МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ
ДОНЕЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
МАРІУПОЛЬСЬКА МІСЬКА РАДА
ГОЛОВНЕ УПРАВЛІННЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
В ДОНЕЦЬКІЙ ТА ЛУГАНСЬКІЙ ОБЛАСТЯХ
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
В ДОНЕЦЬКІЙ ОБЛАСТІ
ДОНЕЦЬКЕ УПРАВЛІННЯ КІБЕРПОЛІЦІЇ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗБІРНИК МАТЕРІАЛІВ НАУКОВОГО КРУГЛОГО СТОЛУ

«Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку»

26 КВІТНЯ 2018 РОКУ

Маріуполь – 2018

УДК 004.738.5(06)
ББК 32.971.353я

Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу, м. Маріуполь, 26 квітня 2018 р. / Маріупольський державний університет; уклад. Проценко О.Б., Меркулова К.В. – Маріуполь: МДУ, 2018. – 145 с.

Рекомендовано до друку засіданням Вченої ради економіко-правового факультету Маріупольського державного університету (протокол № 10 від 20 квітня 2018 р.)

Золотухін Д.Ю.,
заступник Міністра інформаційної політики України

БОРОТЬБА З ФЕЙКОВИМИ НОВИНАМИ: ДОСВІД УКРАЇНИ ТА РЕКОМЕНДАЦІЇ

1. Сутність проблеми та можливі шляхи реагування.

“Фейкові новини” (“фейки”) є узагальненим терміном, який є продуктом медіапростору та ЗМІ, де існує необхідність надати певному явищу або феномену коротку назву для зручності у використанні. Використання цього словосполучення значно ускладнює роботу над науково-практичним та юридичним формулюванням конкретного визначення для цього феномену.

В науковому та сучасному медійному середовищі такі словосполучення мають назву “мемів”. За визначенням американського еволюційного біолога Річарда Доукінза, “мем” – лінгвістично-культурна одиниця, що описує певне явище та стає загальноприйнятою для широкого вжитку.

В широкому сенсі це словосполучення визначається як *сукупність інструментів, що застосовується з метою маніпулювання суспільною свідомістю, і, частіше всього, виражається у інформаційному повідомленні (текст/фото/відео, чи їх комбінація), що містить неправдиву чи частково правдиву інформацію та поширюється традиційними засобами масової інформації, соціальними мережами чи іншими доступними шляхами розповсюдження інформації, і має на меті сформувати у свідомості споживачів (реципієнтів) певне відношення до явища чи об’єкту реального світу*. Наприклад, сформувати ксенофобські настрої щодо якоїсь конкретної соціальної групи, через поширення негативної та емоційно зарядженої інформації про цю соціальну групу.

Через невизначеність підходів до розуміння цього явища, під категорію “фейкових новин” зазвичай потрапляють два явища:

- навмисно створені інформаційні повідомлення, які мають на меті здійснення маніпулювання,
- інформаційні повідомлення, що є результатом непрофесійного та неетичного виконання своїх обов’язків співробітниками медіа.

Однак, оскільки в обох випадках на аудиторію споживачів інформації здійснюється шкідливий вплив, що обумовлює важливість протидії обом типам “фейкових новин”.

Особливої уваги заслуговує той факт, що навмисно створені для маніпулювання аудиторією інформаційні повідомлення є різновидом т.зв. “активних заходів”, які є однією з форм роботи спецслужб та розвідувальних органів. Активні заходи (спеціальні заходи впливу, спеціальні інформаційні операції, інформаційно-психологічні спеціальні операції) використовуються спецслужбами з метою цілеспрямованої та спланованої зміни політичного дискурсу певної спільноти або суспільної думки.

Так, наприклад, “фейковою новиною” є інформація про, нібито, заклик Дмитра Яроша до лідера чеченських бойовиків Доку Умарова, яку 1-2 березня 2014 року розповсюдили провідні російські ЗМІ. В подальшому ця новина була використана для легітимізації застосування Російською Федерацією своєї армії на території України. Це свідчить про спланований та підготовлений завчасно характер цієї інформаційної операції.

Крім того, таким же прикладом є створення російськими ЗМІ (зокрема, Russia Today) віртуального образу “диспетчера Карлоса”, який повідомив, що Боїнг малайзійських авіаліній рейсу MH17 збито українським винищувачем.

Практика планування та здійснення “активних заходів” з розповсюдження дезінформації включає в себе використання подій чи фактів, що дійсно відбулися в реальності, однак в інформаційному повідомленні їх подають в неповному або спотвореному вигляді, чи в контексті емоційного забарвлення.

Нерідко поширення фейкових новин пришвидшується завдяки реплікуванню журналістами та редакторами онлайн-платформ гучних та скандальних новинних матеріалів (що є типовим для фейків). Тобто, фейк поширюється без належної перевірки фактів, з метою підвищення рейтингів чи відвідуваності інформаційних ресурсів. В цілому, гонитва окремих ЗМІ за увагою споживачів інформації істотно сприяє успішній реалізації “активних заходів” та здійсненню впливу на широку аудиторію.

