https://doi.org/10.32820/2074-8922-2018-59-35-40
УДК 378.016

ПРОФЕСІЙНА ПІДГОТОВКА ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ: ТЕЗАУРУС ТА ОНТОЛОГІЯ

©Сачук Ю.Є.
Луцький національний технічний університет

Сачук Юлія Євгеніївна: ORCID: 0000-0002-9313-8716; julijasachuk@gmail.com; кандидат педагогічних наук; старший викладач кафедри комп'ютерних технологій; Луцький національний технічний університет; вул. Львівська, 75м. ЛуцькВолинська обл. 43018, Україна.

Нинішня ситуація в розвитку зберігання, обміну та обробки інформації, що характеризується інтенсивним впровадженням технологій, розповсюдженням локальних, корпоративних та глобальних мереж у всіх сферах життя цивілізованої держави, створює нові можливості та якість інформаційного обміну. Описана ситуація актуалізує питання, щоб інформація була захищеною та безпечною одночасно. У зв'язку з цим, проблеми професійної підготовки висококваліфікованих фахівців із кібербезпеки та захисту інформації, що наразі не є стандартизованою, потребують невідкладного вирішення.

У статті здійснено спробу окреслити тезаурус галузі професійної підготовки майбутніх фахівців із кібезбезпеки та захисту інформації. Акцентовано увагу на перевагах обрання тезаурусного підходу дослідження окресленої проблеми. Детерміновано основні поняття досліджуваної галузі та встановлено зв'язки між категоріями «інформаційна безпека», «кібербезпека» та «захист інформації». Дотично розглядається пріоритетність завдання створення та вдосконалення національної інформаційно-комунікаційної інфраструктури України, яке покладатиметься саме на фахівців досліджуваної спеціальності. Таким чином, тезаурус поряд із онотолією є сучасною формою представлення знань, придатною для їх автоматизованої обробки, що корелює з набуттям та управлінням знань у процесі професійної підготовки фахівців із кібербезпеки та захисту інформації.

Ключові слова: інформаційна безпека, кібербезпека, захист інформації, кіберпростір, захищеність, безпека, тезаурусний підхід, інформаційно-комунікаційна інфраструктура.

Сачук Ю.Е. ″Профессиональная подготовка специалистов по кибербезопасности и защите информации: тезаурус и онтология″.

Нынешняя ситуация в развитии хранения, обмена и обработки информации характеризуется интенсивным внедрением технологий, распространением локальных, корпоративных и глобальных сетей во всех сферах жизни цивилизованного государства, создает новые возможности и качество информационного обмена. Обозначеная ситуация актуализирует вопрос, чтобы информация была защищена и безопасна одновременно. В связи с этим, проблемы профессиональной подготовки высококвалифицированных специалистов по кибербезопасности и защиты информации, которая пока не является стандартизированной, требуют безотлагательного решения.

В статье предпринята попытка очертить тезаурус области профессиональной подготовки будущих специалистов по кибезбезопасности и защите информации. Акцентировано внимание на преимуществах избрания тезаурусного подхода исследования обозначенной проблемы. Детерминировано основные понятия изучаемой области и установлены связи между категориями «информационная безопасность», «кибербезопасность» и «защита информации». Касательно рассматривается приоритетность задачи создания и усовершенствования национальной информационно-коммуникационной инфраструктуры Украины, которая возложена именно на специалистов исследуемой специальности. Таким образом, тезаурус рядом с онотолией является современной формой представления знаний, пригодной для их автоматизированной обработки, коррелирует с приобретением и управлением знаний в процессе профессиональной подготовки специалистов по кибербезопасности и защиты информации.

Ключевые слова: информационная безопасность, кибербезопасность, защита информации, киберпространство, защищенность, безопасность, тезаурусный подход, информационно-коммуникационная инфраструктура.

Yu. Sachuk ″Professional Training on Cybersecurity and Information Protection: Thesaurus and Ontology″

The current situation of the development of storage, exchange and processing of information is characterized by intensive technology implementation, the dissemination of local, corporate and global networks in all spheres of life of a civilized state. It creates new opportunities and quality of information exchange. In this context we have the question how to ensure the safety and protection of information at the same time. So, the problems of professional training of highly qualified specialists in cybersecurity and information security are of paramount importance.

