УДК 34.08

Ірина Вікторівна ПАНОВА,
кандидат юридичних наук, доцент,
доцент кафедри загальноправових дисциплін факультету № 6
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-4325-5428

ЩОДО ОКРЕМИХ ПИТАНЬ ВИЗНАЧЕННЯ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ПРИ ПІДГОТОВЦІ ПРАЦІВНИКІВ ДЛЯ КІБЕРПОЛІЦІЇ

Проблемам кібербезпеки приділяється все більше уваги як з боку органів державної влади, так і суспільства в цілому. На початку військової агресії проти України з боку Російської Федерації, саме в інформаційній сфері і були головні «програші», що дозволило без пострілів втратити контроль над Автономною Республікою Крим, розв'язати військовий конфлікт на Донбасі. Все це неабияк вказує на значення кібербезпеки в забезпеченні національної безпеки в Україні.

5 жовтня 2017 року Верховна Рада України прийняла закон України «Про основні засади забезпечення кібербезпеки України». Необхідність прийняття цього закону була нагальною, ще на весні 2017 року, парламент відправив його на повторне друге читання, після доопрацювання закон все ж прийняли.

Однак, детальний аналіз змісту закону вказує на існування ситуації – краще хоч якийсь, ніж взагалі ніякого. На нашу думку, одним із недоліків цього закону є те, як він визначає об'єкти критичної інфраструктури. Так ст. 6 названого закону містить, такі положення:

«1. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:…

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я;…».

Таким чином, підприємства приватної форми власності в повній мірі підпадають під дію цього закону, а відповідальність за кіберзахист цих об'єктів покладається на їх власників/керівників. Такі положення закону фактично створюють корупційні загрози впливу державних органів на приватні суб'єкти господарювання, при цьому зобов'язуючи їх охороняти самим себе за свій рахунок. Звичайно, що будь який фермер чи заклад громадського харчування не потрапить до переліку об'єктів критичної інфраструктури, адже критерії та порядок віднесення об'єктів до об'єктів критичної інфраструктури, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України.

Проте, наприклад аудит інформаційної безпеки здійснює Державна служба спеціального зв'язку та захисту інформації України, так само вона встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації). При цьому в Законі не передбачено можливості надання та/або прийняття результатів аудиту міжнародними інституція за міжнародними стандартами. Так само не йде мова про стандарти за якими буде оцінюватися рівень кібербезпеки.

Намагання в Україні створити якусь власну систему кіберзахисту, яка буде працювати без урахування міжнародних стандартів, приречена на винайдення власної конструкції велосипеда. Неврахування міжнародного досвіду та стандартів може призвести до того, що, наприклад, навіть за умови запровадження більш сучасної системи кіберзахисту приватною компанією, вона не пройде державного аудиту, адже не буде відповідати вимогам, які встановлюються державним органом. Для ілюстрації можна згадати ситуацію, яка складалася при відправленні електронних носіїв інформації (дискет, компакт-дисків). Для переправлення за кордон в кінці 1990-х – початку 2000-х років таких носіїв вимагалося перевірка компетентними органами змісту носія та опломбування його з використанням металічної проволоки, і це в час глобального розвитку та використання мережі Інтернет та вільного переміщення через кордон осіб з портативними комп'ютерами в ручній поклажі.

© Панова І. В., 2017

Фахівцями у сфері кібербезпеки розроблені певні стандарти, які пропонується застосовувати і в Україні [1]:

– NIST Cybersecurity Framework – фреймворк з кібербезпеки, розроблений американським інститутом стандартів;

– серія міжнародних стандартів ISO-27XXX – з інформаційної та кібербезпеки;

– галузеві стандарти з кібербезпеки, розроблені в різних країнах для таких галузей як енергетика, хімічна промисловість, залізничний транспорт, охорона здоров'я, водопостачання, телекомунікації та медіа, тощо.

В цьому зв'язку, актуальним питанням при підготовці фахівців із боротьби з кіберзлочинами як раз і має бути – до яких стандартів в роботі вони повинні бути готові.

На нашу думку, майбутній працівник кіберполіції має володіти всіма сучасними інструментами в сфері кіберзахисту, орієнтований на роботу з новітніми системами та стандартами. Зрозуміло, що оволодіння національними стандартами буде вимагатися, але не тільки на них потрібно зосереджувати увагу при підготовці якісних кадрів для підрозділів кіберполіції.

Список бібліографічних посилань

1. Янковський О. Закон «Про кібербезпеку» як спроба тотального контролю // Українська правда : сайт газ. 10.06.2017. URL: http://www.pravda.com.ua/columns/2017/06/10/7146438/ (дата звернення: 01.11.2017).

Одержано 01.11.2017

УДК 342.9:351.74

Оксана Олександрівна ПАНОВА,
кандидат юридичних наук, доцент, доцент
кафедри адміністративної діяльності поліції факультету № 3
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-3533-5076

ОСОБЛИВОСТІ КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ПУБЛІЧНОЇ БЕЗПЕКИ В УКРАЇНІ

Сучасний стан політичного, економічного та культурного розвитку України, вимагають від суспільства та провладної групи звернути свою увагу на стан національної безпеки України, невід'ємною частиною якої є забезпечення публічної безпеки, дотримання норм правопорядку усіма суб'єктами та інституціями в державі.

Відповідно до положень Стратегії державної кадрової політики на 2012–2020 роки, основними цілями останньої є:

розроблення механізмів залучення до роботи у сферах державного управління висококваліфікованих фахівців, успішних підприємців, працівників фінансово-економічної сфери, здібних випускників вищих навчальних закладів;

відновлення технології добору кадрів для зайняття управлінських посад із числа працівників, які мають досвід роботи на посадах нижчого рівня у відповідній сфері діяльності;

формування дієвого кадрового резерву на зайняття керівних посад у сферах державного управління [7].

З метою, якісного розкриття теми доповіді, пропонується розглянути особливості кадрового забезпечення публічної безпеки крізь призму наведених вище цілей Стратегії державної кадрової політики на 2012–2020 роки.

По-перше, освоєння та впровадження в навчальний процес інноваційних методів навчання, використання інформаційно-технічних та пошукових ресурсі у вищих навчальних закладах зі специфічними умовами навчання, та тих закладах, де здійснюється підготовка спеціалістів за напрямами підготовки «правознавство» та «правоохоронна діяльність», активне залучення практичних працівників, патронаж молодого спеціаліста, адаптація майбутніх випускників ВНЗ до практичної роботи в нових умовах – основні шляхи залучення кваліфікованих кадрів до забезпечення публічної безпеки.

© Панова О. О., 2017