available: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml. (in Russian).
[31] N. P. Dementiievska, "Formation of the skills of critical evaluation of web resources and the problem of student safety on the Internet", Kompiuter u shkoli ta simi , 7, 46-51, 2015 (in Ukrainian).

This work is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.