The article aims to outline the scientific ontology and thesaurus areas of cybersecurity and information security as a basis for professional development of specialists in the chosen specialty. We used the thesaurus approach to study the terminology of the cybersecurity industry. The article outlines the advantages of the thesaurus approach, defines the notion of "information security", "cybersecurity", "information protection" and establishes links between them. Thesaurus and ontology are a modern form of the presentation of knowledge that is suitable for its automated processing, and correlates with the acquisition and management of knowledge in the process of professional training of cybersecurity and information security specialists. The thesaurus of the field of professional training in cyber security and information security is rather broad, debatable and requires further research and unambiguous identification. The exhaustively formulated and deterministic terminology will be the first step that will help the specialists of the specialty under study to fulfill their main professional task – providing cybersecurity of information and communication infrastructure.

Keywords: information security, cybersecurity, information protection, cyberspace, security, protection, thesaurus approach, information and communication infrastructure.

Постановка проблеми. Розвиток інформаційної та комунікаційної інфраструктури, динамічність новітніх технологій є характерною рисою сьогодення. Недарма наш час названий «інформаційною ерою», адже сфера інформації стала невід'ємною складовою економіки країни та активно впливає на стан політичної, економічної, оборонної та інших граней безпеки України.

Сучасна ситуація в розвитку зберігання, обміну та обробки інформації, що характеризується інтенсивним впровадженням технологій, розповсюдженням локальних, корпоративних та глобальних мереж у всіх сферах життя цивілізованої держави, створює нові можливості та якість інформаційного обміну. У даному контексті постає питання, щоб інформація була захищеною та безпечною одночасно. Необхідність вирішення цього питання актуалізується такими факторами:

- експоненціальний ріст кількості персональних комп'ютерів, лептопів та інших авоматизованих пристроїв для обміну інформацією;
- стрімке розширення кола користувачів, що безпосередньо мають доступ до цифрових мереж та інформаційних ресурсів;
- грандіозне збільшення об'ємів інформації, що накопичується, зберігається та обробляється з допомогою засобів автоматизації;
- бурхливий розвиток апаратно-програмних засобів та технологій, що не відповідають сучасним вимогам безпеки;
- невідповідність між надшвидким розвитком засобів обробки інформації, вітчизняної теорії інформаційної безпеки та розробкою міжнародних стандартів і правових норм, що забезпечать необхідний рівень захисту інформації;
- інформаційна війна, зумовлена політичною ситуацією в країні;
- кіберзлочини, що іноді набувають державно важливого значення;
- становлення кіберполіції України.

У зв'язку з цим, проблеми професійної підготовки висококваліфікованих фахівців із кібербезпеки та захисту інформації, що наразі не є стандартизованою, набувають пріоритетного значення.

Метою статті є окреслити науковий тезаурус та онтологію сфери кібербезпеки та захисту інформації як базу для професійного становлення фахівців з обраної спеціальності.

Аналіз останніх досліджень і публікацій. Відсутністю чіткої детермінованості понять галузі кібербезпеки та захисту інформації переймалась низка вітчизняних та зарубіжних науковців. Зокрема, Д. Дубов зробив спробу впорядкування кібербезпекової термінології та огляду підходів, що існують у цій сфері в практиці вітчизняних і західних досліджень [4]. Проблему визначення й обґрунтованості понятійно-категорійного апарату професійної діяльності із забезпечення кібернетичної безпеки в контексті реформування вищої освіти України розглянуто С. В. Мельником

[7], деталізовано та систематизовано тлумачення понять «інформаційна безпека» та «кібернетична безпека». Дослідженням кіберпростору як тріади інформації, інфраструктури та діяльності людини займались С. В. Рибка, Є. В. Кільчицький та О. М. Післегін [8]. Дослідження терміноутворення кібербезпекової політики в текстах нормативно-правових актів України здійснюється І. В. Діордіца [3].

