Сабіщенко О.В.
студент;
Мокрієв М.В.
кандидат економічних наук, доцент,
Національний університет біоресурсів і природокористування України

ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРПРОСТОРУ ТА НАПРЯМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Кіберпростір дедалі частіше використовується для шпигунства, несанкціонованого доступу до інформації та для досягнення політичних і кримінальних цілей, він став інструментом терористів і криміналітету. Російська агресія проти України супроводжується спробами блокувати штатний режим роботи державних інформаційних ресурсів та об'єктів критичної інфраструктури. Так, наприкінці минулого року працівниками Служби безпеки попереджено хакерську атаку на енергооб'єкти України, виявлено шкідливе програмне забезпечення в мережах окремих обласних енергопідприємств.

Українські користувачі на першому місці в Європі за ризиком кіберзагроз. Так, зараження через локальне встановлення відбувається у 54,7% випадків, зараження через Інтернет, за відсутності процесів всередині організацій, – 35,7%, зараження мобільними загрозами через мобільні пристрої – 8,39%. Українські користувачі значною мірою схильні до зараження через неоновлення програмного забезпечення. Наприклад, 17% усіх заражень, відбувається внаслідок використання застарілої операційної системи Windows XP. Також, Україна посіла п'яте місце у світі та перше в Європі за ризиком зіткнення з веб-загрозами [5].

Україна в загальносвітовому кіберпросторі посідає насправді значне місце. За словами Гарі Маків, стратегічного аналітика European Cyber Crime Centre (EC3), Europol «... в Україні сильно обмежені тим, що ми самі можемо знайти в інтернеті.», проте «... українські правоохоронці та експерти – важлива частина світового правопорядку і неодноразово продемонстрували як бажання брати участь у розслідуваннях, так і свою ефективність» [6].

Саме тому, завданням держави є прискорення розбудови національної системи забезпечення кібербезпеки. Це означає вдосконалення механізму державного управління в цій сфері, формування відповідної нормативно-правової бази, інтегрування до системи колективної безпеки НАТО та розробку власних кіберзахисту і кіберзброї [5].

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку.

Враховуючи викладене, інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є

важливою самостійною сферою забезпечення національної безпеки. У зв'язку з цим, забезпечення інформаційної безпеки у процесі використання інформаційно-комунікаційних технологій є однією з найважливіших умов успішного розвитку інформаційного суспільства [3].

В Україні питаннями кібербезпеки переймаються кілька державних відомств (мають спеціальні підрозділи): СБУ, МВС, Державна служба спеціального зв'язку та захисту інформації, Міністерство оборони України [7]. Незважаючи на таку розгалуженість відомств, що займаються кібербезпекою, ми маємо проблеми, які потребують стратегічного вирішення.

Останнім часом держава здійснила ряд заходів, спрямованих на посилення кібербезпеки:

1. З 1 липня 2015 року в Державній службі спеціального зв'язку та захисту інформації розпочав роботу Державний центр кіберзахисту та протидії кіберзагрозам. Його завдання – оцінити стан захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах органів державної влади.

2. Створено Трастовий фонд Україна – НАТО з питань кібербезпеки. Його мета – надання фінансово-консультативної та методичної допомоги державами – членами Північноатлантичного альянсу у справі розбудови національної системи кібербезпеки, налагодження взаємодії з відповідними органами іноземних держав та міжнародними організаціями.

3. У жовтні минулого року утворено Департамент кіберполіції Національної поліції України, який боротиметься з кіберзлочинністю.

4. Україна взяла участь в деяких міжнародно-правових заходах боротьби з кіберзлочинністю [5].

Крім того, Указом Президента України від 15.03.2016 № 96/2016 затверджено Стратегію кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1].

Вказана Стратегія передбачає, що розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у:

– виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

– створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

– формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;

– розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

– залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі;

– розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

– розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;

– розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;

– створенні умов для впровадження в Україні сучасних технологій кіберзахисту [1].

Удосконалення системи державного реагування на сучасні виклики та загрози інформаційній безпеці потребує цілеспрямованого вивчення зарубіжного досвіду організації і проведення інформаційних операцій, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів. Все це дає можливість стверджувати, що система забезпечення інформаційної безпеки має бути міжвідомчою і ієрархічно організованою, її структура і організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів [4]. Окремо постає питання тіснішої співпраці зі світовими системами кіберзахисту та інтеграції в міжнародну систему безпеки.

Список використаних джерел:

1. Указ Президента України від 15 березня 2016 р. № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» // Урядовий кур'єр, 2016, 03, 18.03.2016 № 52.

2. Указ Президента України від 01 травня 2014 р. № 449/2014 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» // Офіційний вісник України, 2014, № 37 (16.05.2014), ст. 986.

3. Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 356 «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» // Офіційний вісник України, 2013, № 44 (21.06.2013), ст. 1581.

4. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці [Електронний ресурс] http://www.dy.nayka.com.ua/?op=1&z=747

5. Парламентські слухання Верховної Ради України на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» від 3 лютого 2016 року [Електронний ресурс] http://static. rada.gov.ua/zakon/new/ par_sl/sl0302116.htm

6. Ярова М. Кібербезпека в Україні: У 2015 році наша країна – «найгарячіша» точка Європи [Електронний ресурс] http://news.finance.ua/ua/news/-/363836/kiberbezpeka-v-ukrayini-u-2015-rotsi-nasha-krayina-najgaryachisha-tochka-yevropy

7. Дубов Д. В. Стратегічні аспекти кібербезпеки України / Д. В. Дубов // Стратегічні пріоритети. – 2013. – № 4. – С. 119-127.