

2. Харитонова О. Глобалізація та інтернаціоналізація вищої освіти у вимірі публічно-правових досліджень. Національний юридичний університет імені Ярослава Мудрого.
3. Сопілко І. М., Череватюк В. Б. Інтеграція в європейський науковий і освітній простір: очікування для молодих вчених і студентів // Юридичний вісник. – № 3 (44). – 2017.
4. Нітенко О. В. Інтернаціоналізація вищої освіти як фактор розвитку університету / О. Нітенко // Освітологічний дискурс. – 2015. – № 2 (10). – С. 206-215.
5. Концепція вдосконалення правничої (юридичної) освіти для фахової підготовки правника відповідно до європейських стандартів вищої освіти та правничої професії. Проект. [Електронний ресурс]. – Режим доступу : http://www.kmu.gov.ua/control/uk/publish/article?art_id=249321194&cat_id=244277212

Бучма О. В.
*кандидат філософських наук, доцент,
 професор кафедри теорії та історії держави і права
 Національного педагогічного університету
 імені М. П. Драгоманова (м. Київ)*

Гнинюк Р. Ю.
*магістрант спеціальності “Правознавство”
 факультету політології та права
 Національного педагогічного університету
 імені М. П. Драгоманова (м. Київ)*

ОСОБЛИВОСТІ СУЧАСНОГО СТАНУ КІБЕРБЕЗПЕКИ УКРАЇНИ

Останнім часом відносно нове поняття безпеки в кібернетичному просторі або кібернетичної безпеки все більше актуалізується та розглядається як стратегічна проблема держави. Діяльність комерційних структур, робота урядів та забезпечення системи національної безпеки держав з кожним роком все більше залежать від інформаційних технологій та ІТ інфраструктур кіберпростору. Тотальна інформатизація всіх сфер діяльності суспільства, відсутність кордонів в кібернетичному просторі призвели до драматичного збільшення кількості загроз, актів кібертероризму та кіберзлочинів у всьому світі.

Забезпечення національної безпеки зміщується у бік не стільки декларованої, скільки реально розглядуваної проблеми. Ліпкан В. та Діордіца І. відзначають, що це обумовлено активізацією зовнішніх загроз безпечного розвитку України: посиленням мілітаризації держав у регіоні, використанням положення енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї тощо. Разом із тим, зовнішні загрози посилюються наявністю внутрішніх викликів національній безпеці, зокрема, йдеться про розбалансованість та незавершеність системних реформ, зниження обороноздатності держави, боєздатності Збройних Сил України, незадовільний стан фінансування, складне економічне становище [6].

Розуміючи сучасний стан та актуальність проблеми забезпечення кібернетичної безпеки, більшість країн світу проводять комплексні заходи щодо безпеки в кібернетичному просторі. Ці заходи пов'язані перш за все з розробкою та вдосконаленням нормативно-правової бази, що регулює питання сфери кібербезпеки. Також створюються відомчі та державні структури, що відповідають за забезпечення кібернетичної безпеки. Спеціальні служби різних країн вивчають методи діяльності хакерських груп, а іноді навіть активно співпрацюють з ними, використовуючи їхні знання та навички при проведенні кібернетичних операцій, пропонуючи їм натомість лояльність та захист. Тому проблема забезпечення кібернетичної безпеки в державі є доволі важливим та складним питанням, а зневажливе ставлення до цього питання може призвести до непередбачуваних наслідків. За роки незалежності України, зазначає М. Кропивницький, питання кібернетичної та інформаційної безпеки розвивалося за залишковим принципом. Нормативно-правові документи з регулювання цієї сфери розроблялись безсистемно, не рідко базувались на застарілих радянських нормах та вступали у протиріччя один з одним. Це призвело в свою чергу до гнітючого становища в системі кібернетичної безпеки та інформаційно-комунікаційних технологій взагалі [7].

Впродовж останніх років Україна робить певні кроки у напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу у цих сферах діяльності складає: Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV; Закони України “Про інформацію”, “Про основи національної безпеки України”, “Про Державну службу спеціального зв'язку та захисту інформації України”, “Про телекомунікації”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про доступ до публічної інформації”, “Про оборону України”, “Про засади внутрішньої і зовнішньої політики”, “Про об'єкти підвищеної небезпеки”; Укази Президента України, зокрема про: Доктрину інформаційної безпеки, Стратегію національної безпеки України та Воєнну доктрину України; окремі положення Кримінального Кодексу України, окремі Постанови Кабінету Міністрів та Рішення РНБО України.

При цьому ключова роль у забезпеченні кібербезпеки покладається на:

1) Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ систем;

2) Закон України “Про Основні засади розвитку інформаційного суспільства України на 2007–2015 роки” [8] у запропонованих змінах до якого указується на необхідність створення національної системи кібербезпеки;

3) Закон України “Про основні засади забезпечення кібербезпеки України”, який набере чинність 09.05.2018, яким має бути запроваджено низку термінів,

пов'язаних із кібербезпекою, чітко визначено об'єкти та суб'єкти кібербезпеки та кіберзахисту, принципи кібербезпеки, національна система кібербезпеки.

