Liubokhynets Larisa

PhD in Economics, Associate Professor

Khmelnytskyi National University (Ukraine, Khmelnytskyi)

Zhelichovskyi Arthur

student of the Faculty of Economics and Management

Khmelnytskyi National University (Ukraine, Khmelnytskyi)

THREATS OF THE INFORMATION SECURITY AND METHODS OF THEIR NEUTRALIZATION

Любохинець Л.С.

канд. екон. наук, доцент

Хмельницький національний університет

Желіховський А.Л.

студент факультету економіки та управління

Хмельницький національний університет

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ТА МЕТОДИ ЇХ НЕЙТРАЛІЗАЦІЇ

In the article the threats of the information security reviewed, the types and groups of information threats, methods of their neutralization identified, the system of policy measures to ensure information security presented.

Key words: *information security, information, threats to information security, informatization policy.*

У статті розглянуто загрози інформаційній безпеці, визначено типи та групи інформаційних загроз, методи їх нейтралізації, представлено систему заходів політики із забезпечення інформаційної безпеки

Ключові слова: *інформаційна безпека, інформація, загрози інформаційній безпеці, політика інформатизації.*

Розвиток інформаційного суспільства змінює геополітичний стан глобальних систем, впливає на формування нових сфер функціонування господарських суб'єктів та життєдіяльності людства, тому актуальною стає проблема захисту інформації на всіх рівнях економічного, політичного, військового, правового регулювання економіки. З розвитком інформаційних технологій відбувається і розвиток кіберзлочинності, яка використовує у своїх протизаконних діях вразливі сторони інформаційних систем, а проникнення інформаційних технологій в різні сфери суспільного розвитку призводить до стрімкого зростання обсягів інформації, яка потребує обробки, захисту та збереження. Через низьку захищеність національних інтересів в інформаційній сфері від внутрішніх та зовнішніх загроз ми піддаємось кібератакам з боку різних країн, організацій та «хакерів». Всі вони направлені на дезорієнтацію роботи підприємств, організацій, державних установ, населення та учинення збитків в соціальній та економічній сферах життєдіяльності країни.

Аналіз проблем інформаційної безпеки потребує детального розгляду загроз, які виникають в інформаційному середовищі та шляхів їх нейтралізації. Загрози інформаційній безпеці – це сукупність умов, процесів та чинників, що перешкоджають реалізації національних інтересів або створюють небезпеку життєво важливим інтересам особистості, суспільства й держави в інформаційній сфері [1, с.14; 2, с.24], явні чи потенційні дії зовнішніх та внутрішніх суб'єктів, які створюють небезпеку для системи державного управління, життєзабезпечення її системоутворюючих елементів. Як результат, загрози інформаційній безпеці можуть призвести до порушення достовірності, цілісності та конфіденційності інформації, що зберігається, передається або обробляється [3, с.36]. Виділяють політичні, економічні, суспільні, військові, організаційно-технічні типи інформаційних загроз, які в свою чергу можуть класифікуватись в глобальні, регіональні та локальні. Основні загрози інформаційній безпеці можна розділити на такі групи:

- загрози впливу неякісної (недостовірної, фальшивої, дезінформації) інформації на особистості, організації, суспільство, державу;
- загрози інформаційному забезпеченню державної політики країни;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію та інформаційні ресурси;
- загрози інформаційним правам і свободам особистості;
- загрози безпеці інформаційно-телекомунікаційних систем організацій та державних установ.

