МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
МАРІУПОЛЬСЬКА МІСЬКА РАДА
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В ДОНЕЦЬКІЙ ОБЛАСТІ
ДОНЕЦЬКЕ УПРАВЛІННЯ КІБЕРПОЛІЦІЇ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Збірник матеріалів наукового круглого столу

«КІБЕРБЕЗПЕКА ТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: ВИКЛИКИ СЬОГОДЕННЯ»

26 ЖОВТНЯ 2017 РОКУ

Маріуполь – 2017 р.

УДК 004.49(08)
ББК 32.97

Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р. / Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – 104 с.

Рекомендовано до друку засіданням Вченої ради економіко-правового факультету Маріупольського державного університету (протокол № 2 від 18 жовтня 2017 р.)

ТОЛЮПА С. В., д.т.н., професор
КНУ імені Тараса Шевченка

СИСТЕМИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ВИЯВЛЕННЯ ОЗНАК КІБЕРАТАК

Однією з ключових проблем, які в умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства постали перед усіма державами світу, є проблема захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, від викликів і загроз у кібернетичному просторі. Можливості кібернетичного простору, лавиноподібний процес розвитку та впровадження новітніх інформаційних і телекомунікаційних технологій забезпечують безпрецедентні умови для накопичення й використання інформації, а також створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об’єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності й конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам. При цьому особливу занепокоєність викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення військово-політичного та силового протиборства, тероризму та проведення хакерських атак.

В даний час для захисту інформації потрібна не просто розробка приватних механізмів кіберзахисту, а реалізація системного підходу, що включає комплекс взаємопов’язаних заходів. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання кіберзагроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення й знищення службової інформації, забезпечення в рамках діяльності установи.

Системи виявлення мережевих вторгнень і виявлення ознак кібератак на інформаційні системи вже давно застосовуються як один з необхідних рубежів оборони інформаційних систем. Розробниками систем захисту інформації та консультантами в цій галузі активно застосовуються такі поняття, як захист по периметру, стаціонарна і динамічний захист, стали з'являтися власні терміни, наприклад, проактивні засоби захисту.

На сьогодні системи виявлення вторгнень і кібератак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем кібербезпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі мережі за останні роки значно збільшилася, системи виявлення кібератак (СВКа) стали необхідним компонентом інфраструктури безпеки більшості організацій.

Взагалі кажучи, сучасні системи виявлення вторгнень і кібератак ще далекі від ергономічних і ефективних, з точки зору безпеки рішень. Підвищення ефективності ж слід ввести не тільки в області виявлення зловмисних дій на інфраструктуру захищених об'єктів інформатизації, але і з точки зору повсякденної експлуатації цих засобів, а також економії обчислювальних та інформаційних ресурсів власника даної системи захисту.

Якщо говорити безпосередньо про модулі обробки даних, то, кожна сигнатура кібератаки в системі обробки інформації про кібератаку є базовим елементом для розпізнавання більш загальних дій — розпізнавання фази кібератаки (етапи її реалізації). Саме поняття сигнатури узагальнюється до деякого вирішального правила. А кожна кібератака навпаки розбивається на набір етапів її проведення. Чим простіше кібератака, тим простіше її виявити і більше з'являється можливостей щодо її аналізу.

Сценарій кібератаки представляє собою граф переходів, в аналогічний графу кінцевого детермінованого автомата. А фази кібератак можна описати, наприклад, наступним чином: випробування портів; ідентифікація програмних і апаратних засобів; збір банерів; застосування експлойтів; дезорганізація функціоналу мережі з допомогою атак на відмову в обслуговуванні; управління через бекдори; пошук встановлених троянів; пошук проксі-серверів; видалення слідів присутності і т. д. (за необхідності з різним ступенем деталізації).

Переваги такого підходу очевидні - у разі роздільної обробки різних етапів кібератаки з'являється можливість розпізнавати кіберзагрозу ще в процесі її підготовки і формування, а не на стадії її реалізації, як це відбувається в існуючих системах. При цьому, елементною базою для розпізнавання може бути як сигнатурний пошук, так і виявлення аномалій, використання експертних методів та систем, довірчих стосунків та інших інформаційних, вже відомих і реалізованих, мережевих і локальних примітивів оцінки того, що відбувається в інформаційному середовищі потоку подій. Узагальнюючий підхід до аналізу дозволяє визначати відповідно й розподілені (у всіх сенсах) кіберзагрози, як у логічному так і фізичному просторі. Загальна схема обробки вступників подій також дозволяє здійснювати пошук розподілених кібератак - шляхом подальшої агрегації даних з різних джерел і конструювання мета-даних про відомі інциденти.

Системи виявлення кібератак, як і більшість сучасних програмних продуктів, повинні задовольняти ряду вимог. Це і сучасні технології розробки, і орієнтування на особливості сучасних інформаційних мереж і сумісність з іншими програмами. Щоб зрозуміти, як правильно використовувати СВКа, потрібно чітко представляти, як вони працюють і які їх вразливі місця.

Якщо не враховувати різні несуттєві інновації в області виявлення кібератак, то можна сміливо стверджувати, що існують дві основні технології побудови СВКа. Суть їх полягає в тому, що СВКа володіють певним набором знань про методи вторгнень.

Системи виявлення аномального поведінки засновані на тому, що СВКа відомі деякі ознаки, що характеризують правильне чи допустиме поведінку об'єкта спостереження.

Сучасний підхід до побудови систем виявлення кібератак на інформаційні системи сповнений недоліків і вразливостей, що дозволяють, на жаль, шкідливим впливам успішно долати системи захисту інформації. Перехід від пошуку сигнатур кібератак до виявлення передумов виникнення загроз інформаційної безпеки має сприяти тому, щоб докорінно змінити дану ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їх подолання. Крім того, такий перехід має сприяти підвищенню ефективності управління інформаційною безпекою і, нарешті, більш конкретних прикладів застосування нормативних і керівних документів, що вже стали стандартами.

Найбільш широко кіберзагрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення кіберзагрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом, як уразливість. Інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання, вважаємо, що можна виділити такі види кіберзагроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

Список використаних джерел

1. Debar, H., Dacier, M., and Wespi, A. (1999), “Towards a Taxonomy of Intrusion Detection Systems,” Computer Networks, vol. 31, 1999, pp. 805-22

2. Debar, H., Dacier, M., and Wespi, A. (2000), “A Revised Taxonomy for Intrusion-Detection Systems,” presented at Annales des Télécommunications, vol. 55, 2000, pp. 361-78

3. Kabiri, P., and Ghorbani, A., A. (2005), “Research on Intrusion Detection and Response: A Survey”, International Journal of Network Security, Vol.1, No.2, Sep. 2005, pp.84-102

4. Amer, S.H., Hamilton, J.A., “Intrusion Detection Systems, (IDS) Taxonomy – A Short Review,” DOD Software Tech News, vol. 13, no. 2, June 2010, DOD Data & Analysis Center for Software, Air Force Research Laboratory, Rome, N.Y., pp. 23 - 30

ТИМЧУК О. С., к.т.н., Донецький національний університет імені Василя Стуса

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Рівень захищеності IT інфраструктури підприємства залежить від коректної оцінки ризиків кібербезпеки використовуваних IT сервісів і, як наслідок, ефективності обраних контрзаходів з безлічі доступних [1]. Збільшення складності, взаємозв'язку і швидкі зміни, що відбуваються в IT сервісах, унеможливлюють застосування традиційних моделей кількісної / якісної оцінки ризиків кібербезпеки. Існуючі моделі кількісної оцінки вимагають значних витрат часу, а моделі якісної оцінки [2] не дозволяють враховувати вплив суб'єктивних оцінок експертів і невизначеність факторів ризику. Основні причини суб'єктивізму:

- нерішучість експертів при обміні інформацією в присутності керівників відділів підприємства;
- домінування досвідчених експертів при обговореннях в групах;
- складність зіставлення різноспрямованих думок експертів;
- складність збору і аналізу експертних оцінок.

Основні причини невизначеності:

- серед фахівців відсутня однозначна інтерпретація факторів ризику;
- фактори ризику представлені словесним описом, що носить інтуїтивний характер;
- тимчасові ряди факторів ризику мають нелінійну структуру.

У цій доповіді пропонується модель оцінки ризиків кібербезпеки, яка побудована на базі методології ранжирування ризиків відкритого проекту забезпечення безпеки web-додатків OWASP [3]. В роботі проблема суб'єктивізму експертів вирішується за допомогою методів теорії вербальних обчислень і уявлень [4]. Для оцінки факторів ризику експертам пропонується використовувати словник, що складається з 16/32 гранульованих терма (слова). Проблеми невизначеності, що виникають при вербальній оцінці факторів ризику, враховуються за допомогою методів теорії дискретних інтервальних нечітких множин та систем другого типу (DIT2FSs і DIT2FLSs) [5].

Представимо модель оцінки ризиків кібербезпеки

$$\sum_{i=1}^{I} r_i x_i \rightarrow \max,$$
$$\sum_{i=1}^{I} a_i x_i \leq S,$$
$$a_i > 0,\ c_i \geq 0,$$
$$x_i \in \{0,1\},$$

де r_i – рівень і-го ризику,

x_i – логічна змінна - ознака прийняття рішення про нейтралізацію і-го ризику,

a_i – витрати на нейтралізацію і-го ризику,

S – бюджет, виділений підприємством для нейтралізації ризику.

Відповідно до теорії DIT2FSs і DIT2FLSs, рівень і-го ризику визначається за формулою

$$r_i = F(LI, LO, R, IN_i),$$
$$LI = \langle li_n \rangle, n = \overline{1, N},$$
$$R = \langle r_m \rangle, m = \overline{1, M},$$
$$IN_i = \langle in_n^i \rangle,$$

де F – операція нечіткого логічного висновку (алгоритм Мамдані),

LI – набір вхідних лінгвістичних змінних другого типу, які описують фактори ризику кібербезпеки,

N – кількість вхідних лінгвістичних змінних,

LO – результуюча лінгвістична змінна другого типу, що описує рівень ризику кібербезпеки,

R – набір нечітких правил, на основі яких визначається рівень ризику кібербезпеки,

M – кількість нечітких правил,

IN_i – набір нечітких експертних оцінок.

Для отримання експертних оцінок в роботі використовується метод перцептивних міркувань, запропонований Wu і Mendel [6]

$$in_n^i = F^*\left(V, W^i\right),\ in_n^i \in IN,$$
$$V = \left\langle v_j \right\rangle,\ j = \overline{1, J},$$
$$v_j = \left\langle T_j, \tilde{Y}_j \right\rangle,$$
$$W^i = \left\langle w_k^i \right\rangle,\ w_k^i \in V,\ k = \overline{1, K},$$

де F^* – оператор вербальних обчислень,

V – словник,

W^i – набір експертних вербальних оцінок,

v_j – гранульований терм, який описується словом і інтервальною нечіткою множиною другого типу,

J – кількість гранульованих термів в словнику, J = 16/32,

T_j – слово,

$\tilde{Y}_j$ – DIT2FS, яке описує слово,

w_k^i – експертна оцінка,

K – кількість експертів, які беруть участь в опитуванні.

Проведені експерименти показали задовільні результати, так як словесна оцінка факторів ризику є природною для експертів. Оцінки, отримані за допомогою розробленої моделі, є об'єктивними і враховують думки всіх учасників процесу. Крім цього, попередній етап обробки перцептивних даних дозволив виділити погані дані відповідно недобросовісних / некомпетентних учасників процесу оцінки ризиків.

Список використаних джерел

1 Wangen, G. An initial insight into Information Security Risk Assessment practices. In: 2016 Federated Conference on Computer Science and Information Systems (FedCSIS). 2016. № 8. P. 999–1008.

2 IEC 31010:2009. Risk management, Risk assessment techniques. 1st edn. 2009. 176 p.

3 OWASP Risk Rating Methodology. URL: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (дата звернення: 13.10.2017)

4 Zadeh, L.A. Fuzzy logic = computing with words. IEEE Trans. on Fuzzy Systems. 1996. № 4. P. 103-111.

5 Mendel, J.M, John, R.I.B. Type-2 Fuzzy Sets Made Simple. IEEE Transactions on Fuzzy Systems. 2002. № 10 (2). P. 117-127.

6 Mendel, J.M., Wu, D. Perceptual Computing: Aiding People in Making Subjective Judgments. 1st edn. Wiley-IEEE, 2010. 336 p.

НЕЛАСА Г.В., к.т.н.,доцент
кафедри захисту інформації,
Запорізький Національний
технічний університет
ВЕРЕЩАК М. І., аспірант
Запорізький Національний
технічний університет

ВИКОРИСТАННЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ПРИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

В основі сучасних криптографічних алгоритмів лежать методи, що базуються на перетвореннях в алгебраїчних структурах великих порядків. Це забезпечує достатню крипостійкість завдяки великій кількості елементів структури, які необхідно протестувати при проведенні атаки повним перебором. Таким чином, програмування цих алгоритмів вимагає використання довгої арифметики для реалізації операцій найнижчого рівня. Сучасні апаратні засоби дозволяють підвищити швидкість обробки «великих» даних за рахунок розпаралелювання. При реалізації високопродуктивних обчислень розрізняють конвеєрну, паралельну та векторну обробку даних. Авторами використовується технологія масивно-паралельних обчислень CUDA[1], в якій потужна графічна картка використовується як векторний сопроцесор для неграфічних обчислень.

Питання захисту інформації на державному рівні вирішуються за допомогою інфраструктури відкритих ключів, основаній на використанні методів асиметричної криптографії в алгоритмах цифрового підпису та спрямованого шифрування. Основою сучасних стандартів цифрового підпису є алгоритми, засновані на криптографічних перетвореннях у групах точок еліптичних кривих, визначених над полями Галуа. Стандарт України [2] визначає алгоритми основних дій щодо генерації ключових пар, формування та верифікації цифрової підписи, а також набір рекомендованих для використання загальносистемних параметрів.

При детальному дослідженні стандарту було виділено дві задачі, що потребують великої кількості обчислень та піддаються розпаралелюванню: задачі обчислення порядку еліптичної кривої, визначеної над скінченим полем; та криптоаналіз, в даному випадку - вирішення проблеми дискретного логарифмування на еліптичній кривій.

Порядок еліптичної кривої, тобто скінчена кількість точок з координатами з основного поля, що належать кривій, є найважливішим із загальносистемних параметрів, та визначає крипостійкість обраної кривої. При цьому порядок базової точки повинен бути великим простим дільником порядку кривої, щоб уникнути атаки Поліга-Хеллмана. В стандартах

приводяться готові до використання криві, стійкість яких регулюється розробниками стандартів, але з часом вимоги до стійкості неухильно ростуть і в результаті можуть вийти за рамки стандартизованих параметрів. На сьогодні довжина секретного ключа та, відповідно, елементів основного поля для досягнення прийнятної стійкості можуть досягати 1024 біт, що виходить за рамки стандарту.

Авторами розроблено програмне забезпечення для визначення порядку еліптичної кривої екстенсивним способом, за рахунок використання векторного обчислювача. Існує багато математично досить складних методів визначення порядку еліптичної кривої, визначеної над скінченим полем[3]. Але порядок кривої завжди можна обчислити наївним способом перебором всіх елементів поля F_q як суму

$$N_E = 1 + \sum_{x \in F_q} \{\chi(x^3 + ax + b) + 1\} = q + 1 + \sum_{x \in F_q} \chi(x^3 + ax + b),$$

де $\chi(z)$ - квадратичний характер елементу z поля F_q.

Для стандартних комп'ютерів це обчислювально складна задача, але використання масивно-паралельних обчислень дає змогу за рахунок використання великої кількості «lightweight threads» отримати прийнятний за часом результат. Таким чином, використання обчислювальних резервів графічних прискорювачів можна ефективно використовувати для вирішення ресурсоємних криптографічних завдань.

Список використаних джерел

1. Сандерс Дж., Кэндрот Э. Технология CUDA в примерах: введение в программирование графических процессоров. - М.: ДМК Пресс, 2013. - 232 с.

2. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. ормування та перевіряння: ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

3. Бессалов А. В., Телиженко А. Б. Криптостстемы на эллиптических кривых. – К.: ІВЦ Видавництво «Політехніка», 2004. – 224 с.

СВІРСЬКИЙ Б. М.,к.ю.н., доцент
кафедри права та публічного
адміністрування Маріупольського
державного університету,

ПРАВОВІ ЗАСАДИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ В УКРАЇНІ

В останні роки збільшується використання у найрізноманітніших сферах життєдіяльності суспільства комп'ютерних і телекомунікаційних технологій, у тому числі інтернет-технологій, що разом з великою кількістю переваг принесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди як на мікро -, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Це призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї нової сукупності загроз [1].

З огляду на сучасні тенденції суспільного розвитку національна безпека України не могла залишитися поза впливом внутрішнього інформаційного фактора. Адже в умовах інформаційного суспільства всі без винятку об'єкти національної безпеки (людина, суспільство, держава) стають чутливими до інформації, яка їх оточує. Таким чином, цілеспрямовано змінюючи інформацію, зафіксовану на певних носіях, керуючи каналами комунікації, впливаючи на технічні засоби обробки інформації, можна змінювати рішення, а відтак, і дії об'єктів національної безпеки. [2]

Розуміння цим загрозам спонукало державу в останні часи прийняти нормативно-правові акти, які дають більш ефективніше вести системну боротьбу з «кіберчумою» XXI ст.

Так, в реалізації рішень РНБО у 2016 році прийнята «**Стратегія кібербезпеки України»,** яка визначила створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. В цьому нормативно-правову акті окреслено, що забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів… [3]

Тому край важливим і своєчасним є внесення на розгляд парламенту України – Верховній Раді законопроекту «Про основні засади забезпечення кібербезпеки України». Предметом законопроекту є - правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Вперше на законодавчому рівні визначаються основні терміни, що стосуються предмету регулювання у цьому законопроекту такі як – кібератака; кібербезпека; кіберзагроза; кіберзахист тощо.

Визнання на законодавчому рівні таких термінів дає можливість в правоохоронній діяльності однозначно ідентифікувати та кваліфікувати діяння злочинів розташованих у розділі XVI КК, що призведе до недопущення помилок у їх кваліфікації.

Законопроект надав також вичерпний перелік об'єктів кібербезпеки, та повноваження суб'єктів забезпечення кібербезпеки постійної готовності до яких відніс: Раду безпеки і оборони України; Міністерство внутрішніх справ України; Міністерство оборони України; Генеральний штаб збройних сил України; Службу безпеки України; Державну службу спеціального зв'язку та захисту інформації України.

Кібератака, що мала місце у світовому просторі у червні 2017 року, за допомогою програмного продукту Petya блокувала на деякий час роботу державних органів, фінансових установ, енергетичних та транспортних мереж, що в черговий раз довело до людства рівень можливих світових загроз нормальному функціонуванню життєво важливих сегментів суспільства.

Тому одним із правових аспектів боротьби з кіберзлочинністю є визначення в Кримінальному кодексі України (окремим розділом) переліку суспільно-небезпечних дій які загрожують суспільним відносинам у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. На жаль чинне кримінальне законодавство до злочинів в цієї сфері відносить тільки шість складів суспільно-небезпечних дій, що враховуючи значну суспільну небезпеку на мою думку є край недостатньою. Прийняття в найближчий час рамкового Закону про кібербезпеку дасть можливість внести до КК України зміни до розділу XVI і значно розширити перелік дій, що загрожують кібербезпеки Україні.

Таким чином в Україні в останні часи створюються необхідні правові умови щодо протистояння можливим загрозам безпекового використання електронно-обчислювальних машин (комп'ютерів).

Список використаних джерел

1.Баранов ОА. Про тлумачення та визначення поняття «кібербезпека» / ОА. Баранов [Електронний ресурс]. - Режим доступу : ippi.org.u

2.Панченко В.М. Поняття інформаційної безпеки в сучасному юридичному дискурсі / В.М. Панченко //Інформаційна безпека людини, суспільства, держави. - 2009. - № 2 (2). - С. 22 - 27.

3.Указ Президента України «Стратегія кібербезпеки України» від 15.03. 2016 р. № 96/2016

ГОДОВАНИК Є. В., кандидат юридичних наук, доцент кафедри права та публічного адміністрування, Маріупольський державний університет

МІЖНАРОДНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ

Слід зазначити, що інформаційні загрози є однією з новітніх форм т. з. «гібридної» агресії, яку мають сучасні міжнародні конфлікти, тобто інформаційна безпека стає невід'ємною складовою ефективного забезпечення міжнародної безпеки в цілому.

Прикладом «гібридної» агресії є масштабна комплексна збройна, політична, економічна та інформаційна агресія Російської Федерації проти державного суверенітету та територіальної цілісності України, що триває в активній фазі протягом 2014-2017 рр. При цьому інформаційній складовій агресивних дій держава-агресор надає особливого значення, для чого використовується система як державних, так і приватних ЗМІ, інтернет-ресурсів, соціальних мереж, юридично або фактично прямо чи опосередковано підконтрольних державним інститутам РФ, у тому числі – зареєстрованих в інших країнах.

У зазначеному контексті важливим завданням є пошук правильного доктринального визначення категорії «міжнародна безпеки», що має суттєве теоретичне і практичне значення.

На рівні документів ООН сутність терміна «міжнародна безпека» концептуально визначена у Декларації про зміцнення міжнародної безпеки 1970 р., відповідно до положень якої вона розуміється як стан міжнародних відносин, для забезпечення якого необхідним є дотримання цілей і принципів Статуту ООН [1]. Головну перешкоду для збереження зазначеного особливого стану у міжнародних відносинах держави-члени ООН вбачають у наявності криз і спалахів напруги, виникненні конфліктів між державами, триванні та ескалації гонки озброєнь, подальшому збільшенні військових витрат, погіршенні міжнародного економічного становища та збільшенні розриву між розвиненими країнами і такими, що розвиваються [2, с. 9].

Рада Безпеки ООН у низці своїх резолюцій відзначає, що міжнародна безпека являє собою особливий стан міжнародних відносин, причому застосування сили всупереч Статуту ООН порушує такий стан [3].

На погляд М. Тахера, наведені положення міжнародних документів і практика держав дозволяють визначити міжнародну безпеку як «особливий стан міждержавних відносин, за якого всі держави спроможні в умовах міжнародного правопорядку забезпечити свій суверенітет» [2, с. 9]. М. Тахер додає, що «… у сучасних умовах міжнародна безпека може

бути забезпечена тільки системою гарантій…Таку систему складають матеріальні, організаційні та нормативні гарантії міжнародної безпеки» [2, с. 10], причому до організаційних гарантій належить, насамперед, «система колективної безпеки, що створена та діє в рамках ООН» [2, с. 10].

Найбільш вдало поняття «міжнародна безпека» визначає В. Н. Денисов, розглядаючи право міжнародної безпеки як «систему принципів і норм міжнародного права, що встановлює універсальний порядок у сфері підтримання міжнародного миру і безпеки у світі відповідно до Статуту ООН» [4, с. 676-677].

Щодо елементів міжнародної безпеки, то М. О. Баймуратов зараховує до них конкретні юридичні механізми збереження міжнародного миру та безпеки, зокрема, наступні: мирні засоби розв'язання спорів; всезагальна і регіональна безпека (колективна безпека); роззброєння; заходи щодо послаблення напруги та припинення гонки озброєнь; заходи щодо попередження ядерної війни; неприєднання і нейтралітет; заходи щодо припинення актів агресії (самооборона); дії міжнародних організацій; нейтралізація і демілітаризація територій (ліквідація військових баз); створення зон миру у різних районах земної кулі; заходи щодо зміцнення довіри між державами [5, с. 685-686].

Таким чином, як вбачається, забезпечення інформаційної безпеки має стати одним з найважливіших напрямів діяльності Ради Безпеки ООН та безпосереднім об'єктом її правотворчості, зважаючи на характер та принципові якості актів агресії у сучасних умовах глобалізації та значного розширення сфер реалізації конфліктогенних факторів у світі.

Список використаних джерел:

1. Декларация об укреплении международной безопасности : Резолюция ГА ООН 2734 (XXV) от 16.12.1970 г. [Электронный ресурс]. – Режим доступа : http://www.un.org/russian/Docs/journal /asp/ws1.asp?m=A/RES/2734 (XXV)

2. Тахер М. Международно-правовые аспекты обеспечения всеобщей безопасности : автореф. дис. … канд. юрид. наук : спец. 12.00.11 «Международное право» / М. Тахер. – К., 1997. – 20 с.

3. Резолюция СБ ООН 660 (1990) от 2 августа 1990 г. [Электронный ресурс]. – Режим доступа : http://www.un.org/russian/documen/scresol/1990/res660.pdf

4. Великий енциклопедичний юридичний словник / за ред. Ю. С. Шемшученка. – К. : Юридична думка, 2007. – 992 с.

5. Баймуратов М. А. Международное публичное право / М. А. Баймуратов. – Харьков : ООО «Одиссей», 2007. – 704 с.

ТАРАСЮК В. П., доцент, к.т.н., PhD, декан факультету комп'ютерно-інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки Донецького національного технічного університету (м. Покровськ),
АХМЕДОВ Р. Н., аспірант Донецького національного технічного університету (м. Покровськ)

ВИКОРИСТАННЯ ПРОЕКТНИХ РІШЕНЬ PHOENIX CONTACT ДЛЯ ЗАХИСТУ ПРОМИСЛОВИХ МЕРЕЖ У ЦЕНТРІ ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ ДОННТ

З 2014 року викладачами ДонНТУ реалізовано проект «Training in Automation Technologies for Ukraine» (TATU), який спрямовано на створення спеціалізованих центрів підготовки фахівців з промислової автоматизації. Центр промислової автоматизації функціонує на основі обладнання, наданого Phoenix Contact, Germany (рис.1). Викладачі розробили навчальні матеріали, методичні рекомендації та окремі програми підготовки для різного рівня споживача.

