УДК 621.391

Пташко П.М.
Центральноукраїнський національний технічний університет

Кібербезпека в Україні: 2016 та прогнози на майбутнє

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 IT 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.

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 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. Україна кожен рік потрапляла в антирейтингові списки щодо піратства, розповсюдження шкідливого програмного забезпечення, DDoS атак та інше. Так, відповідно до дослідження корпорації Майкрософт (Microsoft Corporation), на 86% комп'ютерів в Україні встановлене неліцензійне програмне забезпечення. В той же час в центральних органах державної влади України використовують 60% неліцензійного програмного забезпечення. Як відомо, «безкоштовний сир - лише в мишоловці», а відтак використання неліцензійного програмного забезпечення - це прямий шлях для надання доступу хакерам до ресурсів систем, на яких воно встановлено.

Поточна ситуація в Україні також не вселяє оптимізму. Експерти Kaspersky Lab сформулювали перелік загроз, які роблять нашу країну однією з головних «гарячих точок» на кіберкарті світу. Вісім тез про кібербезпеку в Україні:

1. Українські користувачі у високому ступені схильні до зараження через неоновлення програмного забезпечення і піратські копії програм. Показово також, що 17% всіх заражень припадає на користувачів, що працюють із застарілою операційною системою Windows XP.

2. Нерідко спамери для розсилки «нігерійських листів» спекулюють на темі політичної ситуації в Україні або ж розсилають

листи від імені «російських наречених»: дівчат з Росії та України, які скаржаться на свою нелегку долю і просять перевести на їх рахунку деякі кошти.

3. Україна посіла п'яте місце в світі (і перше в Європі) за ризиками зіткнення з веб-погрозами в третьому кварталі 2015 року. За даними, Kaspersky Security Network за липень-вересень 2015 третина (33,7%) українських користувачів мережі зіткнулися з погрозами, що поширюються через інтернет.

4. За тим же показником, за період з січня по вересень 2 015 р. Україна посідає третю сходинку рейтингу країн з найбільшим ризиком зараження через інтернет: 35,7% користувачів зіткнулися з веб-погрозами за звітний період.

5. За результатами другого кварталу 2015 року, Україна опинилася на 9 сходинці рейтингу країн з найбільшим ризиком зараження мобільними зловредами (8,39%). Досить високий для українців і ризик зіткнення з локальними погрозами (54,5%). Сюди потрапляють об'єкти, які проникли на комп'ютери шляхом зараження файлів або знімних носіїв або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, програми в складі складних інсталяторів, зашифровані файли і т.д.). За цим показником країна займає передостанню сходинку в топ-20 по світу, але перше в Європі.

6. В Україні було відзначено велику кількість спрацьовування антивіруса на програми-вимагачі і шифрувальники – шкідливі програми, мета яких – заблокувати пристрій або браузер або зашифрувати файли користувача, зробивши їх недоступними без спеціального ключа, за який потрібно заплатити викуп.

7. Серед жертв Turla – однієї з найскладніших кібершпіонських кампаній, яка діє вже більше 8 років, були виявлені комп'ютери українських чиновників. Угруповання, яка стоїть за Turla, заразило сотні комп'ютерів більш ніж в 45 країнах світу, що належать, зокрема, державним установам, посольствам, військовим, дослідницьким центрам і фармацевтичним компаніям. Метою кіберзлочинців є збір необхідних або конфіденційних даних з комп'ютера жертви.

8. Також українці були серед жертв таких кампаній, як CosmicDuke, MiniDuke, Agent.btz, Epic Turla, TeamSpy, BlackEnergy і Red October.

Всі виклики та загрози національній безпеці України в кібернетичному просторі призвели нарешті до появи довгоочікуваної Стратегії кібербезпеки України (далі Стратегія), що булла введена в дію указом Президента України від 15 березня 2016 року. Метою створення стратегії було забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави.

Стратегія є важливим кроком на шляху розбудови системи кібербезпеки України та являє собою програму дій, за якою мають слідувати державні органи. Нарешті в стратегічному документі поставлено завдання щодо формування державного реєстру об'єктів критичної інформаційної інфраструктури, а на власників цих об'єктів покладені зобов'язані створити підрозділи атестованих спеціалістів з IT-безпеки для оперативного виявлення загроз та реагування на інциденти. Також, пунктами «Стратегії» передбачено створення підрозділів із забезпечення кіберзахисту ЗС України як на стратегічному, так і на оперативному і тактичному рівнях. Відповідальність за кібербезпеку у фінансовій сфері покладено на Нацбанк, що має сформувати власні вимоги до банків та інших суб'єктів фінансового ринку, а приватний бізнес визнається повноправним суб'єктом системи кібербезпеки в Україні. Окрім цього, вперше на правовому рівні закріплюється поняття активного кіберзахисту, тобто організація кібератаки у відповідь на загрози. На підставі Стратегії, в червні місяці 2016 року був створений Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, а також затверджений план заходів на 2016 рік з реалізації Стратегії кібербезпеки України.