Інформація стала чинником, під впливом якого зростає потенційна вразливість суспільних процесів, відбувається дезорганізація державного управління, можуть виникати великомасштабні аварії, військові конфлікти, стихійні лиха. Серед інцидентів, пов’язаних з порушенням роботи промислових систем управління (ICS - Industrial Control System), можна виділити такі, як вимкнення зв'язку з вежею управління повітряним рухом в аеропорту Ворчестер, штат Массачусетс підлітковим хакером у березня 1997р. В результаті аварії було вимкнено телефонну службу на контрольній башті, пожежному відділі аеропорту, службі погоди, крім того, не працював принтер, який використовували для моніторингу польотів в аеропорту. Весною 2000р. Вітек Боден (Vitek Boden), незадоволений австралійський інженер системи SCADA компанії Maroochy Water Services, спровокував вилив 800 тисяч літрів стічних вод в місцеві парки, річки і навіть на територію готелю Hyatt Regency. 25 січня 2003 року вірус SQL Slammer на 5 годин вивів з ладу систему моніторингу безпеки атомної електростанції Davis-Besse в Огайо. У 2010 році відбулася одна із масштабних атак на систему ICS на атомній електростанції Натанз в Ірані. У 2014 році один із сталеливарний заводів Німеччини підтвердив факт кібератаки на ICS-мережу, яка не дозволяла відключити доменну піч коректним способом. 23 грудня 2015 року зловмисникам вдалося відключити не менше 7 підстанцій, які працюють під напругою 110 кВ, і 23 підстанції, що працюють під напругою 35 кВ. на українських підприємствах

Прикарпаттяобленерго і Київобленерго. Атака на системи SCADA цих підприємств залишила без електрики близько 80 тисяч осіб на 6 годин [4].

Кожне порушення механізму захисту бази даних може паралізувати роботу цілих корпорацій, призвести до значних матеріальних втрат. Як показують дослідження антивірусної лабораторії PandaLabs компанії Panda Security, кожну секунду здійснюється викрадення 122 записів з баз даних. В 2017 році випадкові втрати даних в результаті необережності досягли найвищого рівня. Хоча вони є причиною лише 18% інцидентів в сфері інформаційної безпеки, але призвели до втрати 1,6 млрд. записів з баз даних, в тому числі компанії Rivers City Media, що склало 86% від всієї кількості викрадених даних. В першому півріччі 2017 року було зареєстровано 918 порушень безпеки в рамках проекту Gemalto's Bresch Level Index, це призвело до втрати майже 2 мільярдів записів, що на 164% більше ніж за весь 2016 рік [5].

В першій половині 2017 року були проведені дві самі великі кібер-атаки WannaCry та GoldenEye/Petya, від яких постраждали майже всі країни світу і велика кількість компаній, більше 230 000 комп'ютерів. За різними оцінками експертів, втрати від цих атак склали від 1 до 4 млрд. дол. США, тобто від 4300 до 17000 дол. в розрахунку на кожний комп'ютер. В цей же період був атакований веб-хостінг Nayana в Південній Кореї, в результаті було зашифровано даних на 153 серверах Linux. Злочинці вимагали викуп в розмірі 1,62 млн. дол. США, але, після перемовин, компанія виплатила їм 1 млн. дол. США [6, с.11-12]. 14 грудня 2017 року Федеральна комісія із зв'язку США проголосувала за скасування принципу «мережевого нейтралітету», який зобов'язував інтернет-провайдерів однаково ставитися до будь-якого трафіку. Як результат, активісти руху Anonymous пригрозили здійснити серію кібератак на online-ресурси Федеральної комісії зі зв'язку США (Federal Communications Commission, FCC) у відповідь на рішення про скасування принципу «мережевого нейтралітету».

Як показує практика справжні масштаби кібератак набагато серйозніші. Так, у 2016 році, за результатами звіту «2016 Internet Grime Report», Центр обробки скарг інтернет-злочинності США отримав в цілому 298 728 скарг, з повідомленнями про збитки, що перевищують 1,3 млрд. дол. США. [6, с.13]. Те, що оприлюднюють медіа, є незначним просоченням резонансної інформації, яка має привернути увагу громадськості до цієї проблеми. Зокрема, у відповідь на посилення позицій Китаю в кіберпросторі Пентагон нарощує зусилля з протидії засобам кібервійн. Агентства оборонних перспективних дослідницьких проектів (DARPA) працює над проектом National Cyber Range (NCR), пов'язаним з розроблення програми, яка дасть можливість в оперативнішому режимі й більш системно оцінювати готовність національних інформаційних мереж до відбиття хакерських нападів. DARPA уклала контракт з Lockheed Martin (орієнтовна сума – 31 млн дол. США) на створення нової версії Інтернету для військових цілей з новим протоколом під кодовою назвою Military Network Protocol (MNP), що має забезпечити підвищену безпеку та динамічний перерозподіл пропускної здатності каналів навіть в умовах масованих кібератак [7, с.399].