Практичними кроками щодо реалізації чинної нормативно-правової бази стало створення 2007 року в складі Державної служби спеціального зв'язку та захисту інформації (ДССЗІ) України Центру реагування на комп'ютерні інциденти. На виконання статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки України на базі спеціального підрозділу для боротьби з кіберзагрозами утворено Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім цього, Указом Президента України “Про виклики та загрози національній безпеці України у 2011 році” від 10 грудня 2010 року № 1119/2010 ухвалено рішення щодо початку створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України “Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України” від 25 січня 2012 року №34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на ступінь та динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю і торгівлею людьми [3].

Сьогодні фахівці з кіберзахисту від ДССЗІ, СБ та МВС України стикаються у своїй роботі з численними труднощами, не маючи змоги самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному та кіберпросторі. Через це їм доводиться дедалі активніше шукати шляхи співробітництва з аналогічними організаціями світового співтовариства, використовуючи для цього всі наявні можливості й механізми, які є в розпорядженні кожної з країн [1].

Ще однією з головних актуальних проблем, яку визначає у своїй праці Дубов Д.В., є “незадовільне кадрове забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки”, про що зазначається у аналітичній доповіді Національного інституту стратегічних досліджень при Президенті України “Кібербезпека: світові тенденції та виклики для України” [5]. незважаючи на те, що ціла низка вищих навчальних закладів України здійснює підготовку фахівців за різноманітними спеціальностями галузі знань 1701 “Інформаційна безпека”. Аналіз недавно введених галузевих стандартів вищої освіти у галузі знань 1701 Інформаційна безпека, зокрема, освітньо-кваліфікаційної характеристики (ОКХ) та освітньо-професійної програми (ОПП) [4] за напрямом 6.170101 “Безпека інформаційних і комунікаційних систем” показує, як зазначають В. Бурячок, В. Богуш, що професійні компетентності, задекларовані в цих галузевих стандартах, недостатньо враховують стан та перспективу розвитку методів та засобів забезпечення кібернетичної безпеки.

Тому проблема побудови профілю навчання бакалаврів, спеціалістів і магістрів щодо кібернетичної безпеки відповідно до найновіших досягнень у галузі розбудови кібернетичного простору та забезпечення кібернетичної безпеки вважається авторам надзвичайно актуальною [2].

Отже, впродовж останніх років Україна зробила чи малий вклад у забезпеченні кібернетичної безпеки шляхом створення нормативно правової бази для забезпечення даного сектору безпеки, створено спеціальні органи та підрозділи : Центр реагування на комп'ютерні інциденти, Національний контактний пункт при СБУ, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки при СБУ та Департамент боротьби з кіберзлочинністю і торгівлею людьми при СБУ. Проте залишається ще ряд проблем, які потребують термінового вирішення, одне з головних, це достатній рівень фахової підготовки співробітників у сфері інформаційної безпеки.

ЛІТЕРАТУРА :

1. 11-12 лютого в Україні пройшли Консультації експертів “Україна – НАТО” з питань кібернетичного захисту [Електронний ресурс]. – Режим доступу : <http://zik.com.ua/ua/news/2010/02/12/216707>.
2. *Бурячок В., Богуш В.* Рекомендації щодо розробки та запровадження профілю навчання “Кібернетична безпека” в Україні// Український науковий журнал інформаційної безпеки, 2014. – 2 вид-во. – С. 128.
3. *Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.* Інформаційна та кібербезпека : соціотехнічний аспект : підручник. – Київ, 2015. – С. 17.
4. Галузевий стандарт вищої освіти України з галузі знань 1701 Інформаційна безпека за напрямом підготовки бакалавра 6.170101 Безпека інформаційних і комунікаційних систем. Освітньо-кваліфікаційна характеристика. Затверджений Наказом Міністерства освіти і науки України 9 липня 2010 р. № 687.
5. *Дубов Д. В.* Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. / Д. В. Дубов, М. А. Ожеван. – Київ : НІСД, 2011. – 30 с.
6. *Ліпкан В., Діордіца І.* Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України // Інформаційне право. – № 5. – 2017. – С. 174.
7. *Кропивницький М.* Кібербезпека в Україні: 2016 та прогнози на майбутнє : матеріали Всеукраїнської науково-технічної конференції 23-25 листопада. – 2016. – С. 21.
8. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007 № 537-V. [Електронний ресурс]. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/537-16>. – Офіц. вид. – Київ : Відомості Верховної Ради України від 23.03.2007.
9. *Ткаченко В. І.* Шляхи формування системи забезпечення національної безпеки / В. І. Ткаченко, Є. Б. Смірнов, О. О. Астахов // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2015. – № 2. – С. 3-8.