Виклад основного матеріалу. Поняття безпеки та захисту в сучасному світі відіграють одну з найважливіших ролей у будь-яких життєвих процесах: біологічних, політичних, економічних, соціальних, технічних, територіальних та ін. Виникає необхідність розширення номенклатури освітніх спеціальностей щодо кібербезпеки та захисту інформації, їх стандартизації. Професійна підготовка повинна здійснюватись комплексно із захопленням проблем інформаційної безпеки в гуманітарній, природничо-математичній та технічній сферах. Тому варто не лише коректно дефініціювати досліджувані поняття та похідні від них, а й правильно застосовувати їх.

Тезаурусний підхід опису досліджуваної галузі передбачає накопичення. В інформатиці та теорії штучного інтелекту акцентують на систематизації даних, що складають тезаурус та їхній орієнтаційний характер. Тезаурус – не просто система понять та зв'язків між ними, він відображає глибину знання. Саме тому обмін тезаурусами між викладачем та студентом, процес розширення та переконструювання тезаурусу особистістю передбачає навчання. Таким чином, перевагами тезаурусного підходу є:

- цілісність, незважаючи на фрагментарність його складових, що забезпечується цілісністю особистості;
- ієрархічність, сприйняття цілісної галузі через призму ціннісного аспекту; виділені пріоритети складають підсистему – ядро тезаурусу;
- творче перетворення, переосмислення, що має герменевтичний аспект у характеристику тезаурусу;
- орієнтаційний вектор тезаурусу;
- дійсність тезаурусу, що впливає на поведінку та інші прояви суб'єкта; носить соціалізуючий характер [6].

Будь-яка галузь теорії та практики фундаментується на чітко визначеному понятійному апараті. Формування вичерпного переліку термінів, їх визначення та інтерпретація, аби забезпечувалось однозначне розуміння кожного з них, пріоритетне значення має й для ефективної професійної підготовки фахівців із кібербезпеки та захисту інформації.

Підійшовши до проблеми визначення термінологічної бази обраної нами сфери, стикаємось із суміжною та відносно ширшою категорією під назвою «інформаційна безпека». Таким чином, перед нами постає завдання визначення відношень між категоріями «інформаційна безпека», «кібербезпека» та «захист інформації».

Тезаурус галузі інформаційної безпеки відображає широкий спектр суттєвих властивостей, ознак та відношень, притаманних даному специфічному виду безпеки. Ми погоджуємось із дослідниками [2], що виділяють три групи термінів теорії інформаційної безпеки.

1) Терміни, що детермінують наукову основу інформаційної безпеки. До цієї групи належать терміни, що використовуються у багатьох галузях знань та є однозначними, семантично уніфікованими та стилістично нейтральними. Це: *інформація, комунікація, конфлікт, вплив, загроза, небезпека, безпека, система*.

   Поняття в цій групі відповідають вимогам однозначності та стабільності, тобто однозначно вживаються в одній галузі знань та зберігають зміст у будь-якій іншій. Лише поняттю «інформація» притаманна специфічна властивість: у різних сферах вжитку, та навіть в одній, може характеризувати предмет, явище, процес та їх властивості й відношення одночасно.
2) Терміни, що детермінують предметну основу інформаційної безпеки. Ця група термінів позначає поняття та їх співвідношення з іншими поняттями в рамках інформаційної безпеки як особливої галузі знань. До них належать: *інформатика, інформатизація, інформаційна система, інформаційні технології, інформаційні процеси, інформаційний об'єкт, інформаційний ресурс, інформаційна інфраструктура, інформаційна сфера, інформаційний потенціал*.
3) Терміни, що детермінують характер діяльності щодо забезпечення інформаційної безпеки. Ця група охоплює терміни, що позначають характерні для цієї сфери предмети, явища, процеси, їх властивості та відношення. Поняття групи охоплюють широке коло дефініцій різноманітного рівня: від технічного каналу витоку формації до інформаційного протиборства. До них належать*: інформаційне протиборство, інформаційна перевага, інформаційна безпека, загрози інформаційної безпеки, забезпечення інформаційної безпеки,*

система забезпечення інформаційної безпеки, інформаційна захищеність, безпека інформації, захист інформації, об'єкт захисту інформації, носій інформації, доступ до інформації, доступність інформації, цілісність інформації, конфіденційність інформації, несанкціонований доступ до інформації, витік інформації, канал передачі інформації, вплив на інформацію, інформаційно-психологічний вплив, інформаційно-психологічна сфера.

