

служба спеціального зв'язку та захисту інформації України, Служба безпеки України та низки інших, які вказані у ст. 8 даного Закону. Проте, у ньому не зазначений головний орган, який буде здійснювати оперативне командування всіма суб'єктами забезпечення кібербезпеки у мирний час [4].

На підставі вищевказаного, необхідно констатувати, що прийняття єдиного комплексного нормативного акта, який би регулював відносини кібербезпеки на національному рівні є вкрай важливим і необхідним для нашої держави на даний час. Однак, на наш погляд, Закон України «Про основні засади забезпечення кібербезпеки України» дуже сильно розширює повноваження державних органів влади, тим самим дозволяє їм втручатися у здійснення господарської діяльності суб'єктами господарювання.

Література:

1. Проект Закону про основні засади забезпечення кібербезпеки України [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.
2. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016 // Офіційний вісник Президента України. – 2016 р. – № 10. – Ст. 198.
3. Демедюк С.В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні [Електронний ресурс] / С. В. Демедюк // Південноукраїнський правничий часопис. – 2015. – № 3. – С. 119-123. – Режим доступу: http://nbuv.gov.ua/UJRN/Pupch_2015_3_39.
4. Що не так із законопроектом про кібербезпеку та як його вдосконалити [Електронний ресурс]. – Режим доступу: <https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci>.

Сучасний стан та розвиток національної системи кібербезпеки України

Олійник Ю.С.

студент Навчально-наукового
інституту інформаційної безпеки
Національної академії СБ України

Климчук О.О.

кандидат юридичних наук, доцент,
завідувач кафедри Національної академії СБ України

Сьогодні наше життя майже неможливо уявити без використання інформаційних технологій. Інформаційне суспільство знаходиться постійно у русі і щодня набуває нових форм, які в кінцевому результаті впливають на формування думок, світогляду та звичок. Віртуальний світ стає буквально всеохоплюючим. Інформаційні технології з кожним днем все більше інтегруються в наше життя. І, як наслідок, це набагато полегшує наше сьогодення, зокрема, набагато простішою та швидшою стала робота державних установ, промисловості, сфери послуг. Все більше у своєму житті використовують новітні інформаційні технології й звичайні громадяни, для яких той же Інтернет став складовою повсякденного життя.

Однак є й інша сторона медалі - у переході нашої життєдіяльності у кіберпростір, наявні так звані «темні» сторони. Увесь світ постає перед новим, досі невідомим видом загроз. Несанкціоноване втручання в роботу комп'ютерних та телекомунікаційних мереж, виготовлення та розповсюдження шкідливих програмного забезпечення, атаки на об'єкти критичної інфраструктури, втручання у політичні процеси в країнах та особисте життя громадян, що в переважній більшості носить транснаціональний організований характер – все це негативна сторона розвитку інформаційних технологій.

На жаль, Україна є однією з країн, яка зараз надзвичайно гостро відчуває на собі усі так звані «побічні ефекти» еволюції інформаційного суспільства. Розповсюдження комп'ютерних вірусів, атаки на українські об'єкти фінансового та енергетичного секторів, викрадення інформації – це ще не повний перелік кіберзлочинів, які відомі в Україні.

Водночас набирає нових обертів процес становлення та розвитку національної системи кібербезпеки України.

15 березня 2016 р. в Україні – день, котрий став відомим завдяки прийняттю важливого документу для захисту національного кіберпростору – Стратегії кібербезпеки України [1]. Також необхідно згадати та відзначити Рішення Ради національної безпеки та оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» від 13 лютого 2017 р., яким ініційовано

підготовку законодавчих пропозицій, та вжиття невідкладних заходів щодо забезпечення повного та об'єктивного розслідування кібератак на інформаційно-телекомунікаційні системи фінансового сектору держави [2].

Відповідні заходи у сфері кіберзахисту вживаються й у правоохоронній сфері України. Так, у грудні 2011 р. було створено Департамент по боротьбі з кіберзлочинністю МВС України, а на початку 2012 р. були утворені відповідні територіальні підрозділи. Новим етапом у протистоянні з кіберзлочинністю в Україні стало створення 13 жовтня 2015 р. Кіберполіції, як структурного підрозділу Національної поліції [3]. Також варто згадати про заснований ще у 2007 році спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України – Команда реагування на комп'ютерні надзвичайні події України (CERT-UA). В СБ України теж існує підрозділ, до компетенції якого входить протидія кіберзлочинності – це Департамент контррозвідального захисту інтересів держави у сфері інформаційної безпеки [4]. Також слід заголосити увагу на Національному координаційному центрі кібербезпеки – робочому органі Ради національної безпеки і оборони України. Центр має забезпечити координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки [5].

Але, на превеликий жаль, зараз доводиться констатувати, що правоохоронним органам рідко вдається передбачити кібератаки та попередити державні органи про можливі кіберзагрози. Діяльність правоохоронців в більшості – це ліквідація наслідків, аніж їх недопущення. Це можна пояснити відсутністю необхідної кількості фахівців в правоохоронних органах, недостатнім рівнем підготовки діючих кадрів в сфері кібербезпеки, неконкурентною оплатою їх праці в порівнянні з їх цивільними колегами.

Також наявні проблеми й в такому важливому процесі, як співробітництво спеціальних структур з приватним бізнесом, який має власний досвід і напрацювання протидії кіберзагрозам. Існують моменти, коли силовики зловживають своїми повноваженнями створюючи перешкоди для бізнесменів. Від цього довіра один до одного тільки втрачається і вже ні про яке співробітництво не може йти мова. А звідси – і про посилення кібербезпеки держави.

Загалом, які б не створювалися умови для «чистого» використання інтернет-простору, та все ж основна боротьба з кіберзлочинністю залежить насамперед від самих громадян, які часом легковажно відносяться до захисту персональної інформації. Дуже часто зазначені дані перехоплюються в публічних місцях із відкритим Wi-Fi доступом під час користування електронною поштою або соціальними мережами. Для попередження таких випадків спеціалісти радять користуватися засобами захисту інформації, які пропонуються поштовими серверами або соціальними мережами. Проте найкращим захистом від викрадення персональних даних в Інтернеті є наявність в ньому мінімальної інформації про себе, або ж взагалі її відсутність.

На державному рівні питання про кіберзахист має необхідність у набутті системного характеру. Можна говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і росту ролі в цьому приватного сектора; встановлення контролю над «кіберзброєю», а також посиленням охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки; вдосконалення освітніх напрямів підготовки фахівців даної сфери діяльності; впровадження на національному та міждержавному рівнях обміну інформацією про кібербезпеку, тощо. Однак без системного та комплексного підходу всі зазначені підходи не дозволять вивести рівень кібербезпеки, а звідси – і національної безпеки України загалом, на новий якісний рівень.

Література:

1. Указ Президента України від 15.03.2016 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу : <http://www.president.gov.ua/documents/962016-19836>;
2. Указ Президента України від 13.02.2017 № 32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [Електронний ресурс]. – Режим доступу : <http://www.president.gov.ua/documents/322017-21282>;
3. Постанова Кабінету Міністрів від 13.10.2015 № 831 «Про утворення територіального органу Національної поліції [Електронний ресурс]. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/831-2015-%D0%BF>;