УДК 342.951

Ткачук Наталія Андріївна
канд. юрид. наук, співробітник СБ України,
м. Київ, Україна

ЦИФРОВА ГРАМОТНІСТЬ ТА КІБЕРГІГІЄНА В УКРАЇНІ

В умовах стрімкої діджиталізації одним із основних чинників негативного впливу на стан кібербезпеки України є низький рівень кібергігієни та ігнорування базових вимог кіберзахисту з боку громадян.

Найбільш чутливою категорією, при цьому, є співробітники органів державної влади, які мають доступ до державних електронних інформаційних ресурсів (у т.ч. реєстрів та баз даних), та працівники об'єктів критичної інфраструктури, які мають доступ до автоматизованих систем управління технологічними процесами вказаних об'єктів, а також особи, які відповідають за технічний захист таких ресурсів і систем.

Порушення вимог технічного захисту інформації з боку цієї категорії осіб уможливлює реалізацію таких загроз кібербезпеці держави як кібертероризм, кібершпигунство, виведення з ладу або блокування роботи державних інформаційних ресурсів, а також проведення масованих атак на об'єкти критичної інфраструктури України.

Причому, низький рівень культури безпечного поводження в кіберпросторі з боку таких суб'єктів фактично зводить нанівець будь які заходи із розбудови національної системи кібербезпеки та удосконалення технічної складової кіберзахисту, передбачені Законом України «Про основні засади забезпечення кібербезпеки України» [1] та Стратегією кібербезпеки України [2].

Незважаючи на гіркі уроки масштабних кібератак 2016-2018 років (у першу чергу вірусу Petya), спостерігається подальше ігнорування з боку відповідальних осіб органів державної влади вимог чинного законодавства у сфері технічного захисту інформації (ТЗІ).

До основних порушень належать:

- використання особистих технічних засобів у складі службових АС (н-д, USB-флеш накопичувачів);
- несанкціоноване підключення до комп'ютерів державних органів технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;
- використання службових мереж для доступу до особистої електро-

нної пошти, загальнодоступних та соціально-орієнтованих ресурсів мережі Інтернет;

- незахищеність інформаційно-телекомунікаційних систем (ІТС) державних органів за допомогою актуальних версій антивірусного програмного забезпечення.

Крім того, чинником негативного впливу, що обумовлює можливість втручання в роботу державних електронних інформаційних ресурсів з боку спецслужб країни-агресора, залишається використання в органах державної влади програмних продуктів російського походження, відмова від яких є не лише вимогою чинного законодавства, але й з огляду на сучасне безпекове середовище – має стати важливим елементом кібергігієни.

До основних причин низької культури безпечного поводження в кіберпросторі та недотримання вимог ТЗІ з боку співробітників держорганів, на нашу думку, належать:

1) відсутність базових теоретичних та практичних знань з кібергігієни;

2) відсутність серед кваліфікаційних вимог до держслужбовців вимог щодо цифрової грамотності;

3) халатне ставлення до положень нормативних актів у сфері ТЗІ та ігнорування потенційних негативних наслідків у разі їх порушення;

4) відсутність дієвого контролю як з боку керівництва держустанов, так і з боку Держспецзв'язку, щодо стану технічного захисту інформації в держорганах та притягнення до відповідальності посадових осіб, винних у порушені законодавства у сфері ТЗІ.

Також потребує підвищення стан цифрової грамотності та культури безпечного поводження в кіберпросторі серед працівників об'єктів критичної інфраструктури (ОКІ), рівень якого безпосередньо впливає на стан кіберзахисту таких об'єктів.

Серед основних порушень вимог технічного захисту інформації на ОКІ найбільш поширеними є наступні:

- інсталяція на службові ПЕОМ безкоштовних програмних додатків розважального характеру, що можуть мати недокументовані функції (ігор, медіаплеєрів, програм для завантаження відео-, аудіоконтенту тощо);
- використання нешифрованого/небезпечного протоколу (н-д, telnet, FTP та ін.) для передачі інформації конфіденційного характеру;
- відсутність централізованого ведення журналу подій у мережі та здійснення його аналізу;
- відсутність програми управління вразливостями та реагуванням на кіберінциденти;

- наявність активних і доступних для використання USB-портів, включаючи задіяні для функціонування периферійних приладів, а також безконтрольне використання бездротових пристроїв;
- наявність віддаленого контролю та доступу до інформації, що циркулює в ІТС об'єкта критичної інфраструктури, з боку представників іноземної компанії-виробника програмного забезпечення, яке використовується в управлінні технологічними процесами об'єкта;
- відсутність спеціалізованого підрозділу з кібербезпеки та кваліфікованого персоналу.

Крім того, чинником негативного впливу, що обумовлює можливість втручання в роботу ІТС об'єктів критичної інфраструктури з боку спецслужб країни-агресора, також залишається використання на вказаних об'єктах програмних продуктів російського походження.

Низький рівень кібергігієни та численні недоліки кіберзахисту об'єктів критичної інфраструктури обумовлені, у тому числі, відсутністю чітких нормативних вимог до власників/операторів таких об'єктів із захисту власних систем (вимоги, що на сьогодні розроблені Держспецзв'язку [3], є суто формальними за відсутності переліку ОКІ в Україні), а також відсутністю ефективного державного контролю у цій сфері.

Таким чином, на сьогодні, існує необхідність комплексного підходу на загальнодержавному рівні щодо підвищення цифрової грамотності й культури безпечного поводження в кіберпросторі та започаткування Національної програми кіберграмотності під егідою Національного координаційного центру кібербезпеки.

Державна політика у цій сфері повинна бути спрямована на вирішення наступних задач:

1. Формування належної мотивації та усвідомлення з боку цільової аудиторії (держслужбовців, операторів ОКІ, інших таргет-груп тощо) важливості цифрової грамотності та потенційних небезпечних наслідків у разі ігнорування базових вимог кібергігієни.

2. Забезпечення необхідної теоретичної та практичної підготовки у сфері кібергігієни в залежності від цільової аудиторії (н-р, проведення обов'язкових щорічних тренінгів та тестувань з кіберграмотності для держслужбовців, результати яких враховувати у подальшій атестації).

3. Формування чітких нормативних вимог у сфері кібергігієни та кіберзахисту.

4. Забезпечення ефективного моніторингу та контролю за станом кібергігієни (у першу чергу в органах державної влади та на об'єктах кри-

тичної інфраструктури) у т.ч. притягнення до відповідальності (дисциплінарної, адміністративної тощо) у разі порушення відповідних вимог.

Враховуючи комплексні аспекти цієї проблематики, реалізацію зазначених заходів є доцільним здійснювати в рамках Національної програми з кіберграмотності із залученням Міносвіти, Мінінформполітики, Держспецзв'язку, Нацполіції, Державного агентства з питань електронного урядування та інших зацікавлених державних органів, а також за широкої участі приватного сектору та міжнародних партнерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19.
2. Указ Президента України від 15 березня 2016 № 96.2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/96/2016.
3. Постанова Кабінету Міністрів України від від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.