Кожній із загроз безпеці в різних сферах інформаційного життя необхідно протиставити певні заходи, способи, методи їх нейтралізації, захисту інформаційного ресурсу, баз даних, національного інформаційного простору. Як зазначається в Концепції інформаційної безпеки держав-учасників Співдружності Незалежних Держав у військовій сфері, основним завданням із забезпечення інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації, а також несанкціоноване її поширення [8]. Для цього необхідно формувати систему заходів політики із забезпечення інформаційної безпеки, що будуть базуватися на принципах законності, дотримання балансу інтересів зацікавлених сторін, з їх взаємною відповідальністю, інтеграції систем національної та міжнародної безпеки. Така система має включати правові, організаційно-технічні та управлінсько-економічні методи забезпечення інформаційної безпеки. До правових відносять

розвиток законодавчої та нормативно-правової бази забезпечення інформаційної безпеки та державної політики інформатизації, вдосконалення форм та методів запобігання і нейтралізації загроз безпеці інформаційного середовища, забезпечення доступу до публічної інформації щодо боротьби з кіберзлочинністю, формування правового статусу користувачів інформаційних та телекомунікаційних систем. Організаційно-технічні методи мають включати розробку та удосконалення, а також сертифікацію систем способів захисту інформації, методів контролю за їх ефективним використання, створення системи інструментів запобігання несанкціонованому доступу до інформації, застосування криптографічних засобів захисту інформації. Управлінсько-економічні методи забезпечення інформаційної безпеки містять розробку основних напрямів державної політики в сфері інформатизації, захисту державних інформаційних ресурсів, створення умов для якісного й ефективного інформаційного забезпечення всіх зацікавлених сторін, підтримку проектів і програм інформатизації, страхування інформаційних ризиків.

Забезпечення інформаційної безпеки сьогодні вимагає пошуку перспективних шляхів тісної взаємодії й координації державних та недержавних структур у системі національної безпеки, при цьому ключовою передумовою успішної імплементації рішень у системі національної та інформаційної безпеки є необхідність єднання навколо цього питання інтелектуальної, економічної і політичної еліт, співробітництва між урядами держав, міжнародними партнерами та бізнесом.

Література:

1. Обгрунтування концептуальних та організаційно-правових засад розробки паспортів загроз національній безпеці України: навчально-методичний посібник / за заг.ред. Г.П. Ситника – К.: НАДУ, 2012 – 52с.

2. Дзьобань О.П. Національна безпека в умовах соціальних трансформацій: Методологія дослідження та забезпечення / О.П. Дзьобань. – Х.: Константа, 2006. – 440с.

3. Нашинець-Наумова А. Концептуальні підходи щодо забезпечення національної безпеки: інформаційно-правові та інституційні засади / А. Нашинець-Наумова. // Підприємництво, господарство і право. – 2017. – № 1. – С. 34─38.

4. Введение в безопасность систем ICS/SCADA [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/analytics/487977.php

5. Количество инцидентов с кражей данных продолжает расти [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/blog/company/PandaSecurityRus/342992.php

6. Panda labs - Отчет за 2 квартал 2017. [Електронний ресурс]. – Режим доступу: https://pandasecurity.bitrix24.ru/docs/pub/1c3e16b44b7eced067ca1ceb9ae381ce/default/?&

7. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці / О.С. Власюк. – К. : НІСД, 2016. – 528 с.

8. Концепції інформаційної безпеки держав-учасників Співдружності Незалежних Держав у військовій сфері[Електронний ресурс]. – Режим доступу: https://www.ngo.dn.ua