Таким чином, ідентифікація та детекція “фейкової новини” за формальними ознаками є дуже ускладненою. Будь-які дії законодавчого, адміністративного чи експертного характеру щодо визначення, атрибуції та описання інформаційного повідомлення в якості “фейкової новини” неминуче призведуть до необхідності чітко регламентувати межі повноважень та компетенції суб’єкта, який здійснює таку діяльність.

Наприклад, чіткий та сталий перелік ознак “фейку” і жорстко регламентований підхід до визначення “фейкових новин” не дасть змогу ефективно протидіяти гнучким та поліморфним гібридним загрозам інформаційного простору, що будуть підлаштовуватися спецслужбами для обходу встановлених процедур. Характерною ознакою “фейкових новин” є постійне вдосконалення механізмів маніпуляції та її поширення, що нівелює спроби уніфікації їх визначення в рамках формальних ознак.

І навпаки, надто широке коло повноважень інституції, яка буде визначати “фейкові новини” на підставі суб’єктивних суджень (без жорсткої регламентації меж та чітких критеріїв і ознак) може призвести до виникнення ризиків для свободи слова.

Таким чином, реагування на “фейкові новини” шляхом їх ідентифікації і описання розцінюється як малоефективна з точки зору розвитку стратегічних комунікацій.

Крім вищеописаних труднощів адміністративно-правового підходу до протидії “фейковим новинам”, питання щодо ефективності викликає практика “розвінчування фейків”.

Процес “розвінчування фейків” полягає у наступній послідовності дій:

1) викладення недостовірної чи маніпулятивної інформації та її джерела (що, доречі, мимоволі сприяє його додатковому поширенню);

2) опис інструментів та підходів перевірки такої інформації;

3) обґрунтування недостовірності чи маніпулятивності інформації за допомогою аргументів та фактів;

4) висновок про те, що поширена інформація є недостовірною чи маніпулятивною.

З точки зору практики комунікації, така конструкція є досить складною для сприйняття широкими аудиторіями і позитивно оцінюється тільки експертами або зацікавленими саме в такому контенті споживачами.

Враховуючи це, а також очевидний факт невідповідності ресурсів, які витрачаються Російською Федерацією на створення та поширення “фейкових новин” у величезних масштабах, та ресурсів компетентних державних інституцій і недержавних організацій, що покликані протидіяти “фейковим новинам”, реактивна протидія розповсюдженню “фейків” розцінюється багатьма експертами галузі як неефективна.

В той же час, представники державних інституцій різних країн Європейського Союзу (наприклад, країн Балтії) наголошують на тому, що вони “не борються з фейками, а просувають свій наратив”. Тобто провідні державні і недержавні експерти відмовляються від реактивної протидії розповсюдженню “фейкових новин” на користь формуванню свого порядку денного в конкурентному інформаційному середовищі. Такий підхід дозволяє уникнути порядку денного, нав’язаному ззовні завдяки зовнішнім маніпуляціям. Натомість, дозволяє працювати над просуванням своїх меседжів в інформаційний простір.

Одним з перших суб’єктів, хто почав просувати таку методику боротьби з “фейковими новинами”, є Міністерство інформаційної політики України. Цей підхід не виключає необхідності реагування на “фейкові новини” шляхом перевірки, спростування брехливої інформації і надання об’єктивної інформації щодо конкретних питань. Однак проактивна діяльність державних інституцій стосовно конкурентного представлення своєї комунікаційної позиції в інформаційному середовищі була визначена пріоритетною.

2. Законодавче врегулювання

Визнання проблематики “фейкових новин” та дезінформації на законодавчому рівні є необхідним кроком для організації подальшої системної протидії інформаційному впливу на суспільство.

Для цього необхідно:

- визнати факт існування “фейкових новин” та реальної загрози, що становить дезінформація для безпеки держави;
- усвідомити необхідність відповідальності етичного та правового характеру за розповсюдження такої інформації;

- закріпити у якості пріоритету державної політики проактивний характер державних стратегічних комунікацій як форми боротьби з дезінформацією;
- визначити просування власного наративу та побудову ефективної і стійкої системи державних стратегічних комунікацій як пріоритетний напрям протидії фейкам.

За відсутності законодавчого визнання проблеми інформаційної агресії, боротьба з дезінформацією залишатиметься неузгодженою системою локальних ініціатив неурядових інституцій та окремих дій органів державної влади, без створення системи превентивної протидії.

Україна, опинившись з 2014 року в умовах широкомасштабної дезінформаційної кампанії з боку РФ, більш двох років вибудовувала власне нормативно-правове забезпечення протидії фейкам. При цьому, в контексті європейської та євроатлантичної інтеграції України, така діяльність ретельно узгоджувалась з точкою зору закордонних партнерів, які постійно наголошували на необхідності пріоритету питань свободи слова над питаннями національної безпеки.