Рисунок 1 - Обладнання Phoenix Contact

При побудова навчальних курсів центру і апробації практичних робіт стало ясно, що Розвиток Industrie 4.0 і інтернет речей (Industrial Internet of Things), забезпечують підвищення ефективності і гнучкості виробництва. У той же час об'єднання всіх установок в єдину мережу має на увазі ризик для безпеки і небезпека збоїв, шкідництва і втрати даних.

Аналіз роботи [1], показав, що «пріоритетне завдання Industrie 4.0 полягає не тільки в побудові цифрової ланцюжка створення вартості, а й в забезпеченні безпеки мереж і даних». Високий ступінь мережевої інтеграції, яка охоплює як користувальницькі додатки, так і в зростаючому обсязі промислові процеси проектування та виробництва, веде до підвищення значущості способів захисту процесів, продуктів та інформаційного обміну.

Phoenix Contact є лідером в області автоматизованих технологій. Враховуючи реальність, в Берліні (Німеччина) на базі Phoenix Contact Cyber Security AG створено власний

центр компетенції в області кібербезпеки. Наявність такого технологічного центру дозволило пропонувати індивідуальні мережеві рішення і продукти, що враховують вимоги промисловості.

Безпека промислових мереж полягає в захисті промислових систем і установок, об'єднаних в мережу, від атак, шпигунства, виходу з ладу в результаті дії вірусів, шкідливих програм і помилок управління. На відміну від стандарту Ethernet поширені концепції безпеки, як програмні міжмережеві екрани [3], досить складно перенести в виробничі мережі. Вони не відповідають спеціальним вимогам промисловості.

Багаторічний досвід в області автоматизованих технологій дозволили Phoenix Contact розбиратися у вимогах промисловості і пропонувати готові рішення на базі перевірених концепцій безпеки та інноваційних продуктів. Наприклад, Phoenix Contact надає:

- спеціальні функції брандмауера для промисловості: умовний і призначений для користувача міжмережевий екран;
- поглиблену перевірку пакетів для промислових протоколів;
- безпечний мережевий доступ для сервісних інженерів.

Особливістю роботи центру промислової автоматизації ДонНТУ є безпечна концепція дистанційного обслуговування для об'єднаних в єдину мережу машин і установок для проведення лабораторного практикуму.

Дистанційне обслуговування виробничих установок дозволяє скоротити витрати на приїзд фахівців, тренерів, студентів і час простою. Для того щоб скористатися всіма перевагами дистанційного доступу, потрібно безпечне, надійне і стійке з'єднання. Так як відсутність захисту дистанційного з'єднання дозволяє стороннім особам проникати в корпоративну мережу: вразливість, яка може привести до істотного економічного збитку.

Для цього використовуються компоненти безпечного доступу, які забезпечують високий ступінь безпеки передачі даних при використанні VPN-тунелю і сучасних стандартів шифрування. У цій області Phoenix Contact пропонує продумані системи, в яких враховуються промислові вимоги. Наприклад, компоненти дозволяють:

- просте підключення машин і установок без використання настановного програмного забезпечення;
- гнучкі з'єднання через інтернет або мобільну мережу;
- міжмережевий екран в VPN-тунелі для захисту доступу;
- VPN-зв'язок без змін брандмауера центру.

Інноваційну технологію для забезпечення безпеки передачі даних в сфері автоматизації процесів виготовлення та обробки центру автоматизації запропонував Phoenix Contact Cyber Security AG, а саме використання технології mGuard для захисту від кіберрисків.

Наприклад, маршрутизатор - FL MGUARD RS4000 TX / TX VPN - 2200515 [2] пристрій для забезпечення безпеки, інтерфейси WAN і мобільного зв'язку. Слот для SD-карт. 10 тунелів VPN, інтелектуальний міжмережевий екран з повним обсягом функцій, маршрутизатор з NAT / 1: 1-NAT, за бажанням з контролем цілісності CIFS. Керований комутатор з 4 портами. 2 слота для SIM-карт. Приймач GPS (рис. 2).

Безпечне хмара mGuard (mSC) - це безпечна служба віддаленого підключення від Phoenix Contact. MGuard Secure Cloud використовує технологію віртуальної приватної мережі (VPN) відповідно до стандарту IPsec. Хмару mGuard Secure Cloud розміщено в центрі обробки даних Phoenix Contact.

Рисунок 2 – модуль FL MGUARD RS4000 TX/TX VPN – 2200515

Система використовує кілька рівнів безпеки - двохфакторний метод бесіди та VPN аутентифікація. MGuard Secure Cloud також підтримує сертифікати X509 і довірений FL-сервер mGuard з технологією IPsec VPN. Кожен підключений модуль FL mGuard, має унікальну вбудовану конфігурацію, яка використовується виключно для спілкування з хмарою mGuard. Пристрої mGuard запускають тунель IPsec VPN в безпечне хмара mGuard і використовують тільки вихідні порти. Немає необхідності відкривати порти в брандмауері, щоб мати можливість використовувати хмарний сервер. Крім того, IPsec стандарт VPN використовує порти (UDP 500/4500), але з технологією mGuard є можливість використовувати вже включені вихідні порти, такі як HTTPS (TCP 443).

Перелік використаних джерел

1) Билл Лайдон, для InTech. Промышленная автоматизация и «Интернет Вещей» [Електронний ресурс] – 2013. – Режим доступу до ресурсу: http://ua.automation.com/content/promyshlennaja-avtomatizacija-i-internet-veshhej
2) Офіційний сайт Phoenix Contact Україна [Електронний ресурс] – Режим доступу до ресурсу: https://www.phoenixcontact.com/online/portal/ua/.

3) Phoenix Contact. mGuard Security Advisory [Електронний ресурс] / Phoenix Contact. – 2016. – Режим доступу до ресурсу: https://www.phoenixcontact.com/online/portal/ua/
4) Phoenix Contact. Industrial Ethernet [Електронний ресурс] / Phoenix Contact. – 2017. – Режим доступу до ресурсу: https://www.phoenixcontact.com/online/portal/ua/
5) Phoenix Contact. Ethernet Basics Rev. 02 [Електронний ресурс] / Phoenix Contact. – 2017. – Режим доступу до ресурсу: https://www.phoenixcontact.com/online/portal/ua/

МЕРКУЛОВА К. В., к.т.н., доцент
кафедри математичних методів та
системного аналізу,
Маріупольський державний
університет

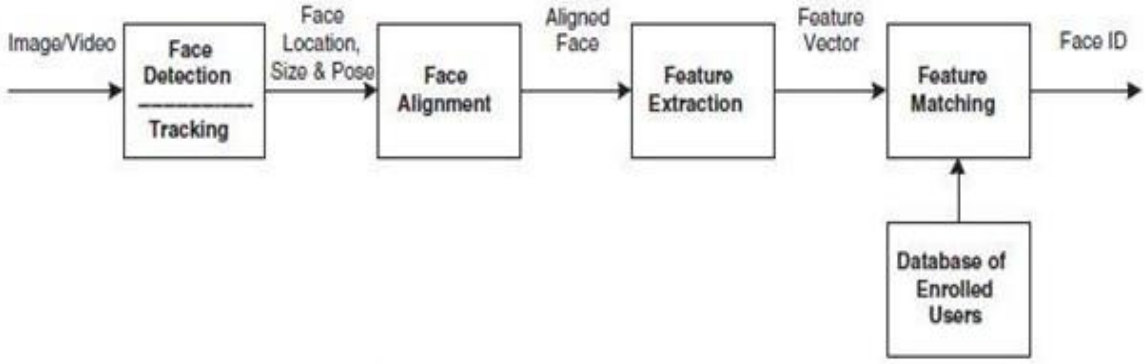
ІДЕНТИФІКАЦІЯ ЗА БІОМЕТРИЧНИМИ ДАНИМИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У теперішній час розвиток комп'ютерних технологій призвів до впровадження інформаційних систем практично на усіх підприємствах та установах нашої держави. Тому на перший план виходять проблеми захисту інформаційних систем загального (цивільного) та спеціального (військового та правоохоронного) призначення. В останній час науковцями досягнуто значних успіхів у розробці біометричних методів ідентифікації та аутентифікації для забезпечення захисту від несанкціонованих дій та втручанням у роботу інформаційної системи.

Біометрика (англ. Biometrics) – це методи ідентифікації особи, що використовують фізіологічні параметри людини – відбитки пальців або долоні, зображення обличчя, райдужну оболонку або сітківку ока, голос, ДНК, тощо [1]. Звичайно біометричні методи розділяють на статичні, коли відповідні ознаки особи практично не змінюються у часі, та динамічні, які використовують дані про особливості поведінки людини.

Один з найактуальніших засобів біометричної ідентифікації є розпізнання обличчя [2]. Основні методи ідентифікації людини за фотопортретом включають аналіз зображення в градаціях сірого для виявлення унікальних характеристик обличчя, аналіз розпізнавальних рис (використовується більш всього метод розпізнавання, адаптований до зміни міміки), аналіз на основі нейронних мереж (порівняння за «особливими точками», метод застосовують для ідентифікації облич у важких умовах), автоматична обробка зображення обличчя (визначення відстаней і співвідношення відстаней між особливостями обличчя людини, що легко визначаються), яку можна ефективно використати в слабоосвітлених приміщеннях та інші. У системах статистичного розпізнавання на основі набору

біометричних даних та їх обробки формується електронний взірець як унікальне число, що стосується конкретної особи. Основні етапи використання методу: сканування об'єкта, вибір індивідуальних характеристик, формування шаблона і його порівняння з базою даних. Сканування обличчя триває 20–30 с. Далі відбувається процес ідентифікації, створення шаблона в реальному часі і порівняння його з файлом шаблона. Необхідний для перевірки рівень подібності – це обчислювальний поріг, який регулюється залежно від різних чинників (потужності ПК, освітлення тощо). Але незважаючи на велику кількість алгоритмів загальна структуру процесу розпізнання обличь виглядає наступним чином:



Face recognition processing flow.

Active Shape Models (ASM) метод є найпоширенішим при реалізації у інформаційних системах [3]. Суть метода ASM [16,19,20] полягає в обліку статистичних зв'язків між розташуванням антропометричних точок на наявній вибірки зображень осіб, знятих в анфас. На зображені експерт розташовує антропометричні точки. На кожному зображенні точки пронумеровані у єдиному порядку.

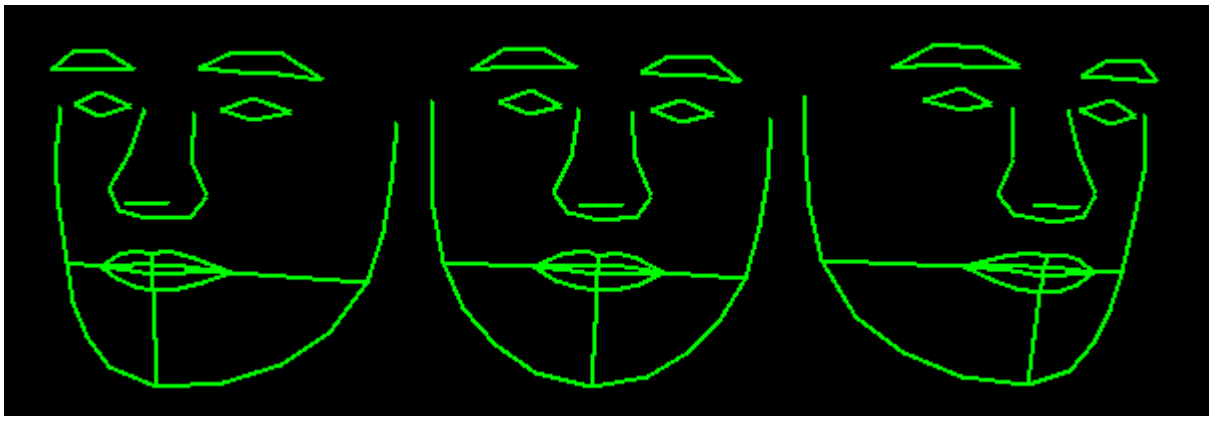
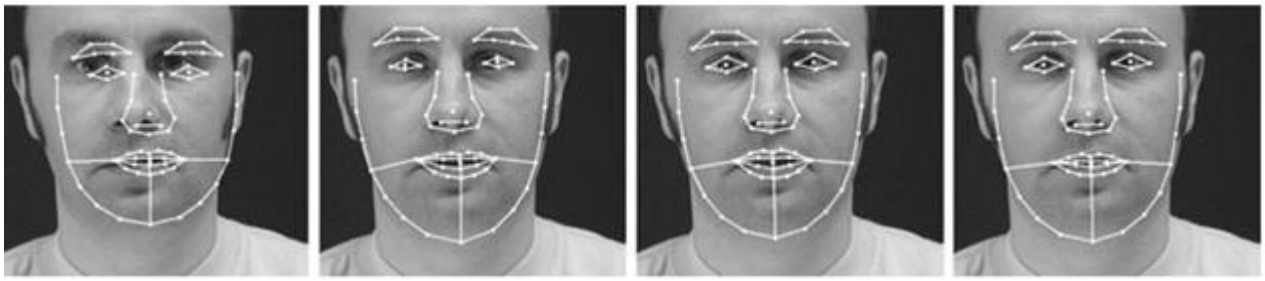


Рис.1. Приклад представлення форми особи з використанням 68 точок

Для того, щоб привести координати всіх образів до єдиної системи, звичайно виконується так званий загальний прокрутов аналіз, в результаті якого всі точки приводяться до єдиного масштабу і центруються. Далі для всього набору образів обчислюється середня форма та матриця коваріації. На основі матриць коваріації вираховуються власні вектори, які потім сортуються в порядку зменшення відповідних їм власних значень. Модель ASM визначається матрицею Ф та вектором середньої форми s. Тоді будь яка форма може бути надана за допомогою моделі та параметрів:

$$b_i = \Phi^T \bar{s}_i = \Phi^T (s_i - \bar{s})$$

Локалізація ASM моделі на новому зображенні, яке не входить до навчальної вибірки зображення, здійснюється в процесі вирішення оптимізаційної задачі.



а) б) в) г)

Рис.2. Ілюстрація процесу локалізації моделі ACM на конкретному зображенні: а) початкове положення б) після 5 ітерацій в) після 10 ітерацій г) модель зішлася

Однак, все ж головні метою ASM методу є не розпізнавання осіб, а точна локалізація особини та антропометричних точок на зображенні для подальшої обробки. Практично у всіх алгоритмах обов'язковим етапом, що передує класифікації, є вирівнювання, під яким розуміється вирівнювання зображення особи у фронтальне положення або приведення сукупності осіб (наприклад, в навчальній вибірці для навчання класифікатора) до єдиної системи координат. Для реалізації цього етапу необхідна локалізація на зображенні характерних для всіх осіб антропометричних точок - найчастіше це центри зіниць або куточки очей. Різні дослідники виділяють різні групи таких точок. З метою скорочення обчислювальних витрат для систем реального часу розробники виділяють не більше 10 таких точок. Моделі ASM якраз і призначені для того щоб точно локалізувати ці антропометричні точки на зображенні особи.

Список використаних джерел

1. Методи і засоби автентифікації біометричних даних в інформаційних системах [Текст] / Я.П.Кісь, В.М.Теслюк. // ACTUAL PROBLEMS OF ECONOMICS #12(138), 2012. – С. 174-180.
2. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно – телекомунікаційних систем [Текст] / В. Л. Бурячок // Захист інформації. НАУ. - К. – 2011. - №3. – С. 1-9.
3. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. [Текст] // Математичні машини і системи / Інститут проблем математичних машин і систем НАН України. – 2011. - №1. – С. 39- 45. – ISSN 1028-9763.

КРИВЕНКО С. В., к.т.н., доцент
кафедри математичних методів та
системного аналізу,
Маріупольський державний
університет

УДОСКОНАЛЕННЯ СИСТЕМНОЇ БЕЗПЕКИ МЕРЕЖ ПРОМИСЛОВОЇ КОМУНІКАЦІЇ

Кількість кібератак на промислові мережі неухильно зростає. У промисловості об'єктами кіберзагроз можуть ставати розподілені системи управління (РСУ), програмовані логічні контролери (ПЛК), системи збору даних (SCADA-системи) і елементи людино-машинного інтерфейсу (HMI). На сьогодні один з ключових факторів вразливості - загальна низька культура процесів забезпечення кібербезпеки. На багатьох підприємствах не проводиться оцінка ключових ризиків, не забезпечується безпечне управління операціями, включаючи базове управління паролями. Відсутній комплексний аудит, не гарантується злагоджене та ефективне дотримання політик безпеки, недооцінюються доступні інструменти контролю і виявлення загроз. Навіть в сучасному світі досить поширеними проблемами залишаються недостатній контроль фізичного доступу на територію, недбале ставлення до процедур авторизації і аутентифікації при вході в корпоративні та промислові мережі (наприклад, занадто легкі, рідко змінювані паролі).

Програмно-апаратними лазівками для зловмисників можуть ставати незахищені канали віддаленого доступу, неадекватні міжмережеві екрани, неправильно вибудувана архітектура мережі, в тому числі відсутність сегментації. Іноді в системах зустрічаються незахищені віддалені термінали, комп'ютери, USB-порти, мобільні і периферійні пристрої і також специфічні види пристроїв людино-машинного інтерфейсу.

Поступовий перехід до використання комерційних IT-рішень, безсумнівно, несе

комерційну вигоду і спрощує експлуатацію та інтеграцію систем. Але при цьому системи управління виявляються більш уразливими перед шкідливим програмним забезпеченням і загрозами безпеці, націленими саме на комерційні системи.

Причиною виникнення вразливостей можуть служити різноманітні помилки «людського чинника», зокрема неправильні дії проектувальника або інсталятора при конфігурації і установки системи. Негативно позначаються на безпеці неадекватні плани супроводу і модернізації АСУ ТП, недостатній рівень кваліфікації персоналу, відповідального за їх впровадження та обслуговування. Виробничий сектор пишається висококваліфікованими фахівцями з систем автоматизації, однак така експертиза в конкретних продуктах і рішеннях далеко не завжди транслюється в адекватну експертизу в промислових IT-мережах. Цей пробіл послаблює здатність організації розробляти всебічні стратегії захисту і запобігання загроз.

Зокрема, компанія Schneider Electric рекомендує промисловим підприємствам використовувати підхід Defense-in-Depth.

Defense-in-Depth була розроблена для оборонних цілей Агентством національної безпеки США, однак згодом виявилася придатною і для цивільних галузей. На думку ряду експертів, у майбутньому ця концепція стане стандартом забезпечення безпеки в промисловому середовищі.

Підхід Defense-in-Depth передбачає шість ключових компонентів:

• Розробка плану забезпечення безпеки: опис процедур оцінки ризиків та їх мінімізації, а також методів аварійного відновлення.

• Відділення мереж промислової автоматизації від інших мереж шляхом створення буферних зон, здатних захистити промислову систему від запитів та повідомлень з корпоративної мережі.

• Захист периметра від несанкціонованого доступу, що включає міжмережеві екрани, засоби аутентифікації, авторизації, VPN (віртуальної приватної мережі) і антивірусне програмне забезпечення.

• Сегментація мережі, що дозволяє обмежити поширення потенційної загрози одним сегментом. Для розділення мережі на підмережі та обмеження передачі трафіку між сегментами використовуються комутатори і VLAN (група хостів із загальним набором вимог, які взаємодіють незалежно від їх фізичного місцезнаходження).

• Посилення захисту пристроїв: управління паролями, визначення профілів користувачів і деактивація невикористовуваних сервісів.

• Регулярний моніторинг та оновлення: постійне спостереження за активністю операторів і мережевими комунікаціями, а також своєчасне оновлення програмного і

мікропрограмного забезпечення.

Хоча підхід Defense-in-Depth вітає створення і реалізацію вичерпного плану захисту, буде невірним вважати, що перехід до цієї концепції здійснюється за принципом «все або нічого».

Ймовірно, що найближчим часом на міжнародному рівні будуть розроблені нормативні вимоги щодо забезпечення кібернетичної безпеки для автоматизованих систем управління технологічними процесами. Необхідно виробити єдину термінологію, правила сертифікації продуктів і стандарти (можливо, таким стандартом міг би стати IEC 62443 8). В першу чергу вони повинні торкнутися підприємств з критично значущою інфраструктурою.

БАРЕГАМЯН С. Х., старший викладач кафедри права та публічного адміністрування Маріупольського державного університету

СИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ В УКРАЇНІ

На сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від безперешкодного функціонування кіберпростору, під яким пропонується розглядати середовище, що виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем. Більшість держав світу активно модернізує власні сектори безпеки відповідно до викликів сучасності, особливо, зважаючи на потенціал використання мережі Інтернет у воєнних цілях. Цей процес відбувається паралельно з активним реформуванням управлінських структур, впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері, активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз, збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту, розробленням кіберзброї та проведенням пробних військово-розвідувальних акцій у кіберпросторі, посиленням контролю за національним інформаційним простором (способами доступу, контентом тощо).

Україна інтегрована у світовий кіберпростір і, відповідно, зазнає різних загроз і негативних впливів, пов'язаних з його розвитком (зокрема від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств

та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки.

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективну систему протидії загрозам у кіберпросторі. До таких проблем належать, передусім, відсутність загальнонаціональних міжвідомчих координаційних структур, що могли б узгоджувати та координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі (співпраця реально існує не на чітко визначеному, а швидше, міжособистісному рівні, а отже, є уразливою), складнощі з кадровим наповненням відповідних структурних підрозділів, а також залежність України від програмних і технічних продуктів іноземного виробництва.

Правову основу забезпечення кібербезпеки України становлять: Конвенція про кіберзлочинність [2], інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації (зокрема, Закони України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», «Про боротьбу з тероризмом»), укази Президента України (зокрема, Указ «Про рішення РНБО від 27 січня 2016 року «Про стратегію кібербезпеки України»), акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України».

Незважаючи на наявність цілої низки чинних нормативно-правових документів щодо проблем забезпечення безпеки кіберпростору держави, вони не охоплюють усього спектра сучасних загроз кібербезпеці держави.

Останнім часом деякі кроки в розробленні нормативно-правової бази були зроблені. Так, Верховною Радою України 5 жовтня 2017 року прийнятий у другому читанні рамковий законопроект № 2126а від 19.06.2015 р. «Про основні засади забезпечення кібербезпеки України». Проте, цей Законопроект на сьогоднішній день ще не підписано, і відповідно, не набрав законної сили.

Законопроектом пропонується визначити правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Під кібербезпекою в зазначеному Законопроекті розуміється «стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі»

[3]. В Законопроекті визначено кібертермінологію, зазначено систему та повноваження військових і правоохоронних органів по забезпеченню кібербезпеки держави, до якої відносяться: Рада національної безпеки і оборони України, Міністерство внутрішніх справ України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Розвідувальні органи України [3].

Звісно, побудова дієвої системи забезпечення кібернетичної безпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на динамічні зміни, що відбуваються у світі в сфері забезпечення кібернетичної безпеки. Для забезпечення цього, перш за все, нормативні документи мають відповідати вимогам часу, а права та обов'язки правоохоронних органів та уповноважених відомств повинні бути чітко визначені у нормативних документах. Отже, після набрання вищезазначеного Законопроекту законної сили, слід і далі удосконалювати нормативну базу шляхом систематизації з урахуванням правозастосовчої практики.

Аналізуючи юридичні джерела, не можна не погодитись з позиціями деяких вчених, які зазначають, що тенденція посилення контролю з боку правоохоронних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі і т.д., свідчить про довгострокову тенденцію формування в мережі Інтернет класичних прав і обов'язків громадянина та держави, що існують в державі, та формування своєрідних «цифрових суверенітетів».

Вважаємо, що Україна потребує проведення комплексних навчань з протидії тяжким злочинам у кіберсфері з метою як практичної підготовки персоналу профільних відомств, так і налагодження зв'язків між інституціями, що відповідають за кібербезпеку держави. Крім навчань на національному рівні, бажаною є активніша позиція України у загальноєвропейських навчаннях з питань кібербезпеки та кіберозброєнь.

Таким чином, узагальнюючи, можна зробити висновки, що, єдина загальнодержавна система протидії кіберзлочинності з відповідним нормативним забезпеченням досі перебуває в процесі розроблення. Україна має продовжити активні кроки на шляху розбудови власної системи кібербезпеки.