Керуючись стандартом кібербезпеки ISO/IEC 27032:2012, IDT [1], наведемо схему зв'язків між інформаційною безпекою, кібербезпекою та захистом інформації (Рис.1). У деяких випадках поняття інформаційної безпеки ототожнюють із захистом інформації.

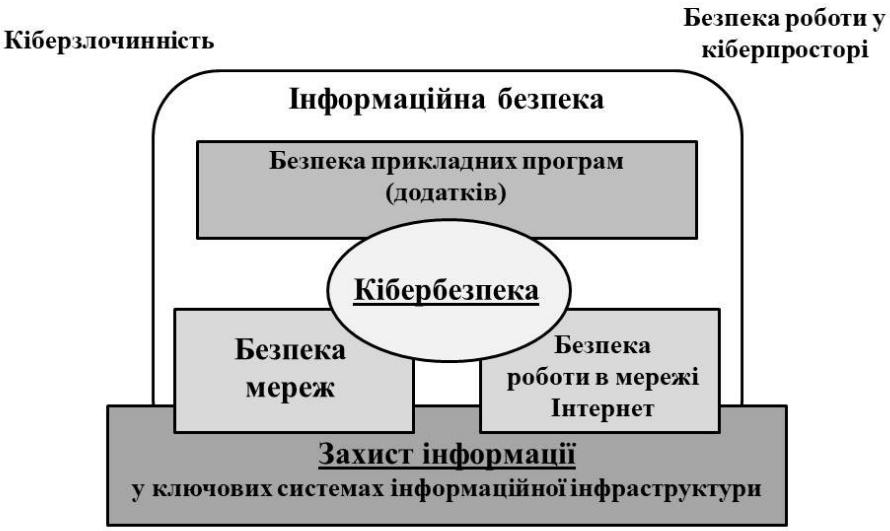

Рис.1. Місце кібербезпеки та захисту інформації відносно інших сфер безпеки

За аналогією з класичним трактуванням інформаційної безпеки, у стандарті [1] під *кібербезпекою* мають на увазі властивість захищеності активів від загроз конфіденційності, цілісності, доступності, але в певних абстрактних рамках – кіберпросторі.

Поняття *кіберпростору* детермінується як комплексне віртуальне середовище, сформоване в результаті діяльності суб'єктів, програм та сервісів у мережі Інтернет посередництвом відповідних мережевих та комунікаційних технологій. Інакше кажучи, кіберпростір – це тріада з активів (статичної та динамічної інформації в цифровому вигляді), інформаційно-комунікаційної структури та діяльності й взаємодії користувачів кіберпростору (Рис.2).

Пріоритетним у забезпеченні кібербезпеки вважається координація взаємодії між організаціями, що формують кіберпростір, самостійні дії яких не забезпечують ефективний захист від кіберзагроз.

Тезаурус кібербезпеки інтегрований із поняттями інформаційної безпеки, безпеки додатків, мережевої безпеки, безпеки Інтернет та безпеки критичної інформаційної інфраструктури (Рис.1). *Безпека додатків* визначається відносно прикладних програмних продуктів, а також інформаційно-програмних ресурсів та процесів, що беруть участь у їхньому життєвому циклі. *Безпека мереж* пов'язана із проектуванням, упровадженням та використанням мереж у середині організації, між організаціями, між організаціями та користувачами. *Безпека в мережі Інтернет* стосується інтернет-послуг та відповідних систем інформаційно-комунікаційних технологій та мереж. *Безпека критичної інформаційної інфраструктури* характеризує захищеність від відповідних загроз, зокрема інформаційної безпеки.