Водночас, саме завдяки ухваленню на початку 2017 року Доктрини інформаційної безпеки в Україні був чітко визначений механізм протидії інформаційній агресії, передбачено компетенції відповідальних органів влади у цій сфері та запроваджено підхід, який враховував пріоритети громадського суспільства та закордонних партнерів України.

Таким чином, інституціоналізація системи захисту інформаційного простору держави є пріоритетним кроком у напрямку протидії дезінформації та фейковим новинам.

3. Питання відповідальності

Окрім вже зазначених вище нормативно-правових та адміністративних аспектів протидії “фейковим новинам”, потребує визначення механізм притягнення до відповідальності суб’єктів поширення дезінформації.

Принципи демократичного розвитку сучасних цивілізованих держав полягають в тому, що права і свободи людини і громадянина мають найвищу цінність. При цьому, пріоритет прав та свобод неодмінно супроводжується обов’язками, які забезпечують прийнятний порядок співіснування усіх членів суспільства. Існування прав і свобод, які не кореспондуються з відповідними обов’язками, може призвести до конфлікту в суспільстві і деформації демократичних інститутів.

Держава в особі органів державної влади є монополістом на застосування механізмів відповідальності та санкцій за невиконання обов’язків. Ці механізми реалізуються через уповноважені державні органи (суд, органи сектору безпеки та оборони, регуляторні органи тощо). Водночас, наділення органів державної влади повноваженнями щодо притягнення до відповідальності за поширення “фейкових новин” несе в собі ризик зловживання таким правом та навіть цензурування ЗМІ, що не відповідає принципам демократичного суспільства.

Крім того, суб'єктивний характер оцінювання "фейкових новин" обумовлює необхідність проведення експертиз (в т.ч. і неурядовими структурами) з метою уникнення безпідставного притягнення до відповідальності.

З огляду на вищезазначене, пріоритетна роль в системі притягнення до відповідальності за поширення "фейкових новин" має належати не державі, а профільним інституціям громадянського суспільства (ІГС).

Зважаючи на монополію держави на застосування примусу та необхідність дотримання принципів невтручання в діяльність ЗМІ, оптимальними видаються два механізми притягнення до відповідальності за поширення фейкових новин:

- змішаний, коли притягнення до відповідальності здійснюється уповноваженим Законом органом влади за висновком ІГС. При цьому, санкції матимуть адміністративний характер (попередження, позбавлення ліцензій, відкриття кримінального провадження тощо);
- недержавний, коли висновок ІГС є достатнім для відповідної реакції суспільства, публічного осуду, що тягне за собою публічну недовіру суб'єкту поширення дезінформації та нівелює його значущість у соціумі (відмова від акредитації на заходах, втрата аудиторії тощо).

Найбільш ефективним є недержавний механізм з наступних підстав. По-перше, втрата довіри до ЗМІ та його фактичне "забуття" має довготривалий ефект. По-друге, публічний осуд не може бути унинкнено за допомогою адміністративних механізмів (наприклад, шляхом оскарження застосування санкції). По-третє, таке рішення засноване на колегіальній узгодженій позиції експертів, що виключає можливість впливу зацікавленої сторони на кінцеве рішення.

Втім, що найважливіше, такий спосіб заснований на принципах саморегуляції та невтручання держави в діяльність ЗМІ. А отже, виключається можливість владного впливу на сферу масової інформації.

Водночас, недержавний спосіб потребує існування ефективного та загальновизнаного в суспільстві органу саморегуляції ЗМІ, механізму прийняття рішення таким органом та застосування відповідного рішення. Адже без належної підтримки суспільством такого рішення, його ефективність буде мінімальною та матиме скоріш декларативний ефект.

Саме тому, на період становлення відповідних громадянських інституцій, можливо тимчасове застосування змішаного механізму, який передбачатиме, по перше, систему стримувань і противаг (держава не може застосувати санкцію без рішення ІГС), а, по-друге, чітко передбачений Законом суб'єкт застосування санкції, механізм прийняття рішення, види санкцій тощо.

Основною проблемою застосування такого механізму є необхідність існування ініціативи від суб'єктів ІГС та підтримки такої ініціативи журналістською спільнотою.

4. Інші способи протидії "фейковим новинам"

Притягнення до відповідальності як спосіб реагування на дезінформацію є найбільш очевидним, втім не найефективнішим способом. Недоліком такого підходу є те, що притягнення до відповідальності – це реагування на вже здійснений факт. А фейки та інші т.зв. "активні заходи" зазвичай створюються так, щоб швидко поширюватись, фіксуватись у свідомості споживачів та гнучко підлаштовуватись під будь-які зміни, в тому числі нормативно-правового характеру. Будь-яке спростування, в тому числі публічне визнання компетентним органом фейкового характеру новини не зможе повністю нівелювати ефект від поширеної інформації.