Список використаних джерел

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. – Режим доступу: http://rada.gov.ua/
2. Конвенція про кіберзлочинність від 23.11.2001 р.: Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 р. № 2824-IV

3. Про основні засади забезпечення кібербезпеки України: Законопроект від 19.06.2015 р. № 2126а. – Режим доступу: www.rada.gov.ua
4. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 р. № 2824-IV. – Режим доступу: www.rada.gov.ua
5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016. – Режим доступу: www.rada.gov.ua

ДЯЧЕНКО О. Ф., аспірант,
Бердянський державний
педагогічний університет

ВПРОВАДЖЕННЯ МАТЕМАТИЧНИХ МЕТОДІВ У ПРОФЕСІЙНУ ПІДГОТОВКУ ФАХІВЦІВ ГАЛУЗІ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ»

Процес реформування системи вищої освіти базується на врахуванні перспектив розвитку країни та. Одним з найважливіших чинників розвитку професійної освіти фахівців галузі «Інформаційні технології», зокрема спеціальності «Кибербезпека» виступає багатоаспектна інтеграція змісту освіти. Інтеграційні міжнаукові взаємодії завжди ведуть до нових результатів, навіть й до появи нових наук. Інтеграція у навчанні – це не лише процес набуття нових знань, кількісного їх розширення, а й нова якість знань. Завдання вищих навчальних закладів, що випускають бакалаврів галузі «Інформаційні технології» сьогодні полягають в тому, щоб студенти вміли інтегрувати знання, отримані в процесі професійної підготовки для роботи за вибраним фахом й усвідомлювали шляхи подальшого розвитку власних професійних компетентностей, вдало розв’язували професійні завдання та задачі, в яких перетинаються декілька наук.

За останній час інтегративні процеси в педагогиці розглядали К. Баханов, Р. Гуревич, М. Жалдак, Н. Ничкало, Дж. Равен, Ю. Рамський, О. Співаківський, І. Фурса, Г. Шишкін, та ін.. Здійснений аналіз праць науковців встановив неузгодженість в практиці роботи вищої школи з виділення основних підходів до інтеграції знань.

Функціями компетентності по відношенню до структури та змісту освіти є надання можливості конструювання цілей, змісту і технології навчання в системному вигляді; інтегрованість дисциплін; багатофункціональність, що дозволяє бакалаврові вирішувати різноманітні професійні проблеми; формування компетенцій через зміст освіти.

Зміст освіти будується відповідно до діагностично-сформульованих цілей, що дозволяє усвідомити внесок даного предмета у досягнення результатів освоєння освітньої

програми і застосовувати відповідні методи і засоби навчання. Відбір і конструювання змісту дисциплін необхідно будувати з урахуванням інтегративних зв'язків, з орієнтованістю на досягнення виділених результатів навчання. Оновлення змісту математичної освти на підставі інтегративного підходу, міждисциплінарна взаємодія математичних та спеціальних інформатичних навчальних дисциплін, координація в часі їх вивчення вирішує центральне питання в підготовці сучасного ІТ-фахівця – покращення якості знань.

Впровадження поняття компетентнісно-інтегративного підхіду спрямоване на якісне вдосконалення існуючих педагогічних систем і обумовлює інноваційний тип діяльності сучасних навчальних закладів. Це сприяє створенню інноваційно-творчої атмосфери взаємодії між учасниками процесу професійної підготовки, формування готовності майбутнього фахівця до реалізації інноваційної діяльності в умовах освітнього простору. При реалізації єдиної стратегії професійної підготовки студентів має бути закладена ідея інтеграції особистісних, соціальних і діяльнісних аспектів, що сприяє координації змісту навчальних дисциплін (зовнішня інтеграція) і формуванню інтегральних характеристик особистості майбутнього фахівця (внутрішня інтеграція).

Отже, впровадження комптентністно-інтегративного підходу в професійну освіту фахівців галузі «Інформаційні технології» суттєво поліпшує якість розуміння спеціальних інформатичних дисциплін, а в наслідку більш ефективно застосовуються отримані знання для вирішення професійних завдань та складних не алгоритмізованих технологічних проблем.

ТИМОФЄЄВА І.Б.,старший викладач кафедри математичних методів та системного аналізу, Маріупольського державного університету

КІБЕРЗАГРОЗИ У ХМАРНИХ ТЕХНОЛОГІЯХ

На сьогоднішній день проблеми виявлення, розслідування та запобігання кіберзлочинам є надзвичайно актуальними. Впровадження сучасних технологій в економіці, управлінні, кредитово-банківській діяльності, стрімкий розвиток інформаційних і телекомунікаційних технологій на основі використання глобальної інформаційної мережі Інтернет зумовило зростання злочинних проявів у різних сферах діяльності людини.

Одним із аспектів розповсюдження широкого діапазону кіберзлочинів, які включають злочини, що здійснюються з метою отримання фінансової вигоди, злочини, пов'язані з використанням інформації, що знаходиться в комп'ютері, а також злочини, направлені проти конфіденційності, цілісності і доступності комп'ютерних систем [3], стає небезпека хмарних технологій.

Термін «хмара» (Cloud) широко використовують для позначення різних технологій та послуг в телекомунікаційній індустрії, як абстрактне позначення мережі в системних діаграмах його застосували вперше, а вже потім в Internet, який в теперішній час відіграє фундаментальну роль у хмарних обчисленнях (Cloud computing), оскільки представляє собою платформу, за допомогою якої сервіси хмарних обчислень стають доступними споживачам [1, с.33].

Згідно з визначенням Національного інституту стандартів і технології (NIST) у США, хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути забезпечені та оперативно надані з мінімальними управлінськими затратами чи зверненням до провайдера послуг. «Хмарою» метафорично називають Інтернет, який приховує всі технічні деталі. Застосовують класифікацію за критерієм надання прав доступу до сервісів та ресурсів адміністративним центром хмари, за яким виділяють чотири типи хмарних обчислень: публічні хмари, які відкриті для широкої публіки; приватні хмари, які розгорнуто на приватному обладнанні та в приватних цілях; гідридні хмари, які є комбінацією двох попередніх типів; суспільні хмари, які характеризуються мульти- адміністративними правами керування, є поєднанням всіх попередніх типів та створюються для дуже специфічних цілей [1, с.36].

В Україні використання систем хмарних обчислень регулюється загальними нормами законів про інформацію та її захист і положеннями приватного права. В свою чергу, у Верховній Раді України 24 березня 2016 року зареєстровано Проект Закону «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень» [2], який має виправити ситуацію із розпоряджанням інформацією.

Із прийняттям вказаного проекту можна говорити про гарантії захисту інформації та забезпечення виконання належним чином обов'язку із її зберігання провайдером шляхом запропонованого у вказаному Проекті переліку чисельних істотних умов, які мають міститись у договорі між надавачем хмарних послуг та володільцем інформації або власником системи. Головними із них є: порядок отримання володільцем інформації або власником системи інформації, яка оброблялась в системі хмарних обчислень, у випадку припинення надання хмарних послуг; порядок видалення інформації із системи хмарних обчислень; відповідальність сторін договору.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом використовуються засоби захисту інформації, які мають сертифікат відповідності чи позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації. Це означає, що для роботи державних інформаційних ресурсів за допомогою хмарних обчислень або для обробки інформації із обмеженим доступом кожному із осередків розміщення інформаційної інфраструктури системи необхідно бути сертифікованим відповідно законодавства України [4].

Існує ряд проблеми, пов'язаних з безпекою хмарних обчислень, але ці питання діляться на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг (організації, які надають програмне забезпечення, платформи, чи інфраструктуру як послуги через використання хмарних технологій) і питання безпеки, з якими стикаються їх клієнтів (компанії або організації, які розгортають додатки або зберігають дані на хмарі) [5]. Відповідальність йде в обох напрямках, тобто: постачальник повинен гарантувати, що їх інфраструктура знаходиться в безпеці і що дані та додатки клієнтів захищені, в той час як користувач повинен вживати заходи, щоб зміцнювати їх застосування, використовувати надійні паролі і перевірку автентичності.

Користувач стає залежним від провайдера хмари та може втратити контроль над інформацією. В такому випадку гостро постає питання порядку витребування інформації у незаконного володільця й відшкодування завданої шкоди за допомогою загальних засобів захисту цивільних прав.

Широке використання віртуалізації в реалізації хмарної інфраструктури спричиняє проблеми безпеки для клієнтів або орендарів публічного хмарного сервісу. Віртуалізація змінює відношення між ОС і базовим обладнанням – будь то обчислення, зберігання чи мережі. Це вносить додатковий шар – віртуалізації – що сам по собі повинен бути правильно налаштований та закріплений. Певні проблеми мають можливе рішення – компромісне програмне забезпечення віртуалізації, або «гіпервізор». У той час як ці проблеми мають здебільшого теоретичний характер, вони все ж існують.

Коли організація вибирає для зберігання даних або розгортання додатків публічному хмарі, вона втрачає можливість мати фізичний доступ до серверів з інформацію. В результаті, конфіденційні дані не зазнають ризику інсайдерських атак. Згідно з недавнім звітом від Cloud Security Alliance, інсайдерські атаки треті за величиною загрози в області хмарних обчислень. Таким чином, постачальники хмарних послуг повинні забезпечити, ретельні перевірки для співробітників, що мають фізичний доступ до серверів в центрі даних. Крім того, центри обробки даних повинні постійно контролювати підозрілу активність.

Для того, щоб зберегти ресурси, скоротити витрати, та зберегти ефективність, провайдери хмарних послуг часто зберігають більше одного разу дані клієнта на тому ж сервері. В результаті, існує ймовірність того, що особисті дані одного користувача можуть бути доступні іншим користувачам (можливо, навіть конкурентам). Для вирішення таких складних ситуаціях, постачальники хмарних послуг повинні забезпечувати правильну ізоляцію даних і логічні сегрегації зберігання [4].

Отже, хмарні обчислення – наступний етап інформаційного розвитку людства. В Україні досі залишається відкритим процес формування нормативно-правової бази врегулювання відносин з приводу їх використання. Досі для появи на теренах нашої держави послуг з надання хмарних сервісів вистачало лише договірного регулювання, однак для їх вдосконалення і подальшого поширення в українське законодавство мають бути внесені зміни з обов'язковим врахуванням розвитку хмарних технологій.

Список використаних джерел

1. Глоба Л. Cloud Computing та його застосування на підприємствах зв'язку / Глоба Л.С., Вольвач Є. О. // СПТЕЛ - 2013 (30 жовтня - 2 листопада 2013 р., м. Львів), 2013. – С. 33-40.
2. Закон України «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень». URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1N268W.html (дата звернення 19.10.2017)
3. Орлов О. Попередження кіберзлочинності–складова частина державної політики в Україні / О.В. Орлов, Ю.М. Онищенко - Теорія та практика державного управління, 2014
4. Хмарні обчислення в правовому полі України. URL: http://jurblog.com.ua/2016/08/hmarni-obchislennya-v-pravovomu-poli-ukrayini/ (дата звернення 19.10.2017)
5. Swamp Computing" a.k.a. Cloud Computing URL: http://security.sys-con.com/node/1231725 (дата звернення 19.10.2017)

ЧУНИЦЬКА В. В., студентка ЗНТУ,
ГАЙТОТА Є. В., студентка ЗНТУ
НІКУЛІЩЕВ Г. І., старший викладач кафедри ЗНТУ

АНАЛІЗ ЗАКОНУ «ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ»

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на одну з ключових арен протиборства. Україна

намагається давати відсіч агресивним діям на всіх фронтах, в тому числі і на інформаційному. Так, у серпні цього року Президент України Петро Порошенко підписав указ, яким ввів в дію рішення Ради Національної Безпеки і Оборони України (РНБОУ) про заходи щодо посилення кібербезпеки. Зокрема, з 1 грудня держорганам і держкомпаніям заборонено купувати послуги для виходу в інтернет у операторів, системи захисту яких не відповідають вимогам в області захисту інформації. Кабмін цього року повинен залучити приватні структури, які захищатимуть держсайти від кібератак.

Нацбанку рекомендовано удосконалити кіберзахист системно важливих банків України. СБУ, Держспецзв'язку та Нацполіція повинні почати співпрацю з зарубіжними партнерами для протидії кібератакам, залучати міжнародну технічну допомогу для забезпечення кіберзахисту державних інформресурсів. У вигляді техдопомоги в липні 2017 року Україна вже отримала від НАТО обладнання і програмне забезпечення на 1 млн євро. Співпраця з міжнародними організаціями та закордонними установами в галузі кібербезпеки триватиме і в перспективі.

Не в останню чергу ведеться робота з розробки законодавчої бази кібербезпеки на додачу до вже існуючих нормативних актів, які стосуються захисту інформації. Зокрема, протягом останніх років Президент України Петро Порошенко своїми указами ввів в дію розроблені спеціалістами з кібербезпеки та затверджені на засіданнях РНБОУ Стратегію кібербезпеки України та Доктрину інформаційної безпеки України.

В продовженні цієї великої і важливої роботи 5 жовтня 2017 року Верховна Рада України ухвалила в повторному другому читанні і в цілому законопроект №2126а «Про основні засади забезпечення кібербезпеки України» (надалі - Закон). На даний час він готується на підпис як закон для набуття чинності.

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі.

Згідно з Законом, координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним РНБОУ – таким чином, кібербезпека нормативно визнається важливою частиною національної безпеки України.

Закон визначає роль і задачі Національного координаційного центру кібербезпеки як робочого органу РНБОУ, який здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку.

Згідно із Законом, Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина,

національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України).

Закон визначає Національну систему кібербезпеки, яка «є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури». Важливою новацією Закону є долучення до забезпечення кібербезпеки як складової національної безпеки України Міністерства Оборони України. З моменту набуття Законом чинності основними суб’єктами національної системи кібербезпеки стануть Державна Служба Спеціального Зв'язку та Захисту Інформації України, Національна Поліція України, Служба Безпеки України, Міністерство Оборони України та Генеральний Штаб Збройних Сил України, розвідувальні органи, Національний Банк України.

Також Закон визначає Урядову команду реагування на комп’ютерні надзвичайні події України CERT-UA.

В Законі, в тому числі, приділяється увага державно-приватній взаємодії у сфері кібербезпеки та встановлюється відповідальність за порушення законодавства у цій сфері і контроль за законністю заходів із забезпечення кібербезпеки України. Очевидним плюсом є те, що Законом передбачається відповідальність не тільки за кіберзлочини, а й за неякісний захист інформації відповідальними особами.

Закон передбачає участь України в міжнародних і європейських системах забезпечення кібербезпеки, що дозволить поліпшити співпрацю з визнаними фахівцями, інтеграцію України в світову спільноту і підняти рівень знань вітчизняних фахівців.

На думку авторів, ще однією беззаперечно позитивною новелою Закону є введення в правове поле термінів, які починаються з "кібер": атака, безпека, загроза, захист, злочин, простір, тероризм, розвідка, шпигунство та інше. Тобто незаконне переведення або зняття грошей з чужого рахунку, порушення роботи електронного (база даних) або фізичного об'єкта (АЕС, аеропорт) стає кіберзлочином, аналогічним звичайній крадіжці; кібертероризм (втручання в роботу електронного реєстру, АЕС і взагалі в діяльність будь-якого важливого об'єкта) підпадає під статтю "Тероризм", а кібершпигунство (збір даних про силові структури країни або бізнес-структури) прирівнюється до звичайного шпигунства.

Також позитивним є те, що в Законі йдеться не тільки про освіту в вишах для фахівців, а й для суспільства, для підняття загальної освіченості населення в питаннях кіберзахисту, тому пересічні користувачі теж мають стати більш захищеними.

Тим не менше, Закон має небезпідставні мінуси. Деякі норми прописані так, що можуть бути трактовані неоднозначно. Зокрема, Закон дає право спецслужбам блокувати будь-які сайти, як загрожують безпеці країни. Ймовірні приводи для звинувачення, наприклад, у підриві суверенітету України настільки абстрактні, що можуть тлумачитись по-різному. Зважаючи на рівень невдоволення владою та зростання напруги в українському суспільстві, звинуватити можна будь-який інформаційний ресурс. Отже, автори доходять висновку, що Закон дає підстави для побоювань щодо виникнення загроз свободі слова і демократії та диктатури в країні за умови зловживань з боку відповідальних органів.

Отже, Закон, за умови набуття ним чинності, виступить насамперед рамковим документом, який юридично визначить ключові поняття у сфері кібербезпеки. Закон надасть нормативну базу і правове підґрунтя для активних дій щодо захисту українського кіберпростору в умовах гібридної війни. Тим не менш, в багатьох статтях Закон повторює основні положення Стратегії кібербезпеки України, ніяк їх не деталізуючи. В цілому, Закон носить доволі декларативний характер, так само, як і Стратегія кібербезпеки України та Доктрина інформаційної безпеки України, і не спонукає до конкретних дій.

Очевидно, що головна мета прийняття спеціалізованого Закону "Про основні засади забезпечення кібербезпеки України" полягає в засвідченні важливості захисту кіберпростору України. Більш конкретні кроки, дії і заходи мають бути прописані у підзаконних актах, прийнятих як відомствами, які входять в Національну систему кібербезпеки, так і всіма іншими, які так чи інакше провадять діяльність з залученням інформаційно-телекомунікаційних систем.

ШИМКОВА Ю. М., викладач І кваліфікаційної категорії
Комунальний вищий навчальний заклад «Уманський гуманітарно-педагогічний коледж ім. Т. Г. Шевченка»

SMS-ШАХРАЙСТВО – НАЙПОШИРЕНІШИЙ ВИД ШАХРАЙСТВА В УКРАЇНІ

Актуальність теми. Розвиток популярності інтернету і дає привід для розвитку шахрайства. Там де багато людей, а головне можливість для заробітку там і шахраї. Шахрайство, обман з метою заволодіння чужого майно, коштів.

Основні положення. Відповідно до статті 190 Карного кодексу України: шахрайство – заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою - карається штрафом до п’ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років.

Досить поширеним в Україні є SMS-шахрайство. Інколи людям приходять смс-повідомлення: «Ви виграли автомобіль!». У таких випадках не варто перераховувати ніяких грошей, а одразу звертатися до кіберполіції тому, що не може бути просто так, коли людина не бере офіційно участь у розіграші, не подаючи документів, що вона виграла автомобіль. Часто там сидять злочинці, які спілкуються по телефонах. Це надзвичайно потужні психологи, які вміють гарно розказувати, входити в те чи інше положення іншої людини і, як правило, є випадки, коли люди перераховують гроші [3].

Серед найпоширеніших схем SMS-шахрайства є:

SMS-шпион. Зловмисники пропонують послугу визначення місцезнаходження людини з номера його мобільного. Для того, щоб скористатися «послугою», абонентам пропонують спочатку зареєструватися за допомогою SMS: абонентові пропонують відповісти на декілька питань, за кожне повідомлення знімається не маленька сума. Посилання, яке присилається в результаті, як правило, містить загальнодоступну інформацію. Щоб не стати жертвою подібної схеми, необхідно дотримуватися простого правила – уважно читати умови надання «послуги».

Вирус, блокуючий екран ПК. Шахраї використовують вірусне ПЗ, яке блокує екран комп’ютера. Для розблокування пропонується прислати SMS на короткий номер. За відправку знімалося близько 30 грн Після чого присилається код, який можна ввести в спеціальне поле на екрані комп’ютера і відновити його роботу. Для захисту потрібний антивірус, бажано, з оновленнями, спрямованими проти SMS-блокеров.

Пропозиція розбагатіти. Шахраї відправляють SMS подібного змісту: «Це повинні знати усі. Існує один варіант отримання грошей по мобільному телефону, грошей, звичайно, ви зняти не зможете, зате вам на рахунок прийдуть гроші. За відправлену SMS з вас нічого не знімуть – це перевірено вже дуже багатьма. Як це зробити» Далі пропонується відправити SMS- повідомлення(набір букв і цифр) на короткий 4-значный номер. Шахраї обіцяють, що впродовж трьох хвилин абонентові прийде на рахунок 30 грн За SMS з рахунку знімаються гроші.

«Заборгованість по кредиту». Абонентові приходить SMS: «Банк Х відмовив Вам у видачі кредиту». Через декілька днів, коли абонент забуде про це повідомлення, йому дзвонять з незнайомого номера. Автовідповідач, представившись банком Х, говорить:

«Нагадуємо Вам про необхідність погасити кредит. Хочете прослухати повідомлення ще раз, натисніть 1. Хочете зв'язатися з оператором, натисніть 2». В процесі розмови з «оператором» у клієнта виманюються відомості про рахунок, особисті дані, номери кредиток.

«Підключися і отримай 100 гривень». За грошову винагороду абонентові пропонують підключитися до мобільного зв'язку на контрактній основі. Зловмисники обіцяють, що візьмуть усі зобов'язання за контрактом на себе і вчасно оплачуватимуть рахунки. Через певний час приходить рахунок на роумінг на дуже велику суму грошей. У МТС попереджають: не можна оформляти на себе контракти для невідомих третіх осіб.

«Отримай удвічі більше». Абонентові приходить SMS такого змісту: «Сервер мобільного оператора Х. Переведіть гроші на номер 8-ХХХ-ХХХ-ХХ-ХХ і отримаєте удвічі більше»!. Мобільний оператор ніколи не проводить акцій, умовою яких є переказ грошей з одного мобільного номера на інший.

«Вистачить реклами». Абонентові приходить SMS з пропозицією відписатися від рекламної SMS- розсилки. Щоб відписатися, потрібно відправити нібито безкоштовне SMS на один з коротких номерів. SMS виявляється платним. Треба звертати увагу на номер, з якого відправлене SMS. Якщо він невідомий, це вже привід подзвонити операторові і уточнити деталі запропонованої можливості. Треба пам'ятати, що шахраї можуть скористатися послугою відправки SMS через Інтернет, підставивши будь-яке ім'я в полі посилача.

«Врятуйте дитину». Абонент отримує сполучення з невідомим номером про необхідність знайти рідкісну групу крові для порятунку дитини. У повідомленні вказується номер телефону, дзвінки на який автоматично спустошують рахунок того, що подзвонив.

Усунення неполадок. Що дзвонить, під приводом несправності мережі, просить абонента набрати певну послідовність цифр і символів, що є командою переказу грошей. Треба пам'ятати, що будь-яка інформація, отримана від невідомих, потребує перевірки.

«Можна подзвонити»? На вулиці перехожий просить вас дати подзвонити хворій мамі або дітям додому, посилаючись на акумулятор, що сів, і терміновість дзвінка. Дзвінок здійснюється на платний номер. У цій ситуації можна попередити, що після відразу дзвінка буде перевірений баланс рахунку: якщо до користувача звернувся шахрай, це повинно його відлякати.

«Потрібна робота»? У оголошеннях з пропозицією високооплачуваної роботи пропонується для отримання детальній інформації пропонується відправити SMS або подзвонити на короткий номер, при цьому з рахунку знімається певна сума грошей, про які в оголошенні не було сказано. У таких випадках треба звертати увагу на дані про вартість дзвінка або SMS. Якщо цієї інформації немає, вартість може бути вища за звичайну.

«Перекинь грошей». Абонентові приходить SMS: «Не можу додзвонитися, немає грошей, перейшли 5 гривень». Надмірно говорити, що з цього номера ніхто не передзвонює. У МТС вказують на те, що такі повідомлення можуть відправити тільки найближчі люди: друзі, рідні. Незнайомий номер повинен насторожити і змусити замислитися, чи за адресою потраплять засоби.

«Поверніть мої гроші». Абонент отримує SMS про те, що хтось переказав на його рахунок певну суму грошей. Через декілька хвилин приходить SMS з повідомленням про помилку і проханням повернути гроші назад. У таких випадках завжди треба перевіряти стан рахунку, або за допомогою запиту або подзвонивши операторові і уточнивши, чи не було поповнень рахунку впродовж дня.

«Ви виграли»! Абонентові приходить SMS з невідомого номера або з Інтернету, де говориться про виграш цінного призу. Щоб його отримати, необхідно купити ваучер поповнення рахунку впродовж певного часу і повідомити код активації по вказаному номеру [1].

Висновки. У разі отримання подібного СМС-повідомлення поліція радить у першу чергу телефонувати за номером телефону банківської установи, який зазначений безпосередньо на Вашій картці чи номери телефонів зазначені на офіційних сайтах банківських установ, в яких Ви обслуговуєтесь [2].

Список використаних джерел

1. SMS-шахраї і їх 15 схем обману. [Електронний ресурс] – Режим доступу до ресурсу: http://bodyguards.com.ua/prikoly/968-sms-mosheniki-i-ix-15-sxem-obmana.html.

2. Кіберполіція розповіла про нові схеми смс-шахрайств [Електронний ресурс]. – 28 вересня 2017 р. – Режим доступу до ресурсу: https://cyberpolice.gov.ua/news/kiberpolicziya-rozpovila-pro-novi-sxemy-sms-shaxrajstv-5118/.

3. Попович Н. І.,. Профілактика протидії легалізації доходів, отриманих у сфері кіберзлочинності [Електронний ресурс] / Попович Н. І., Здирок М. А. // Матеріали VII регіональної міжвузівської студентської науково-практичної конференції «Проблеми українського суспільства: кіберзлочинність». – 2017. – Режим доступу до ресурсу: http://prog-rdak.16mb.com/wp-content/uploads/2017/04/kiberzlochunu.pdf.

АБУЗОВ І. Е., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольский державний
університет

ДО ПРОБЛЕМНОГО ПИТАННЯ ОПИСУ ПОТЕНЦІЙНИХ УМОВ РЕАЛІЗАЦІЇ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ ЕВОЛЮЦІОНУЮЧИХ СОЦІОТЕХНІЧНИХ СИСТЕМ

При проведенні комплексних досліджень актуальних проблемних питань забезпечення безпеки різного типу, а також планування, аналізу та контролю в системах управління силами і засобами при управлінні безпекою, в даний час набувають важливе значення багатосторонні дослідження можливостей підвищення ефективності моніторингу виконання завдань стратегічного планування [1].

У представленій доповіді наводяться деякі наочні практики до опису, з переважним використанням інструментальних засобів [2], послідовності подій, що призводять до реалізації загрози, і наявності зв'язків між цими аналізованими подіями.

Розглянута модель реалізації загроз [3], є узагальненою і цілком застосовна для опису обставин скоєння правопорушень та злочинів як для посадових осіб, які мають допуск до інформації, що захищається (внутрішній порушник), в цьому даному випадку не має значення, зробив він це випадково (ненавмисно) або свідомо (навмисно), так і для інших осіб, які не мають допуску до інформації, що захищається (зовнішній порушник).

В аспекті багатосторонньої взаємодії, етап виникнення дестабілізуючих чинників, що створюють передумови для реалізації загроз, передбачає можливість виникнення наступної послідовності важливих подій [3]:

- виникнення причин (мотивів), що спонукають (штовхають) до здійснення правопорушень;
- наявність обставин, які створює сам «порушник» свідомо чи несвідомо;
- створення умов, які існують або створюються на даному об'єкті захисту і сприяють вчиненню правопорушення і злочини.

На етапі створення дестабілізуючих факторів для реалізації загроз посадову особу ми будемо називати потенційним порушником. І, в залежності від дій порушника, виділимо три ключові етапи реалізації загроз безпеки інформації [1, 3].

1. *Поява загрози.* На даному етапі будемо вважати порушника зловмисником.
2. *Прояв загрози.* На етапі прояви загрози порушника будемо відносити до правопорушників.
3. *Реалізація загрози.* На етапі реалізації загрози порушник стає правопорушником, так як здійснює конкретні протиправні дії, спрямовані на подолання засобів захисту.

У разі якщо правопорушнику все-таки вдається реалізувати загрозу, яка завдала шкоди безпеці інформації, правопорушник (за рішенням суду) визнається злочинцем і йому визначають міру покарання.

Застосування розібраного методичного підходу дозволяє визначити (Скорегувати попередню оцінку можливих ризиків) загрозу здійснення правопорушення на об'єкти захисту. Зокрема, з використанням даного підходу, провідними науковцями з кібербезпеки була запропонована модель попередження конфліктів в середовищі радикалів, визначені перетворення контейнерів середовища радикалів, види конфліктів для вирішення завдання виключення конфлікту управління і сформований метод забезпечення умов виключення конфліктів управління, що дозволяє здійснити багатосторонній комплексний контроль розвитку ситуації [2].

Список використаних джерел

1. Рожнов А.В. О методических основах оценивания эффективности функционирования критичных социотехнических систем в сфере мониторинга и контроля государственного оборонного заказа. С. 338-342.

2. Рожнов А.В., Лепешкин О.М., Гудов Г.Н. Multidiscipline design environment based on radicalchart language / Seoul International Invention Fair 2012. Seoul, Korea: SIIF, 2012. С. 222.

3. Гудов Г.Н., Рожнов А.В., Лобанов И.А., Купач О.С. Методический подход к описанию сложных эволюционирующих систем при реализации угроз безопасности информации.

АВДЄЄНКО В. В.,
ОС «Бакалавр»,спеціальність
«Системний аналіз»,
Маріупольський державний
університет

ВІРУС PETYA

Petya — сімейство шкідливих програм, що вражає комп'ютери під управлінням сімейства ОС Microsoft Windows. Перші представники були виявлені в 2016 році та були звичайними зразками здирницьких вірусів. 27 червня 2017 року сталась масштабна атака останнім представником сімейства, який запозичив деякі модулі з попердніх зразків, але можливо був створений іншими розробниками та вже був вірусом-винищувачем даних, замаскованим під програму-вимагач.

Програма шифрує файли на жорсткому диску комп'ютера-жертви, а також перезаписує і шифрує головний завантажувальний запис (MBR) — дані, необхідні для завантаження операційної системи. В результаті всі файли, що зберігаються на комп'ютері, стають

недоступними. Потім програма вимагає грошовий викуп у біткоїнах за розшифровку і відновлення доступу до файлів. При цьому перша версія вірусу шифрувала не самі файли, а MFT-таблицю — базу даних з інформацією про файли, що зберігаються на диску.

Станом на 28 червня 2017 року вірус заразив 12 500 ПК у 64 країнах світу.

Вперше вірус Petya був виявлений в березні 2016 року. Компанія Check Point тоді зазначила, що, хоча йому вдалося заразити менше комп'ютерів, ніж іншим програмам-здирникам початку 2016 року, таким як CryptoWall, поведінка нового вірусу помітно відрізняється, завдяки чому він негайно був відзначений, як наступний крок в еволюції програм-вимагачів. За відновлення доступу до файлів програма вимагала від користувача 0,9 біткоїнів, що, за станом на березень 2016 року, становило близько 380 доларів США.

Більшість великих антивірусних компаній заявляють, що їхнє програмне забезпечення оновлено, щоб активно виявляти і захищати від проникнення вірусу.

Згодом на сайті Хабр були повідомлення від сисадмінів українських компаній, що постраждали із повідомленнями про те, що у них в компанії вже були встановлені всі останні оновлення, встановлений файєрвол, обмежені права користувачів, антифішинг фільтр для поштовиків і все одно ПК компанії були зашифровані.

Для цієї шкідливої атаки був виявлений ще один вектор захисту. Petya перевіряє наявність файлу perfc.dat, що перебуває в системній папці тільки для читання. Якщо він виявить цей файл, то не буде запускати шифрування програмного забезпечення та інформації. Однак така «вакцина» насправді не запобігає зараженню: шкідливе ПО, як і раніше буде використовувати «точку опори» на зараженому ПК, з метою поширитися на інші комп'ютерні системи через локальну мережу.

Список використаних джерел

1. ExPetr интересуется серьезным бизнесом. blog.kaspersky.ru.
2. Ransom.Petya. Symantec / United States (29 марта 2016).
3. Petya ransomware outbreak: Here’s what you need to know, Symantec Security Response.
4. Петя стирает память. Вирус Petya безвозвратно удаляет файлы пользователя. Газета.Ру (29 июня 2017).

АНЕНКО І.Д., ОС «Бакалавр»
спеціальність «Кібербезпека»,
Маріупольский державний
університет

УКРАЇНА ЯК ПОЛІГОН ДЛЯ КІБЕРВІЙН

Після того як Офіс директора національної розвідки США розкрив весь масштаб хакерської загрози, світова спільнота занервувала. В країні поки не сформована чітка організаційна структура держ.органів щодо відображення хакерських ударів. Хакерам вже вдалося атакувати в Україні десятки об'єктів критичної інфраструктури.

Частина галузей є IT-залежними. Після атак інфраструктура начебто ціла, а користуватися нею неможливо.

Україна - великий полігон для кібервійни. «Країна використовується міжнародними хакерськими угрупованнями для тестування і налагодження нових засобів, які потім будуть використані проти західних компаній і іноземних держав», - підкреслює президент київського відділення міжнародної організації по інформаційної безпеки.

В українських Збройних силах офіційних кіберпідрозділи немає. Деякі з їхніх функцій так чи інакше виконують війська РЕБ і Головне управління розвідки. «У поточній версії Військової доктрини України в формально мирний час будь-які дії в кіберпросторі за межами нашої території (припустимо, відповідні дії на кібератакакі) нелегалізовані», - додає Володимир Кург. Тобто, якби навіть військові хотіли завдати у відповідь кіберудар, то за законом вони не мають права цього робити.

Згідно зі стратегією кібербезпеки президента, окремий центр реагування на кіберзагрози повинен з'явитися в Нацбанку. Як повідомили в прес-службі фінансового регулятора, в 2017 році зі створення власного Центру реагування на інциденти кібербезпеки запланована низка заходів.

Зручний полігон. Україна стала зручним полігоном для використання нових методів кібервійни. Вірус «Petya.A» мав здатність відкладеного дії - комп'ютери могли бути заражені вже давно, і вірус тільки чекав команди про запуск.

Чому так сталося? Цьому сприяє ряд факторів: відсутність потужної протидії задумам хакерів, низька комп'ютерна грамотність населення, неліцензований софт. Державні компанії часто використовують не власні внутрішні захищені мережі, а «орендують» чужі, наприклад, того ж «Укртелекому». І якщо «лягає» одна компанія, то далі починається ланцюгова реакція. Хто використовує настільки потужна зброя - лише питання часу.

Фахівці вважають, що недавня хакерська атака - лише підготовчий етап до більш серйозних намірів. Уже відомо, що кібератака торкнулася і комп'ютерні мережі

Чорнобильської АЕС. Таким чином, масштаби загроз від діяльності хакерів можуть бути більш серйозними. Складно уявити, до яких техногенних катастроф могло б дійти справа, якби подібна атака на об'єкти енергетичного сектора виявилася б успішною взимку.

Після останньої масштабної хакерської атаки генеральний секретар НАТО Йенс Столтенберг повідомив, що в організації допоможуть Україні протистояти подібним загрозам. Для цього був створений трастовий фонд з кібербезпеки.

Одним з ефективних методів протистояння кіберзагрозами є створення закритих захищених мереж для кожного інфраструктурного об'єкта. Оновлення вимагає і програмне забезпечення: в українських органах державної влади досі використовують неліцензійні програми, вразливі для хакерських атак і вірусів.

Список використаних джерел

1. Полигон Украина: Цифровая война на пороге URL: http://www.liga.net/projects/cyberattacs/ (дата звернення 19.10.2017).

2. Новости Украині – как противостоять угрозам хакерских атак «Слово и дело» URL: https://ru.slovoidilo.ua/2017/06/30/kolonka/aleksandr-radchuk/bezopasnost/poligon-xakerskix-diversij-chto-zhdet-ukrainu-eru-kibervojn(дата звернення 19.10.2017).

БОЙКО Я. В., ОС «Бакалавр»
спеціальність «Кібербезпека»,
Маріупольський державний
університет

СУЧАСНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Загальна комп'ютеризація і новий розвиток інформаційних технологій призвели до того, що інформаційна безпека стає обов’язковою. Дії, які можуть призвести до спотворення, несанкційованому використанню або навіть руйнації інформаційних ресурсів керованої системи розуміються, як загроза безпеки інформації. Для цього вченні розробили багато засобів захисту інформації.

У своїх протиправних діях, зловмисники намагаються знайти джерела конфіденційної комп'ютерної інформації, які давали б їм найбільш достовірну інформацію в великих обсягах з мінімальними витратами його одержання. За допомогою багатьох прийомів, різноманітних фокусів і коштів підбираються шляхи й підходи до таких джерел. Під джерелом інформації мається на увазі матеріальний об'єкт, у якого є певні дані, котрі представляють конкретний інтерес для зловмисників чи конкурентів.

На сьогоднішній день комп’ютерні генії розробили нову сучасну технологію — технологію захисту в комп'ютерних інформаційних системах й у мережах її передачі. Для реалізація цієї технології здійснюється потреба в збільшенні витрат і зусиль. Однак це дозволяє уникнути значних втрат і шкоди, які можуть виникнути при реальному здійсненні загроз.

Засоби для створення інформаційної безпеки:

Системний підхід базується на побудові системи захисту, що означає оптимальне поєднання взаємозалежних організаційних програмних,. апаратних, фізичних та інших властивостей.

Принцип сталого розвитку системи - це безперервний процес, що полягає в обґрунтуванні та реалізації найбільш раціональних методів, засобів і шляхів вдосконалення захисту, безупинному контролі, виявленні її вузьких і слабких місць, потенційних каналів витікання інформації та нових засобів несанкційованого доступу.

Поділ і мінімізація повноважень із доступу до оброблюваної інформації та процедурам обробки, т. е. надання як користувачам, і самим працівникам ІВ, мінімуму суворо визначених повноважень, достатніх до виконання ними своїх службовими обов'язками.

Повнота контролю та реєстрації спроб несанкційованого доступу, т. е. необхідність точного встановлення ідентичності кожного користувача і протоколювання його дії щодо

можливого розслідування, і навіть неможливість скоєння будь-який операції обробки інформацією ІТ без її попередньої реєстрації.

Забезпечення надійності системи захисту, т. е. неможливість зниження рівня надійності у разі виникнення у системі збоїв, відмов, навмисних дій зломника чи випадкових помилок користувачів та обслугованого персоналу.

Забезпечення контролю над функціюванням системи захисту, тобто. створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення різноманітних коштів боротьби з шкідливими програмами.

Забезпечення економічної доцільності використання системи. захисту, виражену в перевищенні можливої шкоди ІС та ІТ від загроз над вартістю розробки та експлуатації системи захисту інформації.

Основні засоби захисту інформації:

Перешкода — засіб фізичного прегородження шляху «комп'ютерному пірату» до певної інформації. *Протидія атакам шкідливих програм* - це комплекс різноманітних заходів організаційного характеру і антивірусних програм.*Примус* — метод захисту, у якому користувачі і персонал ІВ змушені дотримуватися правил обробки, передачі й використання захистимої інформації під загрозою матеріальної, адміністративної чи кримінальної відповідальності.*Механізми шифрування* — криптографічне закриття інформації. Ці засоби захисту широко застосовуються як і в обробці, так і при зберіганні інформації на магнітних носіях. *Пробудження* — метод захисту, який спонукує користувачів і персонал ІВ не порушувати встановлені порядки з допомогою дотримання сформованих моральних і етичних норм. *Регламентація* — створення умов автоматизованої обробки, збереження і передачі захистимої інформації, у яких норми і стандарти захисту виконуються найбільше.

Таким чином, як показує статистика, у всіх країнах світу від зловмисних дій втрати безупинно зростають. Причому головні причини збитків пов'язані й не так з недостатністю коштів безпеки як, як із відсутністю взаємозв'язку з-поміж них, тобто, з нереалізованістю підходу. Тому необхідно випереджальними темпами удосконалювати комплексні засоби захисту безпеки інформації.

Список використовуваної літератури:

1. Титоренко Г.А. Інформаційні технології управління. М., Юнити: 2002.

2. Мельников У. Захист інформацією комп'ютерних системах. – М.: Фінанси і статистика, Электронинформ, 1997

ГУТИРА Я. В., ОС «Бакалавр»
спеціальність «Системний аналіз»,
Маріупольський державний
університет

ВІЙСЬКОВА КІБЕРБЕЗПЕКА

Питання кібернетичної безпеки в Збройних Силах України, а особливо в зоні проведення антитерористичної операції на сході країни, сьогодні майже не висвітлюється.

І правда, навіщо турбуватися про якісь там міфічні кіберзагрози під постійним вогнем артилерії противника? Що поганого, коли користуються Wi-Fi-роутером чи бездротовим модемом для доступу до Інтернету? Що може якийсь вірус на одному комп'ютері в порівнянні з танком противника? Нині склалася така ситуація, коли переважна більшість людей, залучених до захисту держави, включаючи працівників і старших офіцерів, елементарно не усвідомлюють небезпеки і можливих наслідків протистояння, що стрімко набирає обертів у площині такого містичного, поки що, кіберпростору.

З одного боку, це можна зрозуміти: одним ніколи цим перейматися — їм важливіше не пропустити чергового «прильоту»; для інших — це щось настільки загадкове, що простіше зробити вигляд, начебто його не існує. Але з іншого боку, дивлячись сюжет ТСН про українських хакерів, які на День Конституції отримали доступ до сімнадцяти сайтів «недоросії», а за три дні до того Держдума РФ прийняла так звані «поправки Ярової» і тепер будь-яка інформація з домену ***.ru*** фактично стає власністю Роскомнагляду, то десь у глибині душі починаєш розуміти, що світ змінюється і треба змінюватися разом з ним. Станом на сьогодні в Збройних Силах України відпрацьовано керівні документи, метою яких є забезпечення кібернетичної безпеки на всіх рівнях управління. Усі ці інструкції, накази та настанови не просто папірці, а дуже цінний матеріал, який реально допомагає зберігати інформацію, а відтак і життя. Отже, для збереження життя необхідно знати і дотримуватися вимог усіх тих паперів про комп'ютери, антивіруси, 3G-модеми й таке інше.

Але війна є війна — всього не передбачиш і не опишеш. Коли обстановка змінюється щохвилини і в кожній ситуації необхідно прийняти правильне рішення — саме ця стаття стане у пригоді. Найголовніше, можна дізнатися, як зробити так, щоб противник не отримав необхідної йому інформації

Нижче наведено кілька простих правил, дотримання яких мінімізує ризики витоку інформації та, відповідно, наслідки, які він може спричинити. Виконувати їх нескладно, але вкрай важливо!.

1. Вимкни визначення місцеперебування на всіх пристроях.

Це може бути телефон, планшет, комп'ютер. Сучасний світ — це світ соціальних мереж, у яких кожен хоче похвалитися тим, де він був та що робив. Саме тому деякі програми самостійно вмикають геопозиціонування пристрою і відправляють ці дані в мережу. Але те, що цікаво і корисно в цивільному житті, на війні вкрай небезпечно.

2. Онови антивірус!

Якщо ти наївно вважаєш, що твій комп'ютер, телефон чи планшет нікому не потрібен, або що віруси — це дрібниця, то серйозно помиляєшся. Сучасні шпигунські програми дають змогу не тільки копіювати інформацію з пристрою і передавати противнику, а ще й умикати камеру, записувати звук чи навіть приховано передавати дані про геопозиціонування.

3. Став сильні паролі.

Не важливо, чи це пароль розблокування телефону, чи пароль до сторінки в соцмережі. Паролі ламаються, і це не поодинокі випадки. Зламаний пароль, наприклад, до електронної скриньки дає доступ противнику до профілів у соціальних мережах, блогах та можливість здійснювати їхнє налаштування. Щоб цього не трапилося, не використовуйте для пароля дати народження близьких людей, номери телефонів та іншу інформацію, яку можна дізнатися з відкритих джерел. Натомість пароль має складатися з не менш ніж десяти символів, мати цифри і літери та містити хоча б одну велику літеру і спеціальний символ..

4. Не завантажуй програм та ігор невідомого походження та не переходь за посиланнями на сайти, про які не знаєш.

Ігри та програмне забезпечення можуть бути написані спеціально для шпигування за користувачем. Дозволи на кшталт «передавати дані», які надаються програмам, уже нікого не насторожують. А даремно. Адже надаючи дозвіл невідомому програмному забезпеченню на передачу даних, самостійне ввімкнення GPS або Wi-Fi, ти наражаєш на небезпеку не тільки себе, а й побратимів...

Дотримуватися цих правил нелегко, вони напружують і створюють дискомфорт у спілкуванні з рідними. Проте найважливіше, що ці правила допоможуть тобі повернутися додому. І нехай сьогодні спілкування з коханою чи батьками буде обмежене, вони не знатимуть точно, спокійно на ВОП чи ні, але вже завтра це допоможе бути разом.

Список використаних джерел

1. Кібербезпека в україні: правові та організаційні питання. Матеріали Всеукраїнської науково-практичної конференції 21 жовтня 2016 року. Одеський державний університет внутрішніх справ «Кібербезпека в Україні: правові та організаційні питання»

2. Кібербезпека: світові тенденції та виклики для України Дубов Д.В., завідувач відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД, к.політ.н. Ожеван

М.А., головний науковий співробітник відділу досліджень інформаційного суспільства та інформаційних стратегій НІСД, д.філос.н, професор

ГУЦОЛ Д. А., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольський державний
університет

ТРОЯНСЬКА ПРОГРАМА

Троянські програми, трояни, троянці (англ. Trojan Horses, Trojans) — різновид шкідницького програмного забезпечення, яке не здатне поширюватися самостійно (відтворювати себе) на відміну від вірусів та хробаків, тому розповсюджується людьми [1].

Троянська програма - це плід праці програміста. Ніяким іншим способом створити її неможливо. Програміст, що пише троянську програму, прекрасно усвідомлює, чого він хоче добитися, і у своїх намірах він завжди дуже далекий від альтруїзму [2].

Більшість троянських програм призначено для збору конфіденційної інформації. Їх завдання, найчастіше, полягає у виконанні дій, що дозволяють отримати доступ до даних, які не підлягають широкому розголосу. До таких даних належать користувача паролі, реєстраційні номери програм, відомості про банківські рахунки і т. Д. Решта троянці створюються для заподіяння прямого збитку комп'ютерній системі, приводячи її в зумовити.

До останніх можна віднести, наприклад, троянську програму PC CYBORG, яка приваблювала нічого не підозрюють користувачів обіцянками надати їм новітню інформацію про боротьбу з вірусом, що викликає синдром набутого імунодефіциту (СНІД). Проникнувши в комп'ютерну систему, PC CYBORG відлічувала 90 перезавантажень цієї системи, а потім ховала всі каталоги на її жорсткому диску і шифрувати знаходяться там файли [1].

Інша троянська програма називалася AOLGOLD. Вона розсилалася по електронній пошті у вигляді заархівованого файлу. У супровідному листі, що додається до цього файлу, говорилося про те, що AOLGOLD призначена для підвищення якості послуг, які надає своїм користувачам найбільший американський Internet-провайдер America Online (AOL). Архів складався з двох файлів, один з яких іменувався INSTALL.BAT. Користувач, що запустив INSTALL.BAT, ризикував стерти всі файли з каталогів C: , C: DOS, C: WINDOWS і C: WINDOWS SYSTEM на своєму жорсткому диску [2].

Подібного роду троянські програми, як правило, створюються підлітками, які хоч і одержимі пристрастю до руйнування, але не мають глибоких пізнань в програмуванні і тому

не можуть завдати істотної шкоди комп'ютерним системам, які зазнали нападу створених ними троянців. Наприклад, програма AOLGOLD прала себе з жорсткого диска, будучи запущена з будь-якого іншого дискового розділу за винятком C.

Троянські програми, авторами яких є професійні програмісти, що займаються розробкою програмного забезпечення в солідних фірмах мають іншу характеристику. Троянці, що входять в поширені комп'ютерні додатки, утиліти і операційні системи, становлять велику загрозу комп'ютерам, на яких вони встановлені, оскільки їх дії носять не деструктивний характер, а мають на меті збір конфіденційної інформації про систему. Виявити такі троянські програми вдається, як правило, чисто випадково. А оскільки програмне забезпечення, частиною якого вони є, в більшості випадків використовується не тільки якоїсь однієї компанією, що купила це програмне забезпечення, але також на великих Internet-серверах і, крім того, поширюється через Internet, наслідки можуть виявитися жахливими [1].

Троянські програми не можуть розповсюджуватися самостійно, тому використовують будь-яку з форм соціальної інженерії. Наприклад, коли користувач отримує електронного листа вкладення електронної пошти може бути замасковане, (наприклад, звичайна форма для заповнення). Троянська програма може нести вірусне тіло - тоді запустив троянця комп'ютер перетворюється в осередок «зарази».

Опишемо маскування троянської програми. Для того, щоб спровокувати користувача запустити троянця, файл програми (його назва, іконку програми) називають службовим ім'ям, маскують під іншу програму (наприклад, установки іншої програми), файл іншого типу або просто дають привабливе для запуску назву, іконку і т.п. Зловмисник може перекомпілювати існуючу програму, додавши до її вихідного коду шкідливий, а потім видавати за оригінал або підміняти його.

Щоб успішно виконувати ці функції, троян може в тій чи іншій мірі імітувати (або навіть повноцінно замінювати) задачу або файл даних, під які вона маскується (програма установки, прикладна програма, гра, прикладний документ, картинка). Схожі шкідливі і маскувальні функції також використовуються комп'ютерними вірусами, але на відміну від них, троянські програми не вміють поширюватися самостійно [3].

Троянська програма, будучи запущеною на комп'ютері, може причинити шкідливі дії:

- заважати роботі користувача (жартома, помилково або для досягнення якихось інших цілей);
- шпигувати за користувачем;
- використовувати ресурси комп'ютера для якої-небудь незаконної (а іноді і завдає прямої шкоди) діяльності і т.д. [3].

Способи видалення**.** Загалом, троянські програми виявляються та видаляються антивірусним і антишпигунським ПЗ так само, як і інші шкідливі програми. Проте їх складніше виявити контекстними методами антивірусів (заснованих на пошуку відомих програм), бо їх розповсюдження краще контролюється й екземпляри програм потрапляють до спеціалів антивірусної індустрії з більшою затримкою, ніж саморозповсюджувані шкідницькі програми. Однак еврістичні (пошук алгоритмів) і проактивні (стеження) методи на стільки ж дієві. [].

ВИСНОВОК. Захистити комп'ютер від вірусів може тільки сам користувач. Правильне і своєчасне застосування антивірусних засобів може гарантувати від зараження або забезпечити мінімальний збиток, якщо зараження відбулося. В даний час заслуженою популярністю користуються комплексні рішення, що поєднують в собі всі методи захисту проти більшості шкідливих програм. Такого роду комплекси ще називають "сьютами" (від англ. Suite - набір, комплект).

До найбільш відомих програм вітчизняного та зарубіжного виробництва для повного захисту комп'ютера слід віднести: Norton AntiVirus Internet Security, Panda Antivirus Internet Security, Trend Micro Enterprise Protection Strategy, McAfee Active Virus Defense, Sophos Anti-Virus, NOD 32, а також найбільш популярні вітчизняні засоби захисту - полифаг Doctor Web і антивірусний комплекс «Доктор Касперський».

Список використаних джерел

1. Троянські програми в ОС Windows. URL: http://ukrbukva.net/page,10,93766-Troyanskie-programmy-v-OS-Windows.html (дата звернення 16.10.2017).

2. Троянська програма : https://uk.wikipedia.org/wiki/Троянська_програма (дата звернення 17.10.2017).

3. Виявлення вірусів і шкідливих програм і їх усунення: http://stud.com.ua/62478/menedzhment/viyavlennya_virusiv_shkidlivih_program_usunennya (дата звернення 17.10.2017).

ДЕЙНЕГА Г. О., ОС «Бакалавр»
спеціальність «Системний аналіз»
Маріупольський державний
університет

ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Актуальність теми полягає в тому, що національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів організаційного, правового, політичного, соціально-економічного, науково-технічного, правоохоронного, оборонного, інформаційного, освітнього характеру, заходів із захисту інформації та кіберзахисту.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

- державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту комунікаційних та технологічних систем критичних інфраструктурних об'єктів, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів кібербезпеки щодо кіберзахисту;
- забезпечує створення та функціонування національної телекомунікаційної мережі, упровадження організаційно-технічної моделі кіберзахисту;
- здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них;
- координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем критичних інфраструктурних об'єктів на вразливість; забезпечує функціонування з цією метою державного центру кіберзахисту.

Функціонування національної системи кібербезпеки забезпечується шляхом:

- вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами ЄС та НАТО;
- створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту

інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

- формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;
- залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;
- проведення навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;
- функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;
- розвитку мережі команд реагування на комп'ютерні надзвичайні події;
- розвитку та вдосконалення системи технічного і криптографічного захисту інформації;
- забезпечення виконання вимог із захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;
- створення та забезпечення функціонування національної телекомунікаційної мережі;
- упровадження організаційно-технічної моделі національної системи кібербезпеки, як комплексу заходів, сил та засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, що здатні зменшити вразливості комунікаційних систем;

Отже, порядок функціонування національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

Список використаних джерел

1. Гальчинський А. Кібербезпека: особливості та функціонування / А.Гальчинський // Кібербезпека України. – 2017. - №3. – С.4-13.

2. Ковальчук В.В. Національна система кібербезпеки України. [Навчальний посібник]/ В.В.Ковальчук. – К.: «Слово», 2016. – 240 с.

3. ЛудченкоА. Функціонування національної системи кібербезпеки / А.Лудченко, Я.Дудченко, Т.Примак. – К.: Знання, 2015.- 113с.

4. Романенко О.Г. Кібербезпека. [Навчальний посібник]/О.Г. Романенко, Г.Ю. Максимович, О.Р. Самойлюк та ін. - М.: Рос. Екон. Акад., 2016. - 198 с.

5. Цехмістрова Г.С. Кібербезпека України Навч. посібник / Г.С. Цехмістрова. – К.: Слово, 2015. – 240 с.

ЗАХАРОВА А. Р., ОС «Бакалавр»,
спеціальність «Системний аналіз»
Маріупольський державний
університет

АКТУАЛЬНІ КІБЕРЗАГРОЗИ І СПОСОБИ ЗАХИСТУ ВІД НИХ

На сьогоднішній день актуальною темою є кібербезпека, так як какждий з нас напевно стикався з недоброзичливцями в мережі інтернет. Головним завданням кібер фахівців є забезпечення безпеки ресурсів організацій і користувачів.

Кібербезпека є фундаментальним питанням для кожного бізнесу, який представлений в інтернеті. Насправді, кібербезпека є важливою для будь-якого інтернет-користувача, тож для серйозних компаній вона особливо значуща. Ось чому ми раніше розповідали вам головне, що варто знати про безпеку Drupal-сайтів, а також, як захистити веб-сайт. У сьогоднішній статті ми згадаємо кібер-загрози, які дуже поширені на даний час. Крім того, запропонуємо вам поради, які допоможуть підготуватися до них, щоб уникнути кібер-атак.

Найбільші загрози кібербезпеці у 2017 році.

Програми-вимагачі (віруси-вимагачі) здатні заблокувати доступ жертви до своїх данних. Зловмисники їх використовують для вимагання викупу, погрожуючи оприлюднити отриману секретну інформацію або її знищити. Доповідь, підготовлена SonicWall у 2017 на основі їхніх щорічих досліджень показала, що кількість випадків злому ПЗ із метою отримання викупу останнім часом різко зросла від 3,2 млн. у 2014 та 3,8 млн. у 2015 до 638 млн. у 2016 році.

«Locky» — один з видів вищезгаданого шкідливого програмного забезпечення. Це програма-шифрувальник, яка виглядає, як Word-документ, який просить користувача активувати макроси. Locky шифрує всі файли жертви, включаючи зображення, відеозаписи і т. п.

Фішинг (phishing) — це вид шахрайства, метою якого є отримання конфіденційної інформації довірливих чи неуважних користувачів (паролів, логінів, даних кредитних карток тощо). Згідно із дослідженням Wombat 2017 State of the Fish, 44% організацій стали жертвами фішингу через SMS-повідомлення (smishing) і телефонні дзвінки (vishing). Хакери також можуть відправляти шахрайські листи електронною поштою від імені співробітників чи з акаунтів, котрим довіряють.

61% компаній відчули на собі наслідки так званого цілеспрямованого фішингу. У таких випадках збирається інформація про важливих осіб серед співробітників компанії з метою створення більш персоналізованих, індивідуальних, а отже, і більш переконливих повідомлень, щоб спонукати жертв добровільно надати конфіденційну інформацію.

Малвертайзинг (malvertising) або шкідлива реклама є способом поширення шкідливих програм через онлайн-рекламу. Сучасні методи дозволяють обійти блокування реклами без дозволу користувача, щоб запустити код вірусу. RiskIQ 2016 Malvertising Report показав, що випадки малвертайзингу зросли на 132,6% в 2016 у порівнянні з 2015 роком [1].

7 порад для запобігання хакерським атакам і підвищення веб-безпеки:

Створіть надійні бекапи та копіюйте дані щодня чи навіть щогодини, якщо це можливо, і поміщайте їх в надійне місце. Краще використовувати кілька бекапів або кілька систем резервного копіювання. Це допоможе вам відновити данні після хакерського злому.

Перейдіть з HTTP на HTTPS, адже цей протокол був розроблений для автентифікації і шифрування комунікацій в інтернеті. SSL та TLS створюють додатковий шар захисту, особливо необхідний, якщо ви працюєте з приватними данними користувачів чи платіжними системами.

Оновіть сайт до останньої версії. Підтримання найновіших версій означає покращені функціональні можливості, які забезпечують вищий рівень безпеки.

Регулярно проводьте аудит безпеки сайту, перевіряйте наявність вразливих місць та багів, та фіксіть у разі їх виявлення.

Моніторте аптайм і даунтайм сайту, щоб бути в змозі вчасно зреагувати так швидко, як це можливо в тих випадках, коли ваш сайт впав і є недоступним.

Захистіть свої акаунти в соцмережах, свої бізнес-сторінки, щоб уникнути їх компрометації.

Не звантажуйте неперевірені файли, документи, вкладення чи додатки. Не натискайте на невідомі посилання, оголошення, сайти і так далі [2].

Неповноцінність у системі органів державного управління кількісного складу юристів, які спеціалізуються на інформаційному праві, зумовлює недостатність забезпечення обсягу вироблення конкурентоспроможного в глобальному інформаційному просторі національного інформаційного продукту. У цьому сенсі інформаційна безпека конвертується в економічну. Через неналежний рівень підготовки юристів у більшості вищих навчальних закладах щодо інформаційного права, правової інформатики, правового регулювання інформаційної безпеки наближається до критичного стан застосування інформаційно-комп'ютерних систем у галузі державного управління, внутрішніх і міжнародних комунікацій [2].

Ураховуючи різноманіття проблем, досліджених в юридичній науці, слід зазначити, що аспект інформаційної безпеки в умовах глобалізації інформаційного простору ставить завданням вироблення теоретико-правових, методологічних, концептуальних, доктринальних, стратегічних, тактичних та оперативних правових засобів, здатних урегулювати суспільні інформаційні відносини, що здійснюються у взаємозв'язку з

міжнародними правовими процесами гармонізації законодавства про інформаційну безпеку як підгалузь законодавства про інформацію.

У висновку хочу сказати, що дотримуючись простих правил і остерігаючись невідомих сайтів і програм, ви можете убезпечити себе або свій бізнес від небезпеки ховається на просторах інтернету.

Список використаних джерел

1. RiskIQ Finds Malvertising on the Rise Once Again URL: https://www.riskiq.com/blog/labs/malvertising-on-the-rise-once-again/ (дата звернення 16.10.2017)

2. Аудит безпеки сайту: більше ніж просто душевний спокій! URL: https://drudesk.com.ua/blog/audit-bezpeki-sajtu (дата звернення 16.10.2017)

КОНЄВА О.І., ОС «Бакалавр»
спеціальність «Системний аналіз»,
Маріупольський державний
університет

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Поняття безпеки є досить широким в області захисту інформації. Ця дефініція має на увазі і надійність роботи комп'ютера, і збереження цінних даних, і захист інформації від внесення в неї змін не уповноваженими особами, і збереження таємниці листування в електронному зв'язку. Завжди існує проблема вибору між необхідним рівнем захисту і ефективністю роботи в мережі.

Розглянемо проблем захисту інформації в комп'ютерних мережах та шляхи їх вирішення. Основні проблеми захисту інформації при роботі в комп'ютерних мережах, можна умовно розділити на три типи: 1) перехоплення інформації (порушення конфіденційності інформації); 2) модифікація інформації (спотворення вихідного повідомлення або заміна іншою інформацією); 3) підміна авторства (крадіжка інформації та порушення авторського права).

Сьогодні захист комп'ютерних мереж від несанкціонованого доступу характеризується зростанням ролі програмних і криптографічних механізмів в порівнянні з апаратними. Нові проблеми в галузі захисту інформації вже вимагають використання протоколів та механізмів з порівняно високою обчислювальною складністю.

Особливостями сучасних інформаційних технологій, прямо або побічно впливають на безпеку інформації, є [1, с. 45]:

1. Збільшення числа автоматизованих процедур в системах обробки даних і посилення важливості прийнятих на їх основі рішень;

2. Територіальна розподіленість компонентів комп'ютерних систем і передача інформації між цими компонентами;

3. Ускладнення використовуваних програмних і апаратних засобів комп'ютерних систем;

4. Накопичення та довготривале зберігання великих масивів даних на електронних носіях, часто не мають твердих копій;

5. Інтеграція в єдиних базах даних інформації різного призначення і різних режимів доступу;

6. Безпосередній доступ до ресурсів комп'ютерних систем великої кількості користувачів різних категорій і з різними повноваженнями в системі;

7. Зростання вартості ресурсів комп'ютерних систем.

Вирішення проблем захисту мереж *сучасної практичної* інформатики призвели до виникнення наступні групи засобів:

1. Організаційна захист інформації - це регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво ускладнює неправомірне заволодіння конфіденційною інформацією, що включає в себе організацію режиму охорони, організацію роботи з співробітниками, з документами, а також організацію використання технічних засобів і роботу по аналізу загроз інформаційній безпеці.

2. Способи антивірусного захисту становлять технічні та програмні засоби захисту інформації від вірусів. Вірус - це програма містить, шкідливий код, тому основним засобом від їх захисту є антивірусне ПЗ - додаток, що забезпечує відстеження і знищення вірусів.

3. Використання надійного пароля є одним з найбільш важливих факторів захисту комп'ютера від зловмисників та інших небажаних користувачів.

4. Криптографія - це комплексна наука про захист даних. Захист здійснюється на основі математичних перетворень даних.

5. Стенографія - (від грец. «Тайнопис») розділ знань про захист даних здійснюється на основі математичних перетворень даних та основі приховування каналу передачі.

Висновок. Важливою особливістю використання інформаційних технологій є необхідність ефективних рішень проблеми захисту інформаційного ресурсу, що передбачає розосередження заходів щодо захисту даних серед користувачів. Інформацію необхідно захистити в першу чергу там, де вона міститься, створюється і переробляється, а так само в тих організаціях, на інтереси яких негативно впливає зовнішній доступ до даних. Це

найраціональніший і ефективний принцип захисту інтересів організацій, що є первинним осередком на шляху вирішення проблеми захисту інформації та інтересів держави в цілому.

Список використаних джерел:

1. Гафнер В.В. Інформаційна безпека: навч. допомога. - Ростов на Дону: Фенікс, 2010. - 324 с.
2. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96 Державний стандарт України. — [Чинний від 1997-07-01]. — К. : Держспоживстандарт України, 1997. — IV, 5 с. — (Національний стандарт України)
3. Антонюк А. Аналіз складу профілів захищеності інформації / Анатолій Антонюк, Денис Берестов, Сергій Пустовіт // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.- техн. збірник. – 10 вип., 2005. – С. 46 – 51.

КСЕНОФОНТОВА А. Е.,
ОС «Бакалавр» спеціальність,
«Системний аналіз»,
Маріупольський державний
університет

ЗМІСТ КІБЕРЗАГРОЗ СЬОГОДЕННЯ

Кіберзагрози у сучасному суспільстві набирають значного масштабу. Відтепер успішна атака хакерів може знеструмити цілу область або країну, призвести до пограбування банку чи знищити успішну організацію. Наприклад, за різними оцінками, за 2015 рік з рахунків підприємств України зникло близько 100 млн грн.

З метою проведення коректних та ефективних заходів щодо відвернення кіберзагроз та ліквідації їх негативних наслідків, перш за все, необхідним є їхня легітимація – вироблення та закріплення законодавчої дефініції, задля уникнення порізненості при застосуванні даної категорії, а також колізії з іншими нормативно-правовими актами, та визначення їх змісту, уніфікованості правозастосовної практики.

Зауважу, що, незважаючи на досить часте використання категорії «кібернетичні загрози» у доктрині, публіцистиці та у повсякденному житті, її законодавче уніфіковане визначення поняття відсутнє, як на національному, так і на міжнародному рівнях. Це відбувається на тлі того, що кіберзагрози за своєю природою не є локальними, тобто обмеженими певної територією або навіть державними кордонами, а навпаки: вони становлять глобальне явище, яке носить негативний і почасти деструктивний характер.

Кібернетична загроза (кіберзагроза) – наявні та потенційно можливі явища і чинники, що створюють небезпеку інтересам людини, суспільства та держави через порушення

доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури.

У Доктрині інформаційної безпеки України (втратила чинність) було зазначено, що в інформаційній сфері України вирізняються такі життєво важливі інтереси:

1) *особи*: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

2) *суспільства*: збереження і примноження духовних, культурних і моральних цінностей українського народу;

3) *держави*: недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур;

В міжнародному законодавстві й досі відсутнє єдине визначення понять «кібернетична безпека», «кібернетична загроза», «кібернетичний захист», «кібернетичний простір», «кібернетична злочинність». Проблема кібербезпеки специфічна та глобальна, тому максимальна ефективність у боротьбі з новими загрозами може бути забезпечена.

Кібернетичні загрози являють собою загрози, реалізація яких пов'язана з використанням відповідних ресурсів інформаційно-телекомунікаційних систем. Уразливими для реалізації кібернетичних загроз є об'єкти, функціонування комп'ютерних систем яких пов'язане з використанням ресурсів кіберпростору.

Нині виокремлюють такі загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Україна має швидко, надійно та ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів кібербезпеки. Аналіз законодавства у сфері кібербезпеки, а також організаційних заходів, спрямованих на розбудову ефективних систем кіберзахисту.

У питаннях протидії кіберзагрозам повинні застосовуватися принципово нові механізми. Ефективним засобом протидії кіберзагрозам може стати розбудова нових ліній оборони. З тим, щоб у разі кібератаки компетентні органи сторони, яка зазнала нападу, і сторони, з території якої походить кібератака, оперували механізмами оперативного сповіщення про такий інцидент, а також спільної боротьби з ним.

Саме тому надзвичайно важливо якомога швидше консолідувати зусилля держав для запобігання новітнім кіберзагрозам і одним із основних напрямків є зміцнення політичної довіри між урядами.

Список використаних джерел

1. «Віртуальний ворог»: як захистити бізнес від кібератак? [Електронний ресурс]. — Режим доступу : http://www.polukr.net/uk/blog/2016/08/virtualnyj-voroh-jak-zahistiti-biznes-vid-kiberatak/.

2. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В. П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 312-320.

3. Сучасні тренди кібербезпекової політики: висновки для України [Електронний ресурс]. — Режим доступу : http://www.niss.gov.ua/articles/294.

4. Кіберзагрози і кібербезпека: чи здатні фахівці протистояти хакерам? 19.09.2016 р. [Електронний ресурс]. — Режим доступу : http://ukr.obozrevatel.com/news/34918-kiberzagrozi-i-kiberbezpeka-chi-zdatni-fahivtsi-protistoyati-hakeram.htm

МІТЬКО Н. В. . ОС «Магістр»,
спеціальність «Право»,
Маріупольський державний
університет

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ У СФЕРІ КІБЕРЗАХИСТУ УКРАЇНИ

З моменту отримання незалежності в Україні сформоване нове національне законодавство, яке регулює суспільні відносини в інформаційній сфері. Норми в цій сфері істотно впливають на нормативно-правове регулювання відносин між суспільством, його членами і державою. Тобто на сучасному етапі інформаційні відносини виступають, з одного боку, змістовним наповненням будь-яких відносин в житті країни, суспільства і громадян, з іншого тими засадами, на яких формується законодавство в інших сферах їх існування.

У свою чергу, для створення сучасної та ефективної системи істотне значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити всі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави і ефективно реалізовувати політику національної безпеки в інформаційній сфері.

Законність функціонування є одним з головних вимог до системи. Ця законність повинна базуватися на сукупності законів та підзаконних нормативних актів, спрямованих на створення необхідних умов для захисту національних інтересів в інформаційній та інших сферах життя країни.

Функціонування та захист вітчизняного інформаційного простору є важливим завданням держави на сьогоднішній день.

Негативні тенденції, які спостерігаються у вітчизняному мас-медіа та інтернет-ресурсах, свідчать про необхідність посилення заходів щодо забезпечення державою інформаційної безпеки і, насамперед, кібербезпеки як складової системи захисту вітчизняних інформаційних ресурсів.

Акутальні питання інформаційної безпеки держави досліджували: А.Марущак, В.Петрик, В.Ліпкан та інші фахівці. Проблемні питання забезпечення кібернетичноїбезпеки розглядали у своїх наукових працях В.Бурячок, А.Бабенко, В.Бутузов, В.Гавловский, В.Голубєв, С.Гнатюк, Д.Дубов, В.Номоконов, В.Петров,М.Погорецький, В.Шеломенцев.

В Україні за час її незалежності сформовані необхідні законодавчі основи системи, зокрема було прийнято великий масив нормативно-правових актів, де визначено основні повноваження державних органів в інформаційній сфері. Акти національного законодавства, які визначають правовий статус державних органів, організацій і громадян, встановлюють повноваження державних органів України.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

У сучасних умовах вітчизняні інформаційні відносини, пов’язані із забезпеченням кібернетичної безпеки в державі, врегульовані низкою законодавчих актів України: «Про інформацію», «Про науково-технічну інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», проте не існує єдиного нормативно-правового акта за вказаною проблематикою. Правові основи забезпечення кібербезпеки України.

Таким чином, у контексті вітчизняного законодавчого регулювання кібернетичної безпеки існує достатня кількість правових норм, спрямованих на регламентацію засад забезпечення вітчизняної кібернетичної безпеки. На сьогодні реальні прояви кібератак можуть призвести до порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони.

У зв’язку із цим існуючі загрози вимагають вжиття державою комплексних заходів щодо забезпечення кібербезпеки. За таких умов сучасна державна політика у сфері забезпечення кібернетичної безпеки має бути спрямована на забезпечення інформаційного суверенітету України у кіберпросторі, створення надійного захисту національного сегменту

кіберпростору; зміцнення обороноздатності держави у кіберпросторі; боротьбу з кіберзлочинністю та кібертероризмом; недопущення та запобігання втручанню у внутрішні справи України і припинення посягань на її інтернет-ресурси з боку інших держав.

Виходячи з цього розбудовувати національну систему кібербезпеки слід за трьома основними напрямами: протидія кіберзлочинності; захист вітчизняного інформаційного простору в комп'ютерних мережах; забезпечення інформаційної безпеки критичної інфраструктури тому актуальними як з позиції фундаментальної теорії, так і практичної складової державного управління залишаються подальші наукові дослідження у контексті розробки дієвого механізму державного регулювання та забезпечення кібернетичної безпеки.

Список використаних джерел

1. Конституція України// Верховна Рада України; Конституція, Закон від 28.06.1996 № 254к/96-ВР

2. Про інформацію // Верховна Рада України; Закон від 02.10.1992 № 2657-XII

3. Інформаційна складова державної політики та управління : монографія / С. Г. Соловйов, О.Є. Бухтатий, Ю.В. Нестеряк [та ін.] ; за заг. ред. Н. В. Грицяк ;Нац. акад. держ. упр. при Президентові України. –К. : К.І.С., 2015. – 319 с.

4.Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А. Л. Бурячок // Сучас. спец. техніка. –2011. – № 3 (26). – С. 104–114.

5. Рязанцева І. М. Проблемні питання розбудови національної системи кібербезпеки / І. М. Рязанцева, В. В. Тулупов // Право і Безпека : наук. журн. – 2014. –№ 2 (53). – С. 140–144.

НОВИКОВ І. О., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольський державний
університет

ЗАХИСТ СОЦІАЛЬНИХ МЕРЕЖ

Зараз новим середовищем, де зосереджений величезний обсяг інформації, є Інтернет. З його появою, популярним явищем стали соціальні мережі, в яких мають облікові записи до 82% всіх користувачів мережі.

Обліковий запис, як правило, містить відомості, необхідні для впізнання користувача при підключенні до системи. Обліковий запис може містити також додаткові дані - фотографії, ПІБ, псевдонім, віросповідання, дату народження, адресу e-mail, домашню адресу, номер телефону та інші.

Методи захисту

Яким же чином можна захистити свою сторінку і персональні дані? Для цього буде потрібно виконання наступних рекомендацій:

- використовуйте механізми безпеки, що надаються соціальними мережами;

- використовуйте загальні механізми безпеки, не прив'язані до соціальних мереж;

- перебуваючи в соціальній мережі, робіть дії, які не загрожують ваших персональних даних.

Майже всі соціальні мережі мають правила розмежування доступу різних категорій користувачів до інформації, що міститься на сторінці користувача. Наприклад, можна дати доступ до одного зі своїх альбомів всім користувачам, а до іншого - тільки друзям. Або надати можливість перегляду коментарів до записів на своїй стіні тільки деяким з друзів. Таким чином, уважно поставтеся до налаштування доступу інших користувачів до своєї особистої інформації в соціальних мережах.

Варто окремо згадати про пошук в соціальних мережах, який дає можливість будь-якому користувачеві отримати певний перелік інформації про конкретний профілі (навіть якщо останній максимально захищений вбудованими засобами від всіх незнайомих профілів). Суть його полягає в пошуку даного (вже відомого) профілю з застосуванням фільтрів пошуку. Наприклад, про даному профілі знаємо тільки ім'я, прізвище і країну проживання. Ввівши тільки ці відомості в пошук, отримуємо деяку кількість профілів з такими ж параметрами. Потім додаємо додатковий фільтр, наприклад вік. Якщо при заданому додатковому параметрі цікавий для нас профіль знову з'являється в результатах пошуку, то знову введене значення фільтра виявилося вірно, і можна продовжувати уточнення інших відомостей аналогічним способом (використовуючи інші фільтри). Якщо ж ні, то необхідно взяти інше значення цього фільтра. Безумовно, даний алгоритм можна оптимізувати.

Безпека: Зловмисники використовують сайти соціальних мереж не тільки для пошуку компромату, а й для атаки на вас або ваші мобільні пристрої. Ось деякі кроки, які допоможуть вам захистити себе:

- **Логін:** Використовуйте для захисту облікового запису тільки надійний пароль і нікому його не повідомляйте або не використовуйте повторно для інших сайтів. Крім того, багато сайтів підтримують більш надійну аутентифікацію, наприклад двоступеневу перевірку. По можливості, користуйтеся їй.

- **Шифрування:** Більшість сайтів соціальних мереж використовують мережевий протокол HTTPS для безпечного з'єднання. HTTPS забезпечує шифрування даних при передачі по комп'ютерних мережах. Деякі сайти, такі, як Twitter, Google+ використовують

цей протокол за умовчанням, на інших потрібно конфігурувати з'єднання HTTPS. Використовуйте безпечний протокол HTTPS, якщо це можливо.

- **Електронна пошта:** З обережністю ставитеся до листів, які приходять від імені соціальних мереж; зловмисники легко можуть підробити їх для атаки. Найбезпечніший спосіб відповіді на такі листи безпосередньо з самого сайту соціальних мереж, наприклад, з закладок; перевіряйте повідомлення або повідомлення тільки з веб-сайта.

- **Шкідливі посилання / Обман:** Будьте обережні з підозрілими посиланнями або помилковими публікаціями на сайтах соціальних мереж. Кіберзлочинці можуть розміщувати шкідливі посилання. Якщо ви клацніть по ним, то потрапите на шкідливі сайти, які спробують заразити ваш комп'ютер. Увага, якщо прийшло повідомлення від одного, це не означає, що він його відправляв - його аккаунт могли зламати. Тому якщо ви отримали підозріле повідомлення від члена сім'ї або друга (наприклад, що його пограбували і йому потрібні гроші), зв'яжіться з ним по телефону, щоб розвіяти сумніви.

- **Додатки:** Деякі соціальні мережі надають можливість встановити програми, створені сторонніми розробниками, наприклад, гри. Пам'ятайте, ці програми піддаються мінімальної перевірці або зовсім не перевіряються на предмет наявності недекларірованних функцій і шкідливого коду, Через них можна отримати контроль над вашим аккаунтом або доступ до персональних даних. Встановлюйте лише ті додатки, які вам дійсно потрібні, завантажуйте їх з відомих, перевірених сайтів і відразу ж видаляйте після використання.

Соціальні мережі являють собою потужний і зручний спосіб спілкування зі світом. Якщо ви будете слідувати нашим рекомендаціям, то ваше онлайн спілкування стане безпечніше. Ви можете ознайомитися з додатковими правилами безпеки на сайті веб сервісу, який ви використовуєте. У випадках несанкціонованої активності повідомляйте в службу підтримки користувачів.

ОВСЯНИЦЬКИЙ В. В.,
ОС «Бакалавр», спеціальність
«Системний аналіз»,
Маріупольський державний
університет

АНАЛІЗ КОМП'ЮТЕРНОГО ВІРУСУ PETYA.A

Не так давно, а саме влітку 2017 року десятки українських компаній та установ зазнали масштабної хакерської атаки. Вірус-вимагач Petya.A атакував банки, поштових і телеком-операторів і енергетичну систему країни.

Що таке Petya.A? 27 червня комп'ютерний вірус, спрямований на Windows-системи, паралізував роботу багатьох установ в Україні, включаючи банки, державні підприємства та приватні компанії. Вважається, що це модифікація вірусу Petya, який лютував ще в 2016 році. За іншими даними, це модифікація вірусу WannaCry, який заразив понад 100 тис. комп'ютерів в травні 2017 року [2].

Які основні джерела зараження Petya.A? Основним джерелом зараження вірусом Petya були посилання, розповсюджувані по електронній пошті і в месенджерах. Шкідливий спам містив посилання на сервіс Dropbox, при активації якої відбувалася завантаження інсталятора Malware [3].

Що відбувається з жертвами після зараження? Запуск *.exe файлу призводить до падіння системи в синій екран і наступному перезавантаженню. Після перезавантаження комп'ютера жертва бачить імітацію перевірки диска (CHKDSK), по закінченні якої на екрані комп'ютера завантажується зовсім не операційна система, а екран блокування Petya.

Вимагач повідомляє потерпілому, що всі дані на його жорстких дисках були зашифровані за допомогою «військового алгоритму шифрування», і відновити їх неможливо.

Кібератака переслідує мету вимагати у жертв гроші - 300 доларів США, але в цифровий валюті, так званих біткоїнах. Для цього вірус-вимагач шифрує дані комп'ютера користувача, вимагаючи викуп за розшифровування.

Вимоги вірусу надмірно небезпечні: якщо протягом трьох днів користувач не заплатить викуп, необхідна сума збільшується удвічі. Після семи днів відновити дані буде неможливо, погрожують нападники. Атака вважається небезпечною, тому що вірус копіює сам себе до безкінечності, якщо знаходить інші комп'ютери, у яких є аналогічна дірка в системі безпеки [4].

Хто може заразитися? Вірус поширюється тільки на комп'ютери, на яких встановлена операційна система Windows і загрожує лише тим користувачам, які відключили функцію автоматичного оновлення системи. Оновлення у вигляді виключення доступні навіть для власників старих версій Windows, які вже не оновлюються: XP, Windows 8 і Windows Server 2003.

Як видалити Petya.A? Так як вірус Petya дуже схожий на Wncry. Раніше боролися з Wncry так:

1. Варто включити безпечний режим із завантаженням мережних драйверів. У Windows 7 це можна зробити при перезавантаженні системи після натискання клавіші F8. Також є інструкції по виконанню цього кроку для інших версій, у тому числі Windows 8 і Windows 10.

2. Можна самостійно видалити небажані програми через «Видалення програм». Однак щоб уникнути ризику помилки і випадкового збитку системі, варто скористатися антивірусними програмами на кшталт SpyHunter Anti-Malware Tool, Malwarebytes Anti-malware або STOPZilla [1].

Як розшифрувати файли після Petya.A? Після видалення даного вірусу потрібно буде відновити зашифровані файли. Інакше можна завдати шкоди системних файлів і реєстрів.

Для відновлення файлів можна використовувати декрипторы, а також утиліту Shadow Explorer (поверне тіньові копії файлів і початковий стан зашифрованих файлів) або Stellar Phoenix Windows Data Recovery. Відзначимо, що ці способи не гарантують повного відновлення файлів.

Як поширюється вірус Petya?

Тут як з зомбі-апокаліпсисом – джерело вже не важливе. Хтось десь відкрив у пошті прикріплений файл від невідомої особи, заразив комп'ютер, а той в свою чергу, використовуючи уразливість в Windows, заразив інші комп'ютери в цій мережі.

А все чому? Тому що люди лінуються оновлювати Windows (звідси можливість для вірусу заражати ПК по мережі), а клацати на вкладення від невідомих джерел – це без проблем.

Таким чином з усього вище сказаного можна зробити висновок: оновлюйте систему і не клацайте на незрозумілі посилання.

Список використаних джерел:

1. Юлія Гуреваі «Рада прийняла закон про кібербезпеки України» [Електронний ресурс]. – Режим доступа: https://www.unian.net/politics/2171886-poroshenko-vnes-v-vrdorabotannyiy-zakonoproekt-o-prodlenii-osobogo-statusa-ordlo.html

2. Vesti Ukraine «Все что известно о вирусе WannaCry и Petya.A» [Електронний ресурс]. – Режим доступа: http://vesti-ukr.com/mir/244843-vse-chto-izvestno-o-viruse-wannacry-i-

3. Новое время «Захисти себе сам. Все ще потрібно знати про вірус Petya.A» [Електронний ресурс]. – http://nv.ua/ukr/techno/gadgets/zahisti-sebe-sam-vse-shcho-potribno-znati-pro-virus-petya-a-1392163.html

4. Tech today «Все что нужно знать о вирусе Petya и как с ним бороться» [Електронний ресурс]. – https://techtoday.in.ua/ru/reviews-ru/vse-chto-nuzhno-znat-o-viruse-petya-kak-s-nim-borotsya-75861.html

ПАНОВ К. В., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольський державний
університет

БОТНЕТ

Ботнеты являются объектом нелегальной торговли. Ботнет (англ. botnet) —сегодня распространенная проблема в интернете и его безопасности, это сеть компьютеров иногда серверов, которые через уязвимости в ПО или по обычной глупости юзеров заражены вирусами и троянами предназначенными для «зомбирования» вашего пк (обычно потому управляют через удаленный контроль или скрытого пользователя), цель которых в первую очередь не навредить вашим данным или удалить их, а превратить компьютер в «зомби» (или бота), в таком состоянии в котором злоумышленник сможет использовать вычислительные ресурсы компьютера в своих целях. Как вариант — использовать как анонимный удаленный пк в незаконных схемах(кардинг, теневой бизнес и др).

В одним из крупнейших известных ботнетов контролировал сеть более чем на 12 млн. Это стало известно в марте 2010, хакера который его запустил так и не поймали

Основная опасность и возможности Ботнета

Список возможностей ботнета сам по себе довольно большой как и способы применения их различаются(и каждый день меняются и добавляются новые), но в основном все они разделяются на такие категории:

1. Loader: есть почти во всех вирусах и троянах использующие для ботнета. Обновляет или устанавливает старые версии бота, загружает через сеть все что нужно хакеру и не нужно вам (трояны, новые боты и т. д.). С помощью этой программы на все компьютеры одновременно могут быть установлены троянские программы шпионы, которые передают все, когда-либо введенные на данном компьютере данные.(это может быть даже данные кредитной карты или банковский аккаунт)

Keylogger: перехват и сохранение введенных на клавиатуре символов с последующей отправкой хакерам. (как вы понимаете количество данных и возможности такого вируса не ограничены, поскольку такой логгер записывает что и где вводите например на сайте сбербанка данные о карте и прочие)

2. DDoS: атакует сервера или другие пк путём перегрузки множеством запросов от сети ботов. Такая атака может полностью положить сервер или пк, или серьезно навредить его работе . Иногда его используют для кибер-шантажа, требуя выкуп для остановки атаки. Разумеется и в и политических целях, атакуя правительственные сайты и прочие интересные ресурсы (Например хакеры из группировки анонимус часто наказывает своих недругов

именно таким способом и являются владельцами одних из самых крупных сетей ботнет). Одной из успешных и известных атак на сервера майкрософта с помощью вируса-трояна «MSBlast!», который в один день начал долбить запросами со всех компьютеров адрес microsoft.com, из-за чего сайт ушел в отстой и падал пару раз.

3. Spam: (более 80% мирового трафика загружено такими вирусами и сообщениями) заранее заготовленный шаблон спам-сообщения и начать рассылку спама на указанные адреса, и часто в самих сообщения встроен loader, а как мы уже знаем он может загрузить все остальное ...

4. Proxy: использовать компьютера из сети ботнет как прокси-сервер для анонимности, то есть шифрование трафика хакера, который будет пользоваться вашим пк, часто используют кардеры и дельцы теневого бизнеса, а опасность заключается в том что потом приедут за вами и доказать свою невинность будет очень трудно, а иногда даже невозможно

5.VNC

Это удаленный доступ к вашему ПК, часто используется для Cryptomining криптовалют — Это заражение компьюетра скрытым майнером и его подальшие распространение по сети то есть в нем встроенные почти все вышеперечисленные возможности, для того чтобы майнить криптовалюты(к примеру биткоин), это самое распространенное использование ботнета сейчас из-за растущей популярности и стоимости криптовалют.

Контроль и использование сети довольно часто происходит не самими хакерами. а компаниями которые у них их купили, например для уничтожение конкурентов, дудос сайтов конкурента и прочие варианты коммерческого использования и монетизации сети бонет.

Торговля. Ботнеты являются объектом нелегальной торговли, при продаже передаётся пароль к IRC-каналу (пароля доступа к интерфейсу программы на компьютере).

Масштаб. По оценке создателя протокола TCP/IP Винта Серфа, около четверти из 600 млн компьютеров, подключённых к Интернету, могут находиться в ботнетах.

По данным специалиста по безопасности только в США в составе ботнетов порядка 5 млн заражённых компьютеров, что составляет около 10 % национального компьютерного парка

ПУРДИК К. А., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольський державний
університет

ЗАЩИТА ОТ ВЗЛОМА

Предложения взлома можно встретить абсолютно разные, но чаще всего целью является почту или профиль в социальной сети.

Зачастую причиной взлома становится оставленное владельцем аккаунта слабое место в безопасности.

При попытки взлома аккаунта в социальной сети сначала пробуют найти почту, к которой страница привязана.

Двухфакторная авторизация - метод защиты при котором для входа требуется дополнительное подтверждение.

Другой метод взлома - фишинг. Это создание копии сайта, цель которой - заставить пользователя ввести секретные данные на странице взломщике.

Помимо двух приведённых способов, которые считаются классикой взлома, есть менее очевидные и более сложные методы. Один из таких методов - угон сим карты.

Один из самых специфических методов - взлом ресурса.

В сети периодически появляются предложения взлома, причём взломщик заявляет, будто бы способен взломать чуть ли не всё, что угодно.

А как хакеры набирают базы взломанных аккаунтов? Брутфор

Часто в даркнете или на форумах по программированию и взлому можно найти предложения по взлому чужой страницы за деньги. Многим из нас хочется приоткрыть завесу тайны и узнать о ком-то больше, чем он о себе публично пишет. Предложения взлома можно встретить абсолютно разные, но чаще всего целью является почту или профиль в социальной сети. Сегодня мы поговорим о том, настолько возможен взлом аккаунта в крупных социальных сетях или почтовых сервисах и о том, как это делается на практике.

Периодически в новостях говорят о взломах аккаунтов высокопоставленных лиц, поэтому создаётся впечатление, что хакеры способны взломать чуть ли ни что угодно, было бы желание. Ведь важные аккаунты, само собой, защищают надёжными паролями, а уж если это получилось взломать, то у аккаунта обычного пользователя просто нет шансов, но на самом деле у хакеров нет универсального инструмента, который мог бы открыть для них доступ к любому аккаунту. Более того, зачастую причиной взлома становится оставленное владельцем аккаунта слабое место в безопасности. Для примера приведу нашумевший взлом twittera известного политика. Причиной стал не взлом самого пароля от аккаунта, а хакеры

изначально получили доступ к iCloud, где в заметках он хранил свой сложный пароль. Это очень частое явление, когда для взлома происходит не напрямую самого аккаунта, а сначала взламывается менее защищенное звено в цепочке.

При попытки взлома аккаунта в социальной сети сначала пробуют найти почту, к которой страница привязана. Почта зачастую защищена намного хуже. Причина в том, что, если почту не привязать к другой почте или мобильному телефону, то применяется метод восстановления по ответам на секретные вопросы. В некоторых случаях можно с лёгкостью угадать ответ, а если это сделать не получается, всегда можно с помощью социальной инженерии выведать у жертвы необходимую информацию. Давайте сразу упомяну методы защиты от этой стратегии взлома: 1) держим в секрете почту, к которой привязан аккаунт; 2) используем надёжные методы защиты всех связанных аккаунтов 3) пользуемся двухфакторной авторизацией. Двухфакторная авторизация(двухфакторка) - метод защиты при котором для входа требуется дополнительное подтверждение. Этом может быть, например, смс со временным кодом или письмо на почту со ссылкой.

Другой метод взлома - фишинг. Это создание копии сайта, цель которой - заставить пользователя ввести секретные данные на странице взломщике. Поскольку фишинг сайт делается максимально похожим на оригинальную страницу, неопытная жертва с легкостью введёт все необходимые данные без всяких сомнений. Сейчас браузеры активно борются с этим, но с введением новых возможностей взломщики придумывают всё новые пути заставить жертву обманом ввести свои данные. Недавно глобально разрешили в доменах использовать не только ascii символы, что вызвало новую волну фишинг атак с url визуально неотличимыми от целевого сайта. Сейчас это не так актуально, но надо быть всегда на чеку и проверять, куда отправятся вводимые данные.

Помимо двух приведённых способов, которые считаются классикой взлома, есть менее очевидные и более сложные методы. Один из таких методов - угон сим карты. Привязывание к номеру телефона сейчас считается одним из самых надёжных методов защиты своего аккаунта, но, на самом деле, и его можно обойти. Чтобы получить доступ к сим-карте другого человека её нужно переоформить. Это возможно в случае, если старая карта утеряна. Процесс восстановления зависит от оператора, и зачастую надо каким-либо образом подтвердить, что номер принадлежит вам(а он вам не принадлежит). Если получится убедить в этом сотрудника службы поддержки компании, то симку перевыпустят, и на неё можно сбросить все пароли и т.п. Но зачастую просто используются «святи» и работники сотовых операторов за определенный откат.

Один из самых специфических методов - взлом ресурса. Кода без багов не бывает, даже в тщательно проверяемых банковских системах время от времени обнаруживаются ошибки.

Если найти где-то достаточно серьёзную уязвимость, то можно будет получить чуть ли не всю информацию о пользователе. Обычно целью таких атак выбираются не социальные сети, где польза массного взлома сомнительная, а, например, интернет магазины: при взломе коммерческого сайта похищается клиентская база с данными кредитных карт - очень выгодное занятие. Если от методов выше пользователь может сам защититься, то тут большая часть ответственности лежит на самом сайте. Но надо взять за правило использовать для интернет комерции карты с маленьким балансом, чтобы даже в случае взлома потери были минимальными.

Очевидно, что взлом возможен в теории, но на практике осуществим он далеко не всегда. Если пользователь позаботился о своей безопасности, то взлом его аккаунта - незаурядное дело. Однако в сети периодически появляются предложения взлома, причём взломщик заявляет, будто бы способен взломать чуть ли не всё, что угодно. В случае, если в добавок ко всему этому он работает с предоплатой, то сомнений остаётся не много - хочет по быстрому получить предоплаты с как можно большего числа людей и исчезнуть. При реальном взломе никаких 100% гарантий успеха в этом деле быть не может. Заказывая услуги взлома, необходимо получить все возможные гарантии, что это будет действительная добросовестная попытка взлома. Само собой, с теми, кто берёт предоплату, надо быть в двойне осторожней.

А как хакеры набирают базы взломанных аккаунтов: в большинстве случаев используются методы массового взлома. При таком подходе нацеливаются на самые слабозащищенные аккаунты. В самом простом случае это перебор всевозможных логинов со словарём самых часто используемых паролей, по другому - брутфорс. Так же большие базы получаются в результате утечек после взлома.

САХНО О. С., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольський державний
університет

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.Основні принципи захисту інформації

Захист інформації повинна бути заснована на системному підході. Системний підхід полягає в тому, що всі кошти, які використовуються для забезпечення інформаційної безпеки повинні розглядатися як єдиний комплекс взаємопов'язаних заходів. Одним із принципів захисту інформації є принцип «розумної достатності», який полягає в наступному: стовідсоткового захисту не існує ні в якому разі, тому прагнути коштує не до теоретично

максимально досяжному рівню захисту інформації, а до мінімально необхідного в даних конкретних умовах і при даному рівні можливої загрози.

Захист інформації можна умовно розділити на захист: від втрати і руйнування; від несанкціонованого доступу.

2. Захист інформації від втрати і руйнування

Втрата інформації може статися з таких причин:порушення роботи комп'ютера; відключення або збої харчування; пошкодження носіїв інформації; помилкові дії користувачів; дію комп'ютерних вірусів; несанкціоновані умисні дії інших осіб.

Запобігти зазначені причини можна резервуванням даних, тобто створенням їх резервних копій. До засобів резервування відносяться: програмні засоби для створення резервних копій, що входять до складу більшості операційних систем. Наприклад, MS Backup, Norton Backup; створення архівів на зовнішніх носіях інформації. У разі втрати інформація може бути відновлена. Але це можливо тільки в тому випадку, якщо: після видалення файлу на місце, що звільнилося місце не була записана нова інформація; якщо файл не був фрагментований, тобто (Тому треба регулярно виконувати операцію дефрагментації за допомогою, наприклад, службової програми «Дефрагментація диска», що входить до складу операційної системи Windows).

Відновлення проводиться наступними програмними засобами:

Undelete з пакету службових програм DOS; Unerase з комплекту службових програм Norton Utilites.

Велику загрозу для збереження даних представляють порушення в системі подачі електроживлення - відключення напруги, сплески і падіння напруги і т.п. Практично повністю уникнути втрат інформації в таких випадках можна, застосовуючи джерела безперебійного живлення. Вони забезпечують нормальне функціонування комп'ютера навіть при відключенні напруги за рахунок переходу на живлення від акумуляторних батарей.

3.Захист інформації від несанкціонованого доступу

Несанкціонований доступ - це читання, зміна або руйнування інформації за відсутності на це відповідних повноважень.

Основні типові шляхи несанкціонованого отримання інформації: розкрадання носіїв інформації; копіювання носіїв інформації з подоланням заходів захисту; маскування під зареєстрованого користувача; перехоплення електронних випромінювань.

Для захисту інформації від несанкціонованого доступу застосовуються: Організаційні заходи, технічні засоби, програмні засоби,

-- Організаційні заходи включають в себе: пропускний режим; зберігання носіїв і пристроїв в сейфі (дискети, монітор, клавіатура); обмеження доступу осіб в комп'ютерні приміщення.

-- Технічні засоби включають в себе різні апаратні засоби захисту інформації: фільтри, екрани на апаратуру; ключ для блокування клавіатури; пристрою аутентифікації - для читання відбитків пальців, форми руки, райдужної оболонки ока, швидкості і прийомів друку і т.п.

-- Програмні засоби захисту інформації полягають в розробці спеціального програмного забезпечення, яке б не дозволяло сторонній людині отримувати інформацію з системи. Програмні засоби включають в себе: парольний доступ; блокування екрану і клавіатури з допомогою комбінації клавіш; використання коштів парольного захисту BIOS (basic input-output system - базова система введення-виведення).

Захист від читання здійснюється: на рівні DOS введенням для файлу атрибутів Hidden (прихований); шифруванням. Захист то записи здійснюється: установкою для файлів властивості Read Only (тільки для читання); забороною записи на дискету шляхом пересування або виламування важеля; забороною записи через установку BIOS - «дисковод не встановлено»

При захисті інформації часто виникає проблема надійного знищення даних, яка обумовлена наступними причинами: при видаленні інформація не стирається повністю; навіть після форматування дискети або диска дані можна відновити за допомогою спеціальних засобів за залишковим магнітному полю. Для надійного видалення використовують спеціальні службові програми, які стирають дані шляхом багаторазового запису на місце видаляються випадкової послідовності нулів і одиниць.

4.Захист інформації в мережі INTERNET

При роботі в Інтернеті слід мати на увазі, що наскільки ресурси Всесвітньої мережі відкриті кожного клієнта, настільки ж і ресурси його комп'ютерної системи можуть бути за певних умов відкриті всім, хто володіє необхідними засобами. Для приватного користувача цей факт не грає особливої ролі, але знати про нього необхідно, щоб не допускати дій, що порушують законодавства тих країн, на території яких розташовані сервери Інтернету. До таких дій відносяться вільні або мимовільні спроби порушити працездатність комп'ютерних систем, спроби злому захищених систем, використання і поширення програм, що порушують працездатність комп'ютерних систем (зокрема, комп'ютерних вірусів). Працюючи у Всесвітній мережі, слід пам'ятати про те, що абсолютно всі дії фіксуються і записуються спеціальними програмними засобами та інформація, як про законних, так і про незаконні дії обов'язково десь накопичується. Таким чином, до обміну інформацією в Інтернеті слід

підходити як до звичайної листуванні з використанням поштових листівок. Інформація вільно циркулює в обидва боки, але в загальному випадку вона доступна всім учасникам інформаційного процесу. Це стосується всіх служб Інтернету, відкритих для масового використання. Однак навіть у звичайній поштового зв'язку поряд з листівками існують і поштові конверти. Використання поштових конвертів при листуванні не означає, що партнерам є, що приховувати. Їх застосування відповідає давно сформованій історичній традиції та усталеним морально-етичним нормам спілкування. Потреба в аналогічних «конвертах» для захисту інформації існує і в Інтернеті. Сьогодні Інтернет є не тільки засобом спілкування і універсальної довідкової системою - в ньому циркулюють договірні і фінансові зобов'язання, необхідність захисту яких як від перегляду, так і від фальсифікації, очевидна. Починаючи з 1999 року INTERNET стає потужним засобом забезпечення роздрібного торгового обороту, а це вимагає захисту даних кредитних карт і інших електронних платіжних засобів. Принципи захисту інформації в Інтернеті спираються на визначення інформації, сформульоване нами в першому розділі цього посібника. Інформація - це продукт взаємодії даних і адекватних їм методів. Якщо в ході комунікаційної процесу дані передаються через відкриті системи (а Інтернет відноситься саме до таких), то виключити доступ до них сторонніх осіб неможливо навіть теоретично. Відповідно, системи захисту зосереджені на другому компоненті інформації - на методах. Їх принцип дії заснований на тому, щоб виключити або, принаймні, ускладнити можливість підбору адекватного методу для перетворення даних в інформацію

СТУЛІКА В. О., ОС «Бакалавр»,
спеціальність «Кібербезпека»,
Маріупольський державний
університет

ТЕОРЕТИЧНИЙ ОГЛЯД СУЧАСНИХ ПОГЛЯДІВ ЩОДО ПИТАННЯ КІБЕРБЕЗПЕКИ

Актуальність. Проблеми кібернетичної безпеки за сучасних умов і для України, і для переважної більшості інших держав світу стають особливо актуальними. Формування та розвиток інформаційного суспільства базується, як відомо, на синтезі двох технологій - комп'ютерної і телекомунікаційної, та визначається двома простими, але дуже змістовними висловлюваннями: гарантоване зростання швидкості обчислень і об'ємів інформації, що при цьому обробляється; формування на рубежі тисячоліть так званих інформаційного і кібернетичного просторів й виникнення нових, специфічних за формою і способами взаємовідносин їх суб'єктів та об'єктів; основу сучасного інформаційного суспільства

становлять мережі різного функціонального призначення, сукупність та взаємозв'язок яких інформаційний та кіберпростори, які її власне, і утворюють [3].

Виклад матеріалу. Під інформаційним простором розуміють глобальне інформаційне середовище, яке у реальному масштабі часу забезпечує комплексну обробку відомостей про конфліктуючі сторони та їх оточення з метою підтримки прийняття рішень зі створення оптимального для досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах обстановки [1].

Під кіберпростором розуміють комунікаційне середовище, утворене системою зв'язків між об'єктами інформаційної інфраструктури (інформаційними ресурсами, системами і мережами усіх форм власності), що керуються автоматизованими системами управління (АСУ) й використовуються як для передавання інформації, яка в них циркулює, так й для впливу на аналогічні об'єкти протилежної сторони [1].

Розглядаючи кіберпростір як основну високорозвинену модель об’єктивної реальності й враховуючи його сучасні найбільш відмінні ознаки і характерні риси, можна стверджувати, що останнім часом саме він усе частіше використовується протиборчими сторонами для проведення певних, заздалегідь спланованих деструктивних дій.

Про важливість кіберпростору свідчить поява концепцій ведення боротьби у ньому - комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на ІТС супротивника й використовувані ним ІКТ й захисту від такого впливу власних систем і технологій, а також створення у збройних силах ряду країн світу спеціальних структур, призначених для ведення такої боротьби. Такий стан справ, а також глибинні зміни стосовно більшості держав земної кулі до внутрішньої **кібербезпеки** (стану захище ності їх кіберпростору в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується сталий розвиток цих країн, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз їх особистим, корпоративним та/або національним інтересам) й формування, як наслідок, потужних транснаціональних злочинних груп, що спеціалізуються на злочинах у кіберпросторі

З метою уникнення багатозначності у трактуванні термінів **«кіберзлочин»** (фактично неприховані кримінальні дії, що здійснюються з використанням засобів електронно-обчислювальної техніки, і за які передбачається юридична відповідальність) і **"кіберзагроза"** (прояв дестабілізуючого негативного впливу на певний об'єкт, що реалізується за рахунок використаним технологічних можливостей кіберпростору й створює небезпеку як для нього самого, так й для свідомості людини в у цілому) інструктивні матеріали Інтерполу рекомендують поділяти їх на такі групи:

- власне комп'ютерні злочини (порушення авторських прав на програмне забезпечення, розкрадання даних, порушення роботи обчислювальних систем, розкрадання комп'ютерного часу тощо),
- злочини, "пов'язані з комп'ютерами" (головним чином, фінансове шахрайство),
- мережні злочини (використання мереж для здійснення незаконних угод). Найбільший же інтерес із позицій класифікації кібернетичних злочинів і загроз нині становить схема, запропонована Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю [3]. У ній ідеться про чотири можливі групи таких протиправних діянь, а саме:

1) злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем, що реалізуються через несанкціонований доступ в інформаційне середовище, незаконне втручання в дані та/або їх перехоплення, незаконне використання комп'ютерного й телекомунікаційного встаткування або його повне вилучення тощо;

2) злочини, пов'язані з використанням комп'ютерів які передовсім полягають у підробці документів та/або шахрайстві із застосуванням засобів ЕОТ;

3) злочини, пов'язані з розміщенням у мережах протиправної інформації, наприклад, поширенням дитячої порнографії;

4) злочини відносно авторських і суміжних прав [2].

Висновки. Тож, формування й ефективна реалізація кібербезпекової політики, в рамках якої розробляється комплекс заходів щодо прогнозування та протидії кіберзагрозам, є необхідною умовою розвитку суспільства.

Список використаних джерел

1. Гнатюк С. О. Теоретичні основи побудови та функціонування систем управління інцидентами інформаційної безпеки / Гнатюк С. О., Хохлачова Ю. Є., Охріменко А. О., Гребенькова А. К. // Захист інформації. — №1 (54). — 2012. — С. 121-126.
2. Старостина Е. Кибертерроризм – подход к проблеме / Е. Старостина [Електронний ресурс]. - Режим доступу : http ://www.crimeresearch.ru.
3. Сопілко І.В. Інформаційні загрози та безпека сучасного українського суспільства / І.В. Сопілко [Електронний ресурс]. – Режим доступу: http://jrnl.nau.edu.ua/index.php/UV/article/viewFile/8181/9770.

ХЛЮСТОВ С. Я., ОС «Бакалавр»,
спеціальність «Кібербезпека»,
Маріупольський державний
університет

ЗАХИСТ КІБЕРПРОСТОРУ ЯК НАПРЯМ МІЖНАРОДНОЇ ПОЛІТИКИ

Розвиток інформаційних технологій полегшує процес міжнародного відносин. Однак деякі досягнення в інформаційній сфері можуть перешкоджувати забезпеченню інформаційної безпеки і стабільності у кібермережах. Інформація стає фактором, який може призвести до значних технологічних аварій, військових конфліктів, порушити ділову активність та сприяти збоям системи, дезорганізувати державне управління, фінансову систему, роботу наукових центрів.

Все це ознаки того, наскільки сучасне суспільство залежить від стабільного функціонування інформаційних систем. Широке використання інформаційно-комунікаційних технологій призводить до формування абсолютно нових викликів. Саме тому інформаційна безпека розглядається як стратегічна проблема як державного, так і міжнародного рівня. Крім того вона зачіпає всі сфери суспільного життя.

У стратегії інформаційної безпеки висувається ряд державних цілей і пріоритетів, яких необхідно досягти за відповідний проміжок часу. Фактично, стратегія являє собою модель вирішення задачі інформаційної безпеки у державі. Для її реалізації приватний і державний сектори повинні тісно співпрацювати. Співпраця має здійснюватися шляхом обміну інформацією та новітніми досягненнями.

Перша країна, яка почала сприймати інформаційну безпеку, як питання державної важливості були США. У 2003 році тут опублікували Національну стратегію безпеки у кіберпросторі. Цей документ був частиною більш загальної Стратегії забезпечення національної безпеки, створеної у відповідь на терористичні атаки 11 вересня 2001 року.

Україна почала надавати значення кібербезпеці у 2002 році, коли у Міністерстві внутрішніх справ України було створено підрозділи з протидії високотехнологічним злочинам. Про участь військових у боротьбі з кіберзагрозами викладено у «Бюлетені Стратегічної оборони України до 2015 року». Також Україна є учасником робочої групи НАТО з питань кібер та воєнної реформи . Незважаючи на це, в Україні не існує відповідного документа щодо кібербезпеки, що, на мій погляд, призводить до її нездатності протистояти сучасним викликам національній безпеці, пов'язаних із застосуванням інформаційних технологій в умовах глобалізації, в першу чергу кіберзагрозам. Про це йдеться і в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України ». Крім того, нездатність

протистояти кіберзагрозам пов'язано не лише з відсутністю стратегії, але і з помітними відмінностями у розумінні «інформаційної безпеки» як такої.

Відмінність у поглядах на інформаційну безпеку залежить від того, яким чином уряди різних країн дивляться на неї. Кожна держава розглядає глобальні проблеми крізь призму своїх національних інтересів і цінностей.

Наприклад, політика українського уряду щодо інформаційної безпеки зосереджена на пріоритетах, які помітно відрізняються від пріоритетів США і Європи. Американці і європейці під інформаційною безпекою та інформаційним простором розуміють спочатку технологічний аспект. В Україні, так само як і в Росії, під «інформаційною безпекою» та «інформаційним простором» застосовують більш широкі філософські і політичні значення. Технологічна сторона цього питання є лише одним з багатьох компонентів в розумінні Україною інформаційної безпеки. Крім того, ця проблема не є для неї найпріоритетнішою. У «Доктрині інформаційної безпеки України» згадується лише поняття «кіберзлочинність» і «комп'ютерний тероризм», однак відсутні визначення цим термінам у преамбулі. Головними цілями для України в інформаційній сфері є захист національної свідомості і культури, а також забезпечення вільного інформаційного потоку.

Загальне, більш координоване розуміння проблеми і формулювання самого поняття «інформаційної безпеки» допомогло б урядам різних держав легше спілкуватися щодо загроз їхнім мережам, полегшило б співпрацю у відповідь на ці загрози, а також зменшило перспективи їх розвитку у відповідь на кризові ситуації. В першу чергу, цього можна досягти шляхом створення відповідного законодавства в інформаційній сфері, що вимагає певного часу і фінансових витрат.

Список використаних джерел

1. National Strategy for homeland security, Office of Homeland security – July 2002: http://www.ncs.gov/library/policy_docs/nat_strat_hls.pdf

2. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space - June 2009: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

3. Управління боротьби з кіберзлочінністю:

4. http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754

5. NATO and Ukrainian experts discuss cyber defense: http://www.nato.int/cps/en/SID-715E9908-10592FDC/natolive/news_61562.htm,

6. Указ Президента України «Про Рішення Ради національної безпеки й оборони України» № 389/2012 від 8 червня 2012 року «Про нову редакцію стратегії національної безпеки України»: http://www.rnbo.gov.ua/documents/303.html

7. Доктрина інформаційної безпеки України № 514/2009 від 8 липня 2009 року: http://zakon2.rada.gov.ua/laws/show/514/2009

ХОЦЬКИЙ А. Є., ОС «Бакалавр»,
спеціальність «Системний аналіз»,
Маріупольський державний
університет

КІБЕРБЕЗПЕКА ТА ЇЇ РОЛЬ У ЗАХИСТІ КРАЇНИ

Інформаційна кібербезпека України як ключовий фактор протидії зовнішньої агресії. Одна зі складових цієї агресії - це кібератаки. Особливість кіберпростору – відсутність кордонів. Нарощування сегмента кіберзахисту не тільки допоможе відбити агресію, але і в майбутньому забезпечить приплив доходів з-за кордону.

Якщо середньостатистичний громадянин постійно спілкується в «Одноклассниках» і «Вконтакте», використовує російські поштові сервери та антивірусні програми, тримає рахунки в російських банках, платить через Webmoney і Яндекс.Деньги – це створює широкі можливості для впливу на нього.

Кілька країн прийняли рішення про співпрацю з Україною в сфері інформаційної безпеки, з подібними ініціативами виступили США, Канада, Чилі і Туреччина. Іноземні ІТ-фахівці допоможуть Україні протистояти кіберзагрозам. За словами міністра оборони України Степана Полторака, Київ занепокоївся проблемою інформаційного захисту «з огляду на те, що за останні три роки Російська Федерація здійснила понад семи тисяч кібератак на Україну» [1].

Так, в конгрес США 10 травня 2017 року внесений законопроект, згідно з яким американці допоможуть урядовим органам України захистити свої інформаційні системи від злому. «Надати Україні таку підтримку, яка може знадобитися для підвищення рівня безпеки комп'ютерних систем органів державної влади, особливо відповідальних за критично важливу інфраструктуру країни», - йдеться в законопроекті.

Консультуватимуть українських хакерів будуть і фахівці турецької державної корпорації HAVELSAN, яка займається розробкою інформаційних розвідувальних систем і систем ІТ-управління [1].

«Кілька років тому в Туреччині нами був створений найсучасніший центр кібербезпеки. В рамках українсько-турецького співробітництва ми готові надавати консультації щодо створення ще більш якісного проекту в сфері інформаційної безпеки », – заявив директор з кібербезпеки турецької компанії HAVELSAN.

Україна володіє потужним потенціалом, щоб вибудувати надійний захист в кіберсфері і створити «кібервойска».

Україна може скористатися досвідом Польщі, яка в силу подібних зовнішньополітичних проблем вважається однією з найбільш уразливих держав для кібервплив. Поляки вкладають зусилля, щоб виправити ситуацію. У той же час Ізраїль інвестує в галузь кіберзахисту і кібероборони близько 20% від усіх світових витрат [2].

Зараз НАТО створює з Україною єдиний центр з кібербезпеки. Реалізацією проекту буде здійснювати державний концерн «Укроборонпром», що об'єднує велику частину підприємств оборонно-промислового комплексу країни. Як повідомляють в концерні, Київ «звертає особливу увагу на кібербезпека, роблячи все можливе для залучення міжнародного досвіду в цій галузі на Україні».

Зокрема, українські фахівці об'єднаються з експертами Північноатлантичного альянсу для створення нових систем інформаційного захисту та розвитку IT-технологій.

«На Україні є фахівці високого рівня, і зараз ключовою метою є їх об'єднання заради створення надпотужного центру з кібербезпеки. Роботу необхідно почати на умовах співпраці, і ми відкриті для конструктивних пропозицій», - зазначив заступник генерального директора «Укрінмаш» Дмитро Будорін [3].

Наприклад, для Харкова в цьому плані відкриваються можливості, оскільки в місті знаходиться серйозний IT-кластер: потужна навчальна і наукова база, а також конкурентний IT-бізнес. Головні споживачі послуг українських програмістів – це США (25%) і Ізраїль (17,8%) [3].

Отже, Україна намагається добитися успіху в кіберзахисті, але без великих фенансових вкладень це буде важко здійсненне завдання. Я вважаю, що нарощування сегмента кіберзахисту не тільки допоможе відбити агресію, але і в майбутньому забезпечить приплив доходів з-за кордону.

Список використаних джерел

1. Юлія Гуреваі «Рада прийняла закон про кібербезпеки України» [Електронний ресурс]. – Режим доступа: https://www.unian.net/politics/2171886-poroshenko-vnes-v-vr-dorabotannyiy-zakonoproekt-o-prodlenii-osobogo-statusa-ordlo.html

2. Діана Овсепяник «Кіберпрікритіе: інформаційною безпекою України займуться США, Чилі, Канада і Туреччина» [Електронний ресурс]. – Режим доступа: https://russian.rt.com/world/article/387917-ukraina-kiberbezopasnost-ssha-nato-turciia

3. Кібербезпека і кібероборона: поточна ситуація і завдання для України [Електронний ресурс]. – Режим доступа: http://sprotyv.info/ru/news/harkov/kiberbezopasnost-i-kiberoborona-tekushchaya-situaciya-i-zadachi-dlya-ukrainy

ХРИПКОВА А. Р., ОС «Бакалавр»,
спеціальність «Кібербезпека»,
Маріупольський державний
університет

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ

Інтернет - глобальна комп'ютерна мережа, що охоплює весь світ. Сьогодні Інтернет має близько 15 мільйонів абонентів у більш ніж 150 країнах світу. І майже вся важлива інформація цих абонентів, починаючи з особистих фотографій, творів мистецтва, даних про здоров'я людини і закінчуючи фінансами та документацією, зберігається в електронному вигляді. Чим більше розвиваються електронні технології, тим більше людей бачать переваги саме в такому зберіганні, і, отже, з'являється більше способів викрасти цю інформацію.

На жаль, далеко не кожен із нас встиг усвідомити всю крихкість стандартної комбінації логін + пароль. І шахраї від цього тільки виграють. З'являються все більш зручні і безпечні способи заволодіти чужою інформацією, залишаючись при цьому непоміченим.

На щастя, сучасні технології освоюють не тільки інтернет-шахраї. Людство дружно шукає найбільш дієвий спосіб захисту даних. І найкраще рішення на сьогоднішній день - це двофакторна аутентифікація або 2FA.

Двофакторна аутентифікація - це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи аутентифікаційних даних. Введення додаткового рівня безпеки забезпечує більш ефективний захист аккаунта від стороннього доступу.

Двофакторна аутентифікація вимагає, щоб користувач мав два типи ідентифікаційних даних:

- Щось, йому відоме;
- Щось, йому наявне.

До першого пункту належать різні паролі, пін-коди, секретні фрази, тобто щось, що користувач запам'ятовує і вводить в систему при запиті.

До другого пункту - введення одноразового пароля, отриманого в СМС, згенерованого за допомогою апаратного токена або мобільного додатка. Токен - це компактний пристрій, який знаходиться у власності користувача. Сьогодні в якості токенов можуть виступати смартфони, тому що вони стали невід'ємною частиною нашого життя. У цьому випадку так званий одноразовий пароль генерується або за допомогою спеціального додатку (наприклад Google Authenticator), або приходить по SMS - це максимально простий і дружній до користувача метод, який деякі експерти оцінюють як менш надійний.

Суть двофакторної аутентифікації полягає в тому, що навіть якщо шахрай зможе дістати ваші логін і пароль, то буде скомпрометований всього лише один фактор, бо

перехоплювати одноразові паролі не має сенсу, адже діють вони дуже недовго, і кожен наступний пароль ніяк не пов'язаний з попереднім. Обчислити закономірність створення такого пароля також неможливо, для цього потрібно знати секретний ключ, який зберігається тільки на сервері і в самому токені.

Виникає питання: наскільки надійна двофакторна аутентифікація? Використовуючи 2FA ви виключаєте досить велику категорію кібератак, але, якщо бути чесними, вона не є непроникною для зловмисників. Проте вона серйозно ускладнює їм життя, бо щоб зламати двофакторну аутентифікацію, доведеться отримати доступ до cookie-файлів або кодів, що згенерували токени.

Методам захисту, заснованим на методиках багатофакторної аутентифікації, сьогодні довіряє велика кількість компаній, серед яких організації зі сфери високих технологій, фінансового і страхового секторів ринку, великі банківські установи та підприємства держсектора, незалежні експертні організації та дослідницькі фірми. Також ось кілька основних сервісів та соціальних мереж, які пропонують цю функцію - це Facebook, Gmail, Twitter, LinkedIn, Steam. Їх розробники пропонують на вибір: SMS-аутентифікацію, список одноразових паролів, Google Authenticator і ін.

Двофакторна аутентифікація не є панацеєю, але вона допомагає серйозно підвищити захищеність акаунта користувача, витративши мінімум зусиль. Ускладнення життя зломщиків - це завжди добре, тому користуватися 2FA можна і потрібно.

Сьогодні 2FA переживає справжній бум, а будь-яку популярну технологію набагато простіше удосконалювати. Незважаючи на наявність складнощів, її чекає світле майбутнє.

Список використаних джерел

1. http://b-online.ru/infobusiness/4080-dvuhfaktornaya-autentifikaciya-vs-avtozaliv-kto-pobedit.html
2. https://habrahabr.ru/company/1cloud/blog/277901/

БАЛЮРА Ю. Ю., ОС «Бакалавр»,
спеціальність «Право»,
Маріупольський державний
університет

ОСНОВНІ СКЛАДОВІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ИНФОРМАЦІЇНОЙ УКРАЇНИ

Система забезпечення інформаційної безпеки України (СЗІБ) створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему

адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Формування СЗІБ має відбуватись за усвідомлення необхідності функціонування механізму балансу інтересів усієї системи державного управління в інформаційній сфері.

Зазначимо, що за роки незалежності в Україні лише закладено основи для формування системи забезпечення інформаційної безпеки. Так, певним чином можна говорити про напрацювання великого масиву нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері. Президентом України вживаються активні заходи щодо вдосконалення системи управління інформаційною сферою. Важливе політико-правове значення мають діючі Укази Президента України "Про деякі заходи щодо глобальної інформаційної мережі Internet та забезпечення широкого доступу

Водночас функціонування даної системи не обмежується лише великим масивом нормативно-правових актів. Відтак ми не можемо констатувати про остаточне створення основних елементів Системи забезпечення інформаційної безпеки. І причин тому є багато. Це і несформованість системи забезпечення національної безпеки, і невизначеність політики національної, а отже і інформаційної безпеки, і відсутність, врешті-решт, доктрини інформаційної безпеки, яка має розвивати положення Концепції національної безпеки, яка в Україні взагалі відсутня. Згодом недосконалість нормативно-правового регулювання даних процесів негативно впливає і на державне управління у даній сфері.

Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України на сьогодні складають: Конституція України, Закон України «Про основи національної безпеки України», інші законодавчі та нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері. Нормативно-правове підґрунтя має досить розвинений характер, оскільки більшість норм відповідають міжнародним стандартам, принципам і нормам забезпечення прав і свобод людини та громадянина, зокрема права на свободу слова, отримання та поширення інформації. Водночас, системні проблеми даються в знаки і при вирішенні галузевих проблем, тому не сформиваність нормативно-правової бази щодо регулювання суспільних відносин в сфері національної безпеки, відповідним чином негативно впливає на можливість формування достатньої і ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері.

У найбільш загальному плані під системою забезпечення інформаційної безпеки будемо розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів,

спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення.

Безперечно, можна довго дискутувати з приводу того чи іншого терміну, можна пропонувати численні варіанти, водночас змістовними вони будуть лише тоді, коли будуть визначені основи формування і функціонування СЗІБ.

Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки. На дану обставину також зазначають і інші дослідники[05].

Вживаючи термін "система", і ми свідомо акцентуємо увагу на цьому, нами робиться логічний наголос на утворенні нової якості, яку складають загрози та небезпеки, суб'єкти забезпечення інформаційної безпеки. Адже структурна зв'язаність елементів системи забезпечення інформаційної безпеки є істотною її якісною характеристикою і розрив зв'язків між цими елементами може призвести до зникнення самої системи, а отже актуалізується питання забезпечення структурної єдності даної системи.

Так, наприклад, захищеність Кабінету Міністрів України і незахищеність місцевої адміністрації міста Києва у своїй сукупності не утворять стан захищеності усієї системи інформаційної безпеки органів державного управління.

Таким чином, суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, вживаючи при цьому відповідні, визначені законом, адміністративно-правові форми та методи. У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють струнку організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки

Список використаних джерел

1. Структура системи забезпечення інформаційної безпеки та компетенція її складових http://pidruchniki.com/10561127/finansi/finansova_sistema_skladovi (дата звернення 16.10.2017).

ГОЛІКОВ В. А., ОС «Бакалавр»,
спеціальність «Право»,
Маріупольський державний
університет

ІНФОРМАЦІЙНО-ТЕХНІЧНА БЕЗПЕКА В УКРАЇНІ

У сучасних умовах на ринках електронного навчання все більшої популярності набувають хмарні обчислення або хмарні технології. Інформаційна безпека (ІБ) – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи зникнення. Це поняття взято з основних понять безпеки інформаційних технологій [1].

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Говорячи про інформаційну безпеку, часто мають на увазі інформаційну безпеку в найзагальнішому сенсі, як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації.

Інформаційна безпека за сферою застосування:

Інформаційна безпека держави — стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому використовується нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності [2].

Інформаційна безпека організації – цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інформаційна безпеки особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Розглянемо суттєві (з позицій ІБ) властивості інформації для забезпечення інформаційно-технічної безпеки.

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується модель CIA:

Конфіденційність- властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем;

Цілісність) - означає неможливість модифікації неавторизованим користувачем;

Доступність- властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час [3].

Опишемо забезпечення ІБ: 1) створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; 2) Підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань; 3) Вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; 4) розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи.

Висновок. Отже, інформаційно-технічна безпека-це заходи, які спрямовані не допускати шкідливих збитків, яких може зазнати будь-яке підприємство чи організація у разі розголошення конфіденційної інформації.

Список використаних джерел

1. Аудит інформаційної безпеки : підручник / В. А. Ромака, А. Е. Лагун, Ю. Р. Гарасим та ін. ; Держ. служба України з надзвич. ситуацій, Львів. держ. ун-т безпеки життєдіяльності, НАН України, Ін-т приклад. проблем механіки і математики ім. Я. С. Підстригача. -Львів : Сполом, 2015. -363 с. : іл.- Бібліогр.: с. 280-281 (37 назв). -ISBN 978-966-919-123-6

2. Інформаційна безпека людини як споживача телекомунікаційних послуг : Монографія / І.В. Арістова, Д.В. Сулацький ; НДІ інформатики і права НАПрН України. -К. : Право України ; Х. : Право, 2013. -184 с.

3. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. -К.: НТУУ «КПІ», 2001-№ 4.

ДРЕСВЯНІКОВА В. Д.,
ОС «Бакалавр», спеціальність
«Право», Маріупольський
державний університет

СПЕЦІАЛЬНЕ ЗАКОНОДАВСТВО У СФЕРІ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ (ЗАКОН «ПРО ІНФОРМАЦІЮ»)

Із розвитком інформаційних технологій в нашому суспільстві назріла потреба у захисту інформації на всіх етапах діяльності людини. Тому в Україні було створено ряд законодавчих актів щодо безпеки інформаційної діяльності.

Інформаційну діяльність та її безпеку регламентує декілька Законів. Перший - "Про інформацію" введений в дію постановою Верховної Ради від 02.10.1992 із подальшими змінами, внесеними згідно із Законами. Другий - Закон "Про Захист інформації"введений в дію Постановою Верховною Радою від 05.07.94. Також 23.02.2006 рішенням Верховної Ради було створено державний орган задля спеціального зв'язку та захисту інформації. [4]

Закон «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Згідно із першою статтею Закону «Про інформацію» : «інформація - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Захист інформації - це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.» [1]

Закон також визначає, що основними принципами інформаційних відносин є: гарантованість права на інформацію, відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації.» [1] (Ст. 2 положення 1)

Основними напрямами державної інформаційної політики відповідно до статті 3 Закону «Про інформацію» є: "забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; забезпечення інформаційної безпеки України." [1]

Згідно із 7 статтею Закону "Про інформацію": "Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації."[1]

Указом Президента України від 07.11.2005 № 1556/2005 «Про додержання прав людини під час проведення оперативно-технічних заходів» визначено необхідність

створення Державної служби спеціального зв'язку та захисту інформації України, як центрального органу виконавчої влади зі спеціальним статусом.

Законом «Про Державну службу спеціального зв’язку та захисту інформації України» від 23.02.2006 рішенням Верховної Ради було створено державний орган виконавчої влади Державну службу спеціального зв'язку та захисту інформації України. Цей Закон відповідно до Конституції України визначає правові основи організації та діяльності Державної служби спеціального зв’язку та захисту інформації України.[2]

Згідно із 2 статтею Закону «Про Державну службу спеціального зв’язку та захисту інформації України» : «Державна служба спеціального зв’язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, а також інших завдань відповідно до закону. Державна служба спеціального зв’язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України». [2]

Основними завданнями Державної служби спеціального зв’язку та захисту інформації України можна визначити: "Формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку;участь у формуванні та реалізації державної політики у сфері електронного документообігу в частині захисту інформації державних органів та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису, крім питань правового регулювання його застосування, в державних органах та органах місцевого самоврядування».[2]

Статтю 3 Закону «Про Державну службу» було доповнено абзацом згідно із Законом №1313-VII від 05.06.2014 : «забезпечення в установленому порядку та в межах компетенції діяльності суб’єктів, які безпосередньо здійснюють боротьбу з тероризмом». Адже в умовах

сучасного світу тероризм є надзвичайно актуальною проблемою, що потребує особливого ставлення зі сторони держави.

Згідно із статтею 11 Закону «Про державну службу спеціального зв’язку та захисту інформації України» : «До особового складу Державної служби спеціального зв’язку та захисту інформації України належать військовослужбовці, державні службовці та інші працівники».[2]

У сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах відносини регулює Закон "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.06.1994 [3] Із змінами, внесеними згідно із Законами (остання від 27.03.2014, ВВР, 2014, N 22, ст.816) Згідно із статтею 9 Закону "Про захист інформації в інформаційно-телекомунікаційних системах" : «Відповідальність за забезпечення захисту інформації в системі покладається на власника системи». [2] Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації виконує такі функції: розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції; визначає вимоги та порядок створення комплексної систем захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації; здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом; здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Згідно із статтею 10 : «Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Таким чином, проаналізувавши нормативно-правові акти щодо захисту інформації в Україні, можна сказати, що законодавство задовольняє потреби громадян у цьому питанні. Адже є декілька законів, що регламентують права і обов'язки суб'єктів цих право відношень.