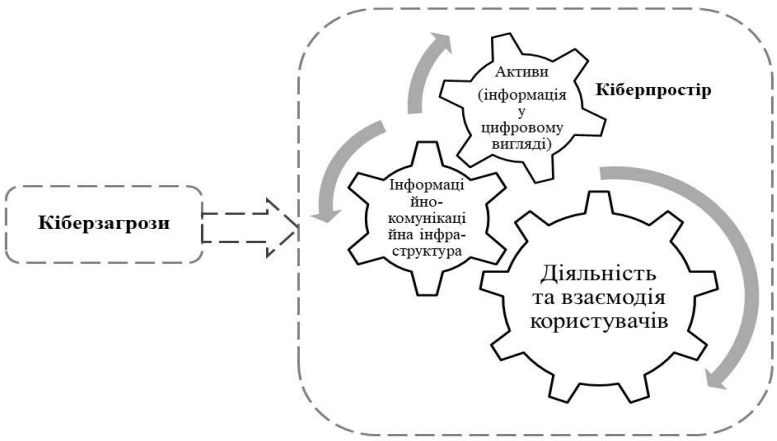

Рис.2. Кіберзагрози та кіберпростір

На перший погляд, абстрактне поняття кіберпростору подамо у вигляді сукупності цілком реальних його складових. До *активів* кіберпростору належить те, що являє цінність, наприклад, інформаційні та програмні ресурси. Незважаючи на «віртуальність» кібербезпеки, активи можуть бути як віртуальними, так і матеріальними, наприклад, віртуальна база даних і фізичний пристрій – usb-ідентифікатор. Активи поділяють на дві групи: персональні та активи організацій. Відповідно до вищесказаного, таксономія кіберзагроз включає класифікацію за видами та типами активів, зовнішніми та внутрішніми ознаками, цілями, джерелами та ін.

Під *інформаційно-комунікаційною інфраструктурою* (яка в рамках держави називається національною), розуміють сукупність територіально розподілених інформаційних та інформаційно-телекомунікаційних мереж, мереж поштового зв'язку, а також організаційних структур, правових та нормативних механізмів, що забезпечують управління інфраструктурою, її ефективне функціонування та надання інформаційних та комунікаційних послуг користувачам. Призначенням національної інформаційно-комунікаційної структури України є формування єдиного інформаційного простору для вирішення проблем соціального захисту, медичного обслуговування, підвищення якості освіти, забезпечення потреб державного управління, правопорядку, оборони країни та національної безпеки; забезпечення суб'єктів інформаційного суспільства якісними інформаційними та комунікаційними послугами; забезпечення інтеграції національної інформаційно-комунікаційної інфраструктури із глобальною [5]. Сучасні тенденції у сфері інформаційно-комунікаційних технологій зумовлюють будову інформаційно-комунікаційної інфраструктури (Рис.3).

Рис.3. Будова інформаційно-комунікаційної інфраструктури

Враховуючи опис кібербезпеки як властивості, зауважимо, що *захист інформації* – комплекс організаційних, правових та технічних заходів щодо запобігання кіберзагроз та усуненню їх наслідків. Захищають інформацію за трьома напрямками: від несанкціонованого доступу, розголосу та несанкціонованих впливів.

Отже, захист інформації спрямований на попередження, виявлення, локалізацію кіберзагроз та кіберзлочинів; ліквідацію їх наслідків та відновлення сатус-кво.

Висновки. Підсумовуючи вищесказане, зауважимо, що тезаурус сфери професійної підготовки фахівців із кібербезпеки та захисту інформації є досить широким, дискусійним та потребує подальших досліджень та встановлення однозначності. У рамках написання статті була здійснена спроба окреслити головні поняття та риси обраної галузі, роз'яснити зв'язки між ними. На нашу думку, саме коректно визначений тезаурус та онтологія кіберсередовища є підґрунтям для ефективних наукових розвідок щодо якісної професійної підготовки фахівців із кібербезпеки та захисту інформації.

Тезаурус поряд із онотолією є сучасною формою представлення знань, придатною для їх автоматизованої обробки, що корелює із набуттям та управлінням знання в навчальному процесі вищої школи. Перевагою тезаурусного підходу є його здатність «розкласти по полицях» великий об'єм інформації для кращого володіння нею, формування суб'єктного тезаурусу, його подальшого поповнення та керування.

На наш погляд, вичерпно сформульована та детермінована термінологія стане першим кроком, що допоможе фахівцям досліджуваної спеціальності виконувати їх головне професійне завдання – забезпечення кібербезпеки інформаційно-комунікаційної інфраструктури.