Тому важливо враховувати та і інші способи протидії фейковим новинам, в т.ч. ті, на яких було наголошено вище:

1) поширення власного наративу;
2) спростування і розвінчування фейків;
3) застосування механізмів суспільної відповідальності за поширення "фейкових новин" і розбудову саморегуляції та співрегуляції медіасередовища;
4) підвищення медіаграмотності суспільства.

Підвищення медіаграмотності суспільства – комплекс превентивних заходів із вдосконалення здатності громадян самостійно виявляти фейки, опиратися маніпулятивному впливу, підлаштовуватися під зміни інформаційного середовища, розвивати власне критичне сприйняття інформації.

Таким чином, діяльність МІП в сфері протидії "фейковим новинам" сконцентрована на вищевикладених напрямках роботи та реалізовується в рамках проектних і програмних ініціатив по створенню системних спроможностей українського уряду і громадського суспільства нівелювати шкідливий маніпулятивний вплив, що створює загрози поступальному демократичному розвитку України на шляху інтеграції до Європейського Союзу та Північно-Атлантичного Альянсу.

Семенишин М.О.,
начальник Головного управління
Національної поліції України в Донецькій області,
генерал поліції третього рангу

СУЧАСНИЙ СТАН РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ВІДНОСНО НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

У тезах розглядаються актуальність впливу інтернету як інструменту на різні сфери життя соціальних груп, застосування заходів безпеки, забезпечення конфіденційності, цілісність та доступність особистих даних.

Соціальний та економічний розвиток все більше залежить від швидкого та безперешкодного доступу до інформації та її використання в управлінні, виробництвом, сфері послуг та громадських сферах. Постійний розвиток мережевих та інформаційних систем, включаючи аналіз великих об'ємів даних,

допомагає розвивати зв'язок, торгівлю, транспорт або фінансові послуги. Створюються та змінюються соціальні відносини в кіберпросторі, а Інтернет став інструментом впливу на поведінку значних соціальних груп, та дієвим інструментом впливу на політичну сферу.

Будь-який суттєвий зрив у функціонуванні кіберпростору, будь то глобальний або локальний, матиме вплив на економічну діяльність громадянина та його відчуття захисту та безпеки, ефективність державного сектору, установи, виробничі та сервісні процеси, врешті решт – і національної безпеки.

Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" зазначив основні завдання, цілі та напрями розвитку інформаційного суспільства в Україні [1]. Він став платформою для розробки завдань щодо розвитку інформаційного суспільства в Україні та визначив інформаційний напрям державної політики одним із пріоритетних.

Основними цілями розвитку інформаційного суспільства в Україні були визначені такі:

– використання інформаційно-комунікаційних технологій (далі – ІКТ) для вдосконалення державного управління, відносин між державою і громадянами, становлення електронних форм взаємодії між органами державної влади та органами місцевого самоврядування і фізичними та юридичними особами;

– захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту інформації про особу, підтримки демократичних інститутів та мінімізації ризику "інформаційної нерівності";

– вдосконалення законодавства з регулювання інформаційних відносин;

– покращення стану інформаційної безпеки в умовах використання новітніх ІКТ.

Відповідно до цього було визначено основні три напрями оновлення підходів інформаційної політики, зокрема:

– медіа-право як важливий базис розвитку інформаційного суспільства;

– інформаційна політика розвитку та захисту національно-ідентифікованого Інтернет-середовища;

– медіаосвіта для всіх без винятку вікових груп як потенційних учасників інформаційного суспільства.

Вказані напрями знайшли відображення у схваленій Урядом 15 травня 2013 р. Стратегії розвитку інформаційного суспільства в Україні [2]. Ця стратегія визначила мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм реалізації цієї Стратегії з урахуванням сучасних тенденцій та особливостей розвитку України в перспективі до 2020 р.

Таким чином прийняті останніми роками концептуальні документи в інформаційній сфері (розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» від 15 травня 2013 року № 386-р [2], «Про схвалення Концепції розвитку

електронного урядування в Україні» від 13 грудня 2010 року № 2250-р [3], але донині відсутня ухвалена Концепція державної інформаційної політики, що спричиняє невідповідність функціоналу підрозділів щодо боротьби з кіберзлочинністю сучасним інформаційним загрозам у сфері громадської безпеки, а загалом слугує дестабілізуючим чинником системи громадської безпеки.

Для вирішення зазначених завдань, на початку 2015 р. Президент України підписав указ «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Цим указом вводиться в дію розроблена спеціалістами з кібербезпеки та затверджена на засіданні РНБОУ Стратегія кібербезпеки України. Цей документ базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, затвердженийі набрав чинності 15 березня 2016 року [4].

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах людини, суспільства і держави.

Таким чином для реалізації Стратегії є вкрай необхідним внесення певних змін до законодавства України, з метою створення фундаментального базису для втілення в життя положень Стратегії, а також посилення відповідальність за порушення в сфері кібербезпеки.

Виходячи з вище вказаного звернемо увагу на поняття кібербезпека – це процес застосування заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних. Кібербезпека забезпечує захист ресурсів (інформація, комп'ютери, сервери, підприємства, приватні особи). Кібербезпека покликана захистити дані на етапі їх обміну та збереження. До таких заходів безпеки входять контроль доступу, навчання, аудит та оцінка ризиків, тестування, управління та безпека авторизації.

Тому сьогодні ми спостерігаємо такі явища як інформаційні війни, що перетворюються на виклик для будь-якої держави. Такі дії спонукають на корегування стратегій під нову загрозу, як великим так і маленьким державам. Як приклад, у Німеччині нещодавно було створено спецпідрозділ Бундесверу, що відповідає за безпеку в інтернет просторі. У ньому працюють більше 100 осіб, і цей підрозділ буде тільки збільшуватися. В такому разі виникає певна етична проблема. Демократичні держави вже тривалий час стоять перед проблемою, як забезпечити свободу слова та одночасно відкрити доступ до інформації і в тойже час зберегти державний і громадський устрій на належному рівні.

Прискорена дигитализация різних сфер людського життя, як і всієї економіки, призвела до того, що злочинні елементи оперативно навчилися використовувати технічні можливості в кримінальних цілях: здійснювати кібератаки, займатися шпигунством та маніпуляціями через мережі інтернет простору. Кіберзлочинність вже давно вийшла на новий рівень і не є дрібним

правопорушенням. Вона загрожує існуванню цілих держав, загальних фінансових систем, банків, особистих заощаджень громадян, в тому числі в такій заможній країні, як Німеччина. З 2016 року міністр внутрішніх справ Німеччини публічно звернув увагу на проблему кібератак і з усією серйозністю закликав населення запастися водою і продовольством на випадок надзвичайного положення. Це викликало обурення та багато запитань у громадськості, але одночасно вказало і на те, що уряд країни діє відповідально і серйозно, тому готується до нового виклику.

З огляду на вище зазначене слід звернути увагу, що такі теми, як кіберзлочинність і шпигунство, які майже не цікавлять більшість громадян. Фактично людина звикає до того, що особисті дані знаходяться у вільному доступі в глобальній мережі, і навіть добровільно сприяють такому розвитку подій, викладаючи про себе все більше особистої інформації. Такі реалії сьогодення, але не слід забувати що це небезпечно.

Підводячи підсумок щодо інформаційної безпеки на території Донецької області слід зазначити що першочерговими завданнями є, такі як, підготовка співробітників Національної поліції України користуватися новітніми засобами інформаційної безпеки відповідно до міжнародних стандартів. В складних умовах агресії протистояти необхідно і в кіберпросторі, тому вважаємо за необхідне забезпечити належний захист внутрішньої та службової інформації. Також в край нагальним є впровадження захисту від кібератак, osint-розвідки, а також розробка дієвих механізмів щодо особливостей документування інтернет шахрайства які останнім часом значно активізувалися.

Список використаних джерел

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки [Електронний ресурс] : Закон України No 537-V від 09.01.2007 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/537-16.
2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні [Електронний ресурс] : розпорядження Кабінету Міністрів України від 15 трав. 2013 р. № 386-р. – Режим доступу: http://zakoNo2.rada.gov.ua/laws/show/386-2013- %D1%80
3. Про схвалення Концепції розвитку електронного урядування в Україні [Електронний ресурс] : розпорядження Кабінету Міністрів України від 13 груд. 2010 р. № 2250-р. – Режим доступу: http://zakoNo2.rada.gov.ua/laws/show/2250-2010- %D1%80
4. Офіційний портал Верховної Ради України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Верховна Рада. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016

Селич В.А.,
начальник Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України, підполковник поліції

КІБЕРПОЛІЦІЯ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

В умовах сучасної глобалізації інформаційні технології щільно увійшли до широкого суспільного обігу, через це виникають нові загрози національній безпеці України.

Останнім часом проблема вдосконалення забезпечення національної безпеки в сфері кібернетичного захисту населення та держави зміщується у бік не стільки декларованої системи, скільки до системи реалізації практичних заходів. На сьогодні, вже законодавчо передбачено положення про створення «активного кіберзахисту» та забезпечення належних умов для безпечного використання кіберпростору, інтересах держави і суспільства.

Входячи з положень Закону України «Про основні засади забезпечення кібербезпеки України» та Стратегії кібербезпеки України, затвердженої Наказом Президента України від 15.03.2016 № 96/2016 основними завданням Національної поліції, як правоохоронного органу в розрізі реалізації державної політики в сфері протидії кіберзлочинності є: «забезпечення захисту прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснення заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі».

У рішенні Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» звертається увага, що серед основних напрямків досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони виокремлюється удосконалення державного управління та керівництва сектором безпеки і оборони, у тому числі систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів, посилення боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері.

У зв’язку із зазначеним, підрозділи Департаменту кіберполіції Національної поліції України слід розглядати, як один із суб’єктів сектору безпеки і оборони разом з іншими правоохоронними органами у сфері боротьби з кіберзлочинністю.

Положенням про Департамент кіберполіції Національної поліції України, затвердженим наказом Національної поліції від 10.11.2015 № 85, передбачено наступне: «Департамент кіберполіції Національної поліції України є

міжрегіональним територіальним органом Національної поліції України відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, здійснює інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції». Також, до основних завдань кіберполіції відносять завчасне інформування населення про появу нових кіберзлочинців, впровадження програмних засобів для систематизації кіберінцидентів, реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів.

Структурні підрозділи кіберполіції мають поділ на Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське і Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному і східному регіонах. Крім того у структурі кіберполіції створено сектор Національного контактного пункту з реагування на кіберзлочини у регіонах, який за своїми технічними і професійними можливостями має змогу миттєво реагувати на кіберзагрози, а також, у відповідності до кращих європейських стандартів забезпечити захист персональних даних громадян у віртуальному просторі, проводити міжнародну співпрацю по знешкодженню транснаціональних злочинних угрупувань у інформаційній сфері.

У створенні кіберполіції використано найкращий світовий досвід, а також пропозиції міжнародних організацій з метою забезпечення міжнародної кібердіяльності та вимог Закону України «Про ратифікацію Конвенції про кіберзлочинність». Крім того, між Україною і Європейським Союзом підписана Угода про процедури безпеки, які стосуються обміну інформацією з обмеженим доступом. Ця Угода закріпила основні положення обміну, збереження, охорони та доступу до такої інформації.

На сьогодні в кіберполіції працюють 329 осіб, або 80% штатної чисельності. Крім того, на службі департаменту є "білі" хакери. Вони працюють в управліннях технологій та програмування, які входять до складу департаменту. Всього таких управлінь чотири: у західному, південному, східному та центральному регіоні. "Білі", або "етичні" хакери, як правило, шукають уразливості в комп’ютерних системах, зламуючи їх не з метою вкрасти або здійснити фальсифікацію даних, а для того, щоб усунути уразливість.

У Нацполіції "білі" хакери проводять поглиблений огляд та вивчення вилучених цифрових доказів з метою їх виявлення або фіксації. "Насамперед йдеться про відновлення видаленої інформації та її аналіз. Проведення розвідки на підставі відкритих джерел" - OSINT. Використання OSINT дозволило встановити повні дані та місцеперебування злочинців резонансних кримінальних проваджень. Співробітники Департаменту кіберполіції цілодобово підтримують зв’язок з колегами по всьому світу, забезпечуючи

процес негайного обміну виявленими слідами злочинної діяльності за результатами реагування на кібератаки і кіберінциденти для оперативного аналізу з подальшим узагальненням отриманих результатів і використання їх для розслідування і протидії кіберзагрозам.

Поряд з тим постійно проводиться аналіз соцмереж, де на сторінках підштовхують неповнолітніх до самогубства і тілесних пошкоджень. Протягом 2017 року було виявлено 945 так званих груп смерті, з яких 760 було заблоковано. Кількість облікових записів, які вдалося ідентифікувати як зареєстровані з території України, становить 58 тис. 848.

Таким чином, в Україні, з метою захисту інформаційних та комунікаційних мереж, а також боротьбою із кіберзлочинністю функціонує Департамент кібербезпеки України, структурні підрозділи якого проходять сумісне навчання з іноземними спецпідрозділами з метою отримання передового зарубіжного досвіду у протидії кіберзлочинам. Однак, для повноцінної реалізації повноважень, покладених на підрозділи боротьби з кіберзлочинністю повинна здійснюватись належна організація та планування необхідних заходів з протидії кіберзагрозам.

Список використаних джерел

1. Стратегія кібербезпеки України: указом Президента України від 15 березня 2016 року № 96/2016 // База даних «Законодавство України» [Електронний ресурс] : Верховна Рада України. – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» [Електронний ресурс] : Верховна Рада України. – Режим доступ: http://zakon3.rada.gov.ua/laws/show/2163-19

3. Рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України», затвердженого наказом Президента України від 14.03.2016 № 92/2016 // [Електронний ресурс] : База даних «Законодавство України»/Верховна Рада України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/92/2016

Панченко В. М.,
кандидат технічних наук, старший науковий співробітник
Національної академії Служби безпеки України

BIG DATA-ТЕХНОЛОГІЇ ЯК ЗАГРОЗА КІБЕРНЕТИЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Одне із найбільших аналітичних агентств світу McKinsey за підсумками минулого року визначило серед ключових пріоритетів, що впливають сьогодні на світові тенденції, Big Data, тобто аналітику великих масивів даних, та кібербезпеку. Усі провідні компанії структурують бізнес-процеси на основі аналізу даних про клієнтів і персонал. Водночас, вони змушені опікуватися

безпекою цих даних. Масштаби й наслідки кібератак у світі лише зростають, і дедалі вразливішим стає середовище інтернету речей [1].

На думку Джеймса Скота, старшого наукового співробітника Інституту технологій для критичної інфраструктури (Institute for Critical Infrastructure Technology), демографічні та психографічні метадані нададуть змогу виконувати передові операції з фішингу стосовно керівників критично важливих інфраструктур та широкомасштабні операції впливу на населення [2].

Аналізуючи етапи формування правових засад кібернетичної безпеки Європейського Союзу, Забара І.М. зазначає, що сучасний період характеризується впливом на безпекове середовище таких інноваційних технологій, як інтернет речей (Internet of Things), великі дані (Big Data), соціальні мережі (Social networking service), сервіси мобільних пристроїв (Mobile device services), хмарні технології (Cloud Technologies), застосування яких вимагає правового регулювання [3].

Таким чином, останнім часом великі дані з одного боку стають стратегічним ресурсом, а з іншого породжують нові проблеми безпеки. Питання кібернетичної безпеки, пов’язані з великими даними, науковці пропонують розглядати у двох аспектах: застосування аналітики великих даних для вирішення проблем кібернетичної безпеки та кібернетична безпека власне самих великих даних [4]. Ми ж пропонуємо звернути увагу на ще деякі важливі аспекти у цьому контексті: підготовка фахівців із захисту великих даних, застосування аналітики великих даних хакерами у злочинних цілях та вплив Big Data-технологій на національну безпеку, зокрема безпеку держави.

Так, однією із новітніх тенденцій у сфері захисту від кібератак є використання аналітичних систем, що ґрунтуються на обробці великих обсягів даних із застосуванням машинного навчання і штучного інтелекту (Machine Learning-based Security Systems on Big Data Analytics). Ці системи надають можливість помічати відхилення у поведінці служб чи користувачів від норми і таким чином виявляти більшість небезпечних кібератак [5-7].

На думку фахівців, безпека обробки, зберігання та передачі великих масивів даних один із важливих аспектів Big Data-технологій, адже інформація має ціну, а її витік може завдати значної шкоди бізнесу. Зокрема, за даними доповіді 2016 року «The EU Data Protection Reform and Big Data: Factsheet», персональні дані європейських громадян (450 млн. осіб) до 2020 року будуть оцінюватися в один трлн. євро. Як свідчить дослідження, довіра клієнтів до компанії безпосередньо залежить від надійності захисту даних. У випадку їх витоку бізнес може втратити довіру та гроші клієнтів, а також понести відповідальність у формі штрафів, призупинення діяльності, судових переслідувань. За останніх три роки найбільше від витоку інформації постраждали Yahoo (витік даних — понад 500 млн. клієнтів), The Home Depot (50 млн. власників пластикових карток), Target (70 млн. власників кредитних і дебетових карток) [8].

У порівнянні з традиційними проблемами кібербезпеки (конфіденційність, цілісність і доступність інформації) проблеми безпеки великих даних характеризуються такими особливостями: відсутність досвіду щодо захисту Big Data, а відтак і відсутність підготовлених фахівців для вирішення таких завдань; відсутність методології та стандартів захисту Big Data; велика, неоднорідна, динамічно зростаюча структура Big Data; відсутність правового регулювання Big Data; при використанні великої кількості даних зростає ймовірність їх витоку; Big Data стають джерелом для APT-атак (advanced persistent threat — «розвинута стійка загроза, або таргетована кібератака, що спрямована на конкретного об'єкта, може тривалий час здійснюватися приховано у різних напрямках та ґрунтується на зібраних про об'єкт даних, у тому числі шляхом соціальної інженерії).

Якщо компанії та організації використовують машинне навчання та штучний інтелект, аби зміцнити кібербезпеку, те ж саме робитимуть і кібернападники. Зловмисники використовують машинне навчання, щоб пришвидшити процес пошуку вразливостей у комерційних (або державних) системах, при цьому приховуючи свої нові можливості. Зокрема, одна із найпотужніших атак відбулася, коли шпигунські програми через Wi-Fi проникли і поширилися державною системою автоматичних камер спостереження [1].

З огляду на подальше впровадження інформаційних систем надання адміністративних послуг, в урядових структурах з'являється все більша кількість реєстрів персональних даних, втрата або витік яких становить загрозу національній безпеці (реєстри медичних декларацій, системи пенсійного страхування тощо). Більше того, як засвідчили результати останніх виборів Президента США, навіть персональні дані соціальних мереж можуть бути використані на шкоду національній безпеці [9].

Водночас, дані соціальних мереж, які використовуються BigData-алгоритмами, не такі точні, як дані з месенджерів мобільних телефонів, оскільки телефоном люди частіше говорять те, що думають та передають відомості про свої реальні дії, не усвідомлюючи цього. Як відомо, мобільні оператори, що функціонують на території України, розвивають власні месенджери (наприклад, Veon від «Київстар»), завдяки яким отримають необмежений доступ до персональних даних українських користувачів. Зауважимо, що ці мобільні оператори на 97% належать російським власникам [10]. При цьому, РФ цілеспрямовано розвиває технології штучного інтелекту для обробки великих масивів даних та інфраструктуру для зберігання таких даних, зокрема персональних даних користувачів мобільних послуг. Покладаючи фінансування цих проектів на бізнес, російська влада зберігає над ними контроль через кадрові призначення, законодавчі обмеження або входження до складу співвласників компаній [11]. Таким чином, в умовах динамічного розвитку BigData-технологій розпорядниками персональних даних українських громадян через соціальні мережі є американські компанії, а даних

мобільних сервісів – підконтрольні російській владі оператори зв'язку. На сьогодні, Україна має вкрай обмежені можливості щодо захисту персональних даних своїх громадян, що врешті може призвести до втрати ще однієї складової суверенітету нашої держави.

На нашу думку, вирішення цієї проблеми потребує вжиття комплексу заходів, одним із яких є імплементація Регламенту ЄС із захисту персональних даних (EU General Data Protection Regulation, GDPR), тим більше, що цей нормативний акт зобов'язує юридичних осіб, які обробляють персональні дані громадян Євросоюзу, захищати такі дані не лише на території ЄС, але й поза його межами. Детальний аналіз нововведень, які запроваджуються цим документом, наведено у публікації [12]. Наведемо найбільш суттєві з них:

GDPR вже набув чинності, але кінцевою датою, з якої він почне застосовуватися до всіх суб'єктів, що підпадають під його регулювання, є 25.05.2018 р.;

види відповідальності варіюються від штрафів у розмірі до 20 млн. євро або 4% від щорічного світового обігу компанії (контролера або обробника) до кримінальної відповідальності (залежно від національного законодавства), а також шкоди репутації;

предметом регулювання GDPR є персональні дані – інформація, за якою прямо чи опосередковано можна ідентифікувати особу (GDPR до персональних даних відносить навіть IP-адреси, філософські й політичні погляди);

у GDPR виділяються «спеціальні категорії персональних даних» – так звані конфіденційні (делікатні) дані, серед яких генетичні чи біометричні дані, інші унікальні ідентифікатори особи;

GDPR поділяє суб'єктів персональних даних на «контролерів» та «обробників». Перші – суб'єкти, які вирішують, як і коли збирати персональні дані. Другі – суб'єкти, які діють на виконання вказівок контролера. Контролером, наприклад, є банк, який збирає персональні дані своїх клієнтів, коли вони відкривають рахунки, тоді як обробляти ці дані (тобто зберігати, оцифровувати тощо) може інша організація – обробник;

у ЄС норми GDPR мають пряму дію та обов'язкові до застосування в усіх державах-членах;

на компанії-нерезиденти ЄС, у тому числі українські, вимоги розповсюджуються у таких випадках:

- компанія має співробітників з ЄС;
- компанія проводить маркетингові чи інші дослідження суб'єктів ринку у ЄС;
- компанія здійснює діяльність (постачає товари / виконує роботи / надає послуги) громадянам ЄС;
- компанія використовує інформацію громадян ЄС у своїх власних продуктах.

Отже, найбільше нові вимоги торкнуться компаній, що мають клієнтів з ЄС або постачають товари/послуги в ЄС: ІТ-компанії, туристичні агентства,

дизайнерські фірми тощо. Разом з тим, зауважимо, що новий Регламент торкнеться не лише приватного сектору, адже обробка персональних даних громадян ЄС може здійснюватися і державними юридичними особами. Отже, його імплементація в Україні хоча і залишається на сьогодні невирішеним питанням, але може стати одним із прикладів державно-приватного партнерства, за умови що обидві сторони (державний і комерційний сектори) об'єднаються для реалізації спільних інтересів.

Загалом впровадження GDPR вимагає наявності належних технічних та організаційних засобів, для того щоб знати, які дані збираються, їхній обсяг, строк зберігання тощо, а також мати можливість відреагувати на будь-який витік даних від випадкового відправлення контактних даних на неправильний e-mail до хакерської атаки та викрадення даних користувачів.

Як свідчить проведене дослідження, питання застосування аналітики великих даних для вирішення проблем кібернетичної безпеки та пошук шляхів безпечної обробки великих даних на сьогодні вже стали предметом уваги науковців та фахівців галузі. Натомість, аспекти застосування аналітики великих даних хакерами у злочинних цілях та вплив Big Data-технологій на національну безпеку, підготовки фахівців із захисту великих даних, на нашу думку, потребують вивчення. Одним із актуальних напрямків наукових досліджень даної теми вважаємо також розробку правових механізмів імплементації Регламенту ЄС із захисту персональних даних (GDPR) в Україні.

Список використаних джерел

1. Іванова К. Головні слова 2017-го – Big Data і кібербезпека [Електронний ресурс] / Кіра Іванова // Режим доступу: https://kfund-media.com/golovni-slova-2017-go-big-data-i-kiberbezpeka/.

2. Юзькова А. Якою буде кібербезпека у 