Проте, на мій погляд, з часом і розвитком технологій у світі та в Україні законодавство буде потребувати деяких змін, удосконалень.

Список використаних джерел:

1. Закон України «Про інформацію» // Офіційний сайт Верховної ради України. - [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/2657-12
2. Закон України «Про державну службу спеціального зв'язку» // Офіційний сайт Верховної ради України. - [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/3475-15
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Офіційний сайт Верховної ради України. - [Електронний ресурс]. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. Офіційний сайт державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. - Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index

КЛИМЕНКО М. С.,
ОС «Бакалавр», спеціальність «Право», Маріупольський державний університет

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ВПЛИВОВИЙ ФАКТОР НА СТАН ПОЛІТИЧНОЇ, ЕКОНОМІЧНОЇ СФЕР ЖИТТЯ ЛЮДИНИ

Інформаційна сфера як системостворюючий фактор життя суспільства, активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України, тому обрана тема є актуальною. Інформаційна сфера охоплює собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збирання, формування, розповсюдження і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин. Інформаційна безпека характеризується рівнем та станом захищеності різних груп інтересів [5].

Загальноприйнятою є думка, що інформаційна безпека є станом захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері . В Україні створена система забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплені в нормативно-правових актах різного рівня – Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів, інших відомчих, нормативних актах.

Основний зміст діяльності по забезпеченню інформаційної безпеки – це захист інтересів, які реалізуються в інформаційній сфері, від загроз зовнішнього та внутрішнього характеру.

Загрози можуть проявлятись у різних видах. Наприклад, за класифікацією Орлова П.:

- неправомірне обмеження органами державної влади та громадськими об'єднаннями конституційних прав та свобод, які реалізуються в інформаційній сфері;

- приховування соціально значущої відкритої інформації;

- використання ЗМІ для обмеження прав людини на вільний вибір переконань;

- пропаганда зразків масової культури, заснованих на культі насильства, таких, що суперечать нормам моралі, прийнятими в Українському суспільстві;

- розголошення відомостей, які складають державну таємницю, та інші таємниці, які охороняються законом, конфіденційну інформацію;

- зловживання свободою масової інформації;

- обмеження законних інтересів людини, які пов'язані з використанням нею результатів своєї інтелектуальної праці;

- протиправне застосування спеціальних засобів впливу на індивідуальну,групову та масову свідомість;

- зруйнування систем накопичення та збереження культурних цінностей,включаючи архівні фонди.

Необхідність забезпечення безпеки є однією з найважливіших соціальних потреб суспільства в цілому і людини зокрема. Будь-які природні чи соціальні явища людина розглядає через призму можливої загрози і можливості забезпечення власної безпеки.

Прогресивний розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови як найповнішого забезпечення належного рівня інформаційної безпеки. Рівень розвитку та безпека інформаційного середовища, які є одними з найвагоміших факторів у всіх сферах державної безпеки, активно впливають на стан політичної, економічної та інших складових державної безпеки України. У зв'язку з цим доцільно розглядати інформаційну безпеку як складову інших сфер державної безпеки.

Серед пріоритетів державних інтересів України в контексті інформаційної безпеки слід зазначити такі:

– гарантування конституційних прав і свобод людини і громадянина;

– розвиток громадянського суспільства, його демократичних інститутів;

– захист державного суверенітету, територіальної цілісності та недоторканності державних кордонів, недопущення втручання у внутрішні справи України;

– зміцнення політичної і соціальної стабільності в суспільстві;

– забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту інших мов національних меншин України.

З основних реальних та потенційних загроз державній безпеці України, стабільності в суспільстві, наведемо ті, які тією чи іншою мірою реалізовуються через інформаційну сферу:

– посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав; спроби втручання у внутрішні справи України з боку інших держав; воєнно-політична нестабільність, регіональні та локальні війни (конфлікти) в різних регіонах світу, насамперед поблизу кордонів України;

– розвідувально-підривна діяльність іноземних спеціальних служб; загроза посягань з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал України, права і свободи громадян; злочинна діяльність проти миру і безпеки людства, насамперед поширення міжнародного тероризму; прояви сепаратизму, намагання автономізації за етнічною ознакою окремих регіонів України;

– недостатня ефективність існуючих структур і механізмів забезпечення міжнародної безпеки та глобальної стабільності; можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами; небезпечне зниження рівня забезпечення військовою та спеціальною технікою та озброєнням нового покоління ЗСУ, інших військових формувань, що загрожує зниженням їх боєготовності;

– порушення з боку органів державної влади та органів місцевого самоврядування Конституції і законів України, прав і свобод людини і громадянина, в тому числі при проведенні виборчих компаній, недостатня ефективність контролю за дотриманням вимог Конституції і виконанням законів України; можливість виникнення конфліктів у сфері міжетнічних і міжконфесійних відносин, радикалізації та проявів сепаратизму в діяльності деяких об’єднань національних меншин та релігійних громад; загроза прояву сепаратизму в окремих регіонах України.

Суттєвим для інформаційної політики будь-якої держави є дотримання балансу інтересів особистості, суспільства і держави. Держава повинна забезпечувати відкритість та проінформованість суспільства про діяльність її органів і суспільних інститутів в інформаційній сфері.

Таким чином, можем зробити висновок, що інформаційна безпека є впливовим фактором на політичне та економічне життя людини, адже вона є складовою безпеки самої людини.

Список використаних джерел:

1. Гуцалюк М. Інформаційна безпека в сучасному суспільстві / М. Гуцалюк // Право України. – 2005. – No 7. – С. 71–74.

2. Комп’ютерна злочинність і інформаційна безпека / А. П. Леонов ; за заг. ред. А. П. Леонова. – Мінськ : АРІЛ, 2000. – 552 с.

3. Лужецький В. А. Інформаційна безпека : навч. посіб. / В. А. Лужецький, О. П. Войнович, А. В. Дудатьєв. – Вінниця : УНІВЕРСУМ-Вінниця, 2009. – 240 с.

4. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия / В. Роговец // Персонал. – 2000. – No 5. – С. 56–69.

5. Орлов П. І. Правове забезпечення інформаційної безпеки / П. І. Орлов // Вісник Харківського національного університету внутрішніх справ. - 2001.

КОНОНОВА К. С.,
ОС «Бакалавр», спеціальність «Право», Маріупольський державний університет

ВИЗНАЧЕННЯ СФЕР НАЦІОНАЛЬНОЇ БЕЗПЕКИ ЗА ЗАКОНОМ УКРАЇНИ «ПРО ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗБЕКИ УКРАЇНИ»

Необхідність національної безпеки існує з давніх часів і актуальна донині, бо регулює такі галузі суспільної діяльності.

Закон України «Про основи національної безпеки України» визначає основні принципи створення державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від загроз в усіх галузях життєдіяльності; []

Національні інтереси - життєво важливі матеріальні і духовні цінності Українського народу, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток;

Воєнна організація держави – сукупність органів державної влади військових формувань, утворених відповідно до законів України, безпосередньо спрямована на захист національних інтересів України від зовнішніх загроз; Правоохоронні органи - органи державної влади, на які Конституцією і законами України покладено здійснення правоохоронних функцій. []

Об'єктами національної безпеки є: конституційні права і свободи людини та громадянина, інтелектуальні та матеріальні цінності суспільства;

Суб'єктами забезпечення національної безпеки є: Президент України, прокуратура України, Рада національної безпеки і оборони України

Основними функціями суб'єктів забезпечення національної безпеки є: стратегії національної безпеки України і здійснення заходів нейтралізації загроз інтересам України;

Контроль за реалізацією заходів здійснюється Президентом України, Кабінетом Міністрів України, Радою національної безпеки і оборони України

Список використаних джерел:

1. Закон України “про основи національної безпеки України” // Офіційний сайт Верховної Ради України – [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/964-15

МИХАЙЛЕНКО І. Ю., ОС «Бакалавр», спеціальність «Право» Маріупольський державний університет

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

У процесі розвитку високих технологій виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережевокомп’ютерної складової. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Кіберпростір став невід’ємною частиною інформаційного простору та п’ятою сферою ведення збройної боротьби. Сама збройна боротьба, завдяки інформаційному чиннику, набула високого ступеня керованості. Деякі країни, з метою захисту свого кіберпростору, почали просування проектів регулювання (правил поведінки) у кіберпросторі.

Система національної безпеки будь-якої країни базується на концептуальних нормативно-правових документах, у яких викладаються офіційні погляди на роль і місце держави у світі, її національні цінності, інтереси й цілі, способи й засоби запобігання зовнішнім і внутрішнім небезпекам і загрозам. Українська держава прагне до забезпечення кібербезпеки на національному рівні, відповідно до стандартів країн-членів ЄС (з метою пришвидшення подальшого вступу). Кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп’ютерного захисту. Діяльність із формування системи забезпечення національної безпеки України була невід’ємною складовою і чинником державотворчих процесів із початку виникнення незалежної України. Доказом цього є прийняття ряду нормативно-правових актів, щодо регулювання кібербезпеки України.

16 березня 2016 року Президент України Петро Порошенко підписав Указ, яким увів в дію рішення Ради національної безпеки і оборони України від 27 січня "Про Стратегію кібербезпеки України". В документі наголошується, що разом з перевагами сучасного цифрового світу та розвитком інформаційних технологій, нині активно розповсюджуються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Стратегія передбачає комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягнення сумісності з відповідними стандартами ЄС та НАТО; формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту; залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпечного поводження в кіберпросторі; розвиток міжнародного співробітництва та підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співпраці України з ЄС та НАТО.

Відповідно до статті 107 Конституції України, частини другої статті 2 Закону України «Про основи національної безпеки України» було прийнято рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Питання кібербезпеки держави регулюється також Кримінальним Кодексом України (ККУ).

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп’ютерного захисту.

Список використаних джерел:

1. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». − [Електронний ресурс]. − Режим доступу: http://www.president.gov.ua/documents/472017-21374

2. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"». − [Електронний ресурс]. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016

3. Ліпкан В. А. Поняття системи забезпечення національної безпеки України / В. А. Ліпкан // Право і Безпека. — 2003.

4. Закон України "Про основи національної безпеки України" від 19 червня 2003 року. − [Електронний ресурс]. − Режим доступу: http://zakon3.rada.gov.ua/laws/show/964-15

ХОЛОД К. В., ОС «Бакалавр»,
спеціальність «Право»,
Маріупольский державний
університет

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Однією з головних проблем процесу інформатизації є хакерські атаки на інформаційні системи, які наносять прямі матеріальні збитки не тільки розробникам інформаційних технологій, але й їхнім користувачам. Недотримання режиму захисту від несанкціонованого доступу може призвести до небажаного запозичення інформації, а недотримання режиму захисту від вірусів – до виходу з ладу важливих систем і знищення результатів багатоденної роботи. У частих хакерських атаках та неспроможності багатьох організацій самостійно забезпечувати захист інформації й полягає актуальність даної теми.

Проблема теоретико-правових засад забезпечення інформаційної безпеки у вітчизняній науковій літературі розглядалася лише через висвітлення окремих її аспектів вітчизняними та зарубіжними фахівцями. У даному контексті слід згадати наукові розробки таких вчених, як В. Артемов, В. Гурковський, О.Логінов,

З точки зору теорії гіперсистем права, провідна системна проблема інформаційної безпеки як процесу інформаційної діяльності — це підтримка (збереження, охорона і захист) суспільних інформаційних відносин від негативних впливів (загроз інтересам суб'єктів суспільних відносин): соціальних (соціогенних, антропогенних, у їх складі криміногенних), техногенних та природних (стихійних).

Захист інформації з обмеженим доступом є одним з першочергових завдань забезпечення інформаційної безпеки. Однак його ефективна реалізація, принаймні на правовому рівні, значно ускладняється відсутністю єдиного розуміння понять «інформація з обмеженим доступом», «конфіденційна інформація», «таємна інформація». Оскільки положення з цього приводу містяться переважно в актах неінформаційного характеру і є доволі суперечливими, для з'ясування суті вищезазначених термінів слід проаналізувати зміст відповідних правових норм.

Згідно ст. 30 «Інформація з обмеженим доступом» Закону України «Про інформацію» [6], інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну (конфіденційна - це більш вдалий і широко вживаний термін) і таємну.

Конфіденціальна (конфіденційна) інформація - це, відповідно до Закону, відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов. Громадяни,

юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї систем (способів) захисту. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої є загрозою для життя і здоров'я людей. До таємної належить інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Ч. 2 ст. 30 Закону України «Про інформацію», перераховуючи повноваження, суб'єкт яких може визначати режим доступу до інформації, містить сполучник «або», який вказує на те, що інформація може вважатися конфіденційною не тільки з волі власника (право власності передбачає право володіння, користування та розпорядження), а й з волі особи, якій належить окреме повноваження щодо інформації. Ч. 3 ст. 30. Інформація може бути предметом певного інтересу для будь-якої особи. Цей інтерес може бути і негативним, тобто мати протиправну спрямованість. Протиправний характер інтересу не виключає можливості придбання особою інформації на власні кошти.

Таким чином, ч. 3 ст. 30 також не передбачає умовою для встановлення режиму доступу до інформації законність права власності або делегованих власником повноважень. Закон охороняє як таємну, так і конфіденційну інформацію, тому неможливо говорити про захист першої за допомогою закону, а іншої - засобами власника. Разом з тим слід зазначити, що суб'єкти встановлення режиму обмеженого доступу для цих категорій інформації є різними. Належність інформації до категорії конфіденційної встановлюють фізичні та юридичні особи з метою захисту власних інтересів (ця інформація за загальним правилом є відкритою, і може такою залишатися, але фізичним та юридичним особам в межах їх компетенції надано право обмежувати доступ до такої інформації), а належність інформації до категорії таємної - держава в публічних інтересах. Для визнання інформації конфіденційною необхідно мати певне право на таку інформацію. Держава ж, визнаючи інформацію таємною, керується своїми повноваженнями щодо захисту публічних інтересів, а не правом на інформацію. Звісно, можна зазначити, що встановлення в законі можливості віднесення інформації до категорії конфіденційної також захищає публічні інтереси, тобто всіх, а не окремої особи. Однак норми щодо віднесення інформації до категорії конфіденційної є диспозитивними (особа може, але не зобов'язана відносити інформацію до

категорії конфіденційної навіть тоді, коли в законі зазначений характер відомостей - комерційні або ін.), що ж стосується віднесення інформації до категорії таємної, тут мають місце імперативні норми - держава наказує визнавати таємною інформацію певного характеру. Різним є також момент отримання інформацією рівня захисту згідно режиму обмеженого доступу: таємною інформація визнається з моменту свого виникнення (якщо її визнання таємною вимагає закон), конфіденційною ж – з моменту відповідного рішення власника

Віднесення інформації до категорії конфіденційної є реалізацією повноважень власника, тобто права власності як абсолютного (ніхто не повинен посягати на власність незалежно від того, чи вжив власник заходів щодо її збереження, а їх вжиття в межах абсолютного права не порушує і не обмежує прав інших осіб). У той же час визнання інформації таємною являє собою безпосереднє виключення з права на інформацію, передбаченого чинним Законом та Конституцією

Таким чином законодавство України з питань комп'ютерних злочинів має відповідати тенденціям розвитку законодавств Західної Європи, законопроектній діяльності в цьому регіоні та принципам систематизації кримінального законодавства в континентальній правовій системі. їх використання дозволить: створити в Україні ефективну нормативно-правову базу для боротьби з комп'ютерними злочинами; проводити роботу щодо гармонізації українського законодавства з законодавством зарубіжних країн, що з огляду на тенденції інтернаціоналізації комп'ютерної злочинності видається актуальним завданням.

Список використаних джерел

1. Блінов «Информаційна безпека» Учбовий посібник Частина 1 – СПб.: Видавництво СПбГУЭФ, 2010. – 96 с.

2.Азаров Д. «Порушення роботи автоматизованих систем - злочини у сфері комп'ютерної інформації» Право України. - № 12. - 2000. - С. 72.

4. Біленчук П.Д., Зубань М.А. «Комп'ютерні злочини: соціально- правові та кримінолого-криміналістичні аспекта: Навчальний посібник.» - К.: Українська академія внутрішніх справ, 1994. - С. 6.

5. Шилан Н.Н., Кривоніс Ю.М., Бірюков Г. М. «Компьютерные преступления и проблемы защиты информации: Монография - Луганск: РИО ЛИВД, 1999. - С. 9.

6. Стаття 30. Інформація з Закону України «Про інформацію». URL: http://www.uapravo.com/hro/text.php?lan=ukr&id=13307&id_book=13274&id_parent=13274 (дата звернення 16.10.2017)

ШАГАБУДІНОВ Д. А.,
ОС «Бакалавр», спеціальність
«Право», Маріупольський
державний університет

ЗАКОНОДАВСТВО В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Актуальність цієї теми обумовлена інтенсивним зростанням різних джерел масової інформації та потребою у відповідному врегулюванні цих джерел, щоб уникнути можливих казусів і конфліктів.

Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз [2].

Завдання інформаційної безпеки - створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками, виступають цілеспрямованість, масштабність та комплексність дій тощо [3].

Проблематика інформаційної безпеки є актуальною в теорії та практиці багатьох галузей права, зокрема й в адміністративному праві. Це зумовлено усвідомленням ролі інформації як суспільного ресурсу, поряд із речами та енергією. Сучасні інформаційні технології, зокрема технології електронної телекомунікації, створюють нові можливості державного управління. Однак вони мають і зворотний бік – масове маніпулювання суспільством, громадською думкою для загострення соціальних конфліктів тощо. Очевидно, що суспільні відносини щодо інформації потребують не лише приватноправового, але і публічноправового регулювання для їх охорони, захисту тощо в контексті прав людини [1].

Під час створення сучасної та ефективної системи забезпечення інформаційної безпеки істотного значення набуває наявність відповідної нормативно-правової бази, без якої неможливо охопити усі сфери життєдіяльності суспільства в рамках єдиного правового поля, розробити загальнонаціональну концепцію розвитку держави й ефективно реалізовувати політику національної безпеки в інформаційній сфері. Це означає, що всі без винятку дії щодо захисту й реалізації національних інтересів України в будь-якій сфері й на будь-якому рівні мають передусім спиратися на чинне законодавство України, підтверджувати законність функціонування системи національної безпеки. Водночас у демократичному суспільстві такі дії суб'єктів забезпечення національної безпеки повинні відповідати

національному законодавству, а також загальновизнаним міжнародно-правовим нормам та бути під контролем громадськості [5].

Найбільш актуальним завданням у сфері забезпечення інформаційної безпеки держави на сьогодні є формування відповідних положень національного інформаційного законодавства щодо правового забезпечення діяльності в інформаційній сфері відповідних суб'єктів, у першу чергу державних органів, на які державою покладено виконання пов'язаних з цим функцій [5].

Неповноцінність у системі органів державного управління кількісного складу юристів, які спеціалізуються на інформаційному праві, зумовлює недостатність забезпечення обсягу вироблення конкурентоспроможного в глобальному інформаційному просторі національного інформаційного продукту. У цьому сенсі інформаційна безпека конвертується в економічну. Через неналежний рівень підготовки юристів у більшості вищих навчальних закладах щодо інформаційного права, правової інформатики, правового регулювання інформаційної безпеки наближається до критичного стан застосування інформаційно-комп'ютерних систем у галузі державного управління, внутрішніх і міжнародних комунікацій [4].

Ураховуючи різноманіття проблем, досліджених в юридичній науці, слід зазначити, що аспект інформаційної безпеки в умовах глобалізації інформаційного простору ставить завданням вироблення теоретико-правових, методологічних, концептуальних, доктринальних, стратегічних, тактичних та оперативних правових засобів, здатних урегулювати суспільні інформаційні відносини, що здійснюються у взаємозв'язку з міжнародними правовими процесами гармонізації законодавства про інформаційну безпеку як підгалузь законодавства про інформацію.

Список використаних джерел

1. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481.

2. Боднар І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія / І. Р. Боднар. – Львів: Видавництво Львівської комерційної академії, 2013. – 320 с.

3. Інформаційна безпека сучасної держави: концептуальні роздуми URL: http://www.crime-research. iatp. org. ua/ library/strateg. htm (дата звернення 16.10.2017)

4. Економіка та організація інформаційного бізнесу - Навчальний посібник (Лазарєва С. Ф.)

5. Нормативно-правове регулювання інформаційної безпеки України URL: http://westudents.com.ua/glavy/51977-rozdl-7-normativno-pravove-regulyuvannya-nformatsyno-bezpeki-ukrani.html (дата звернення 16.10.2017)

ШАМАРА Р. П., ОС «Бакалавр»,
спеціальність «Право»,
Маріупольський державний
університет

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Актуальність даної теми пояснюється тим, що захист інформаційних ресурсів від несанкціонованого доступу є головним обов'язком кожного користувача інформаційного простору в різні моменти часу. Втрата особливо важливої інформації для людини може привести до надзвичайних наслідків.

Проблема захисту інформаційних ресурсів була розглянута в роботах М. Згуровського, Й. Мастяниці, О. Сосніна, Л. Шиманського [2]. Із-за швидкого вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило, крім безперечних переваг, і появу низки стратегічних проблем, а також посилення небезпеки несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем [1]. Тому, розкриємо загрози та характеристику основних шляхів захисту несанкціонованого доступу до інформаційних ресурсів.

За даними, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається із-за цілеспрямованих або випадкових дій людини, оскільки вони становлять 75 % усіх випадків стороннього доступу до особистої інформації [3].

Можна сказати з впевненістю, що «абсолютно» надійних засобів захисту для блокування несанкціонованого доступу в світі немає, прикладом може бути зовсім не давній злом сайту «Пентагону» або зараження комп'ютерів вірусом «Petya.A» із-за якого найбільше постраждала Україна (блокування роботи державних та комерційних підприємств та компаній).

Хоча «абсолютних» засобів захисту немає, проте без застосування примітивних засобів захисту не обійтись. При захисті інформаційних ресурсів від атаки через Інтернет рекомендують: 1) Не заходити на сайти з поганою репутацією, на практиці сучасні браузери мають можливість сповістити користувача про це; 2) уникати повторень пароля у різних сервісах, наприклад: «Вконтакте», «Одноклассники», «Facebook» і т.д.; 3) при вході в особистий кабінет або на власну сторінку використовувати двох етапну аутентифікацію; 4) синхронізувати електрону пошту та всі можливі акаунти з особистим смартфоном; 5)не довіряти електронним листам та запитами даних [4].

Відмітимо, що також слід захисти власний смартфон та персональний комп'ютер (або ноутбук) від вірусних атак. Рекомендують застосовувати поради Кіберполіції:

– Встановити систему захисту від DDoS-атак (безкоштовні програми Deflect, CloudFlare, Google Project Shield).

– Одразу видаляйте спам і не завантажуйте невідомі файли; будь-яку інформацію чи програму завантажуйте лише з перевірених сайтів.

– Постійно оновлюйте свою операційну систему та антивірусну програму;

– Не відвідуйте підозрілі сайти із потенційно небезпечним вмістом.

– Робіть резервне копіювання своїх файлів.

– Використовуйте Брандмауер Windows (міжмережевий екран, вбудований у Windows), який допомагає контролювати доступ програм у мережу і запобігає надсиланню зловмисних програм із вашого комп'ютера на інші [5].

Отже, з розвитком інформаційних технологій також зростає рівень небезпеки і тому захист інформаційних ресурсів від несанкціонованого доступу - це обов'язок кожної людини. Опрацювавши матеріал, можна з впевненістю сказати, що під час несанкціонованого доступу винувата саме людина та її непрофесійні дії. Для особистої безпеки не треба нехтувати правилами користування всіх інформаційних ресурсів, адже крім себе можна наразити на небезпеку інших.

Список використаних джерел:

1. Митні інформаційні технології. Пашко П.В. – 8.1 Захист інформаційних ресурсів від несанкціонованого доступу. – [Електронний ресурс]. – Режим доступу: http://westudents.com.ua/glavy/27658-81-zahist-nformatsynih-resursv-vd-nesanktsonovanogo-dostupu.html

2. Шляхи захисту інформаційних ресурсів від несанкціонованого доступу. − [Електронний ресурс].− Режим доступу: http://www.rusnauka.com/13_NMN_2011/Informatica/4_85740.doc.htm

3. Митні інформаційні технології. Пашко П.В.− 8.1 Захист інформації в інформаційних системах. − [Електронний ресурс].− Режим доступу: http://pidruchniki.com/13670622/informatika/zahist_informatsiyi_informatsiynih_sistemah

4. Захист інформаційних ресурсів від атак через Інтернет. Юридична фірма «Partners».− [Електронний ресурс].− Режим доступу: http://partners.kiev.ua/pobudova-sistemi-korporativnoyi-bezpeki/zahist-informatsiynih-resursiv-vid-atak-cherez-internet/

5. Як захистити свій комп'ютер від хакерських атак . Поради Кіберполіції.− [Електронний ресурс].−Режим доступу: http://ranok.ictv.ua/2017/06/28/yak-zahystyty-svij-komp-yuter-vid-hakerskyh-atak/

ЗМІСТ