Список використаних джерел

1. ISO/IEC 27032 :2012 Information technology. Security techniques. Guidelines for cybersecurity. – Edition confirmed; 2012-07. – 50 p.
2. Информационная безопасность [Электронный ресурс] / О. В. Азамов [и др.]. – Режим доступа : http://www.naukaxxi.ru/materials/41/
3. Діордіца І. В. Репрезентація термінології кібербезпекової політики в текстах нормативно-правових актів України / І. В. Діордіца // Науковий вісник Міжнародного гуманітарного університету. Серія Юриспруденція. – 2017. – Вип. 29(1). – С. 64-67
4. Дубов Д. Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. – 2010. – №5. – С. 19-30.
5. Каличенский А. Концепция создания Национальной информационно–коммуникационной инфраструктуры Украины [Электронный ресурс] / А. Каличенский // Региональный форум МСЭ. – Киев : НКРСИ, ОАО "Гипросвязь". – 2012. – Режим доступа : https://www.itu.int/ITU-D/tech/events/2012/Spectrum_CIS_Kiev_Sept12/Presentations/Session2/A_Kalichensky_a.pdf
6. Луков В. А. Тезаурусный подход: исходные положения [Электронный ресурс] / В. А Луков, В. А. Луков // Информационный гуманитарный портал «Знание. Понимание. Умение». – 2008. – № 9. – Режим доступа: http://www.zpujournal.ru/ezpu/2008/9/
7. Мельник С. В. Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки / С. В. Мельник // Інформаційні технології і засоби навчання. – 2016. – Т. 55, Вип. 5. – С. 187-197.
8. Рибка С. В. Кіберпростір, управління інфраструктурою, кібербезпека / С. В. Рибка, Є. В. Кільчицький, О. М. Післегін // Стратегічна панорама. – 2015. – № 1. – С. 126-134.

References

1. ISO/IEC 27032 :2012 Information technology. Security techniques. Guidelines for cybersecurity 2012, Edition confirmed 2012-07.
2. Azamov, OV et al. n.d., *Informacionnaja bezopasnost*, [Information Security], <http://www.naukaxxi.ru/materials/41/>.
3. Diorditsa, IV 2017, 'Reprezentatsiia terminolohii kiberbezpekovoi polityky v tekstakh normatyvno-pravovykh aktiv Ukrainy', [Representation of the Terminology of the Cyberbezpekovo Policy in the Texts of the Regulatory Legal Acts of Ukraine], *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia Yurysprudentsiia*, iss. 29(1), pp. 64-67.
4. Dubov, D 2010, 'Pidkhody do formuvannia tezaurusu u sferi kiberbezpeky', [Approaches to the formation of a thesaurus in the field of cybersecurity], *Politychnyi menedzhment*, no. 5, pp. 19-30.
5. Kalichenskij, A 2012, 'Koncepcija sozdanija Nacionalnoj informacionno-kommunikacionnoj infrastruktury Ukrainy', [The concept of creating the National Information and Communication Infrastructure of Ukraine], *Regionalnyj forum MSJe 11.09.-13.09.2012*, Nacionalnaja komissija regulirovanija svjazi i informatizacii, OAO Giprosvjaz, Kiev, <https://www.itu.int/ITU-D/tech/events/2012/Spectrum_CIS_Kiev_Sept12/Presentations/Session2/A_Kalichensky_a.pdf>.
6. Lukov, VA & Lukov, VA 2008, 'Tezaurusnyj podhod: ishodnye polozhenija', [Thesaurus Approach: Starting Positions], *Informacionnyj gumanitarnyj portal Znanie. Ponimanie. Umenie*, no. 9, <http://zpu-journal.ru/e-zpu/2008/9/>.
7. Melnyk, SV 2016, 'Poniatiino-katehorialnyi aparat u systemi profesiinoi pidhotovky maibutnikh fakhivtsiv z kiberbezpeky', [Concept-categorical device in the system of professional training of future cybersecurity specialists], *Informatsiini tekhnolohii i zasoby navchannia*, vol. 55, iss. 5, pp. 187-197.
8. Rybka, SV, Kilchytskyi, YeV & Pislehin, OM 2015, 'Kiberprostir, upravlinnia infrastrukturoiu, kiberbezpeka', [Cyberspace, Infrastructure Management, Cybersecurity], *Stratehichna panorama*, no. 1, pp. 126-134.

Стаття надійшла до редакції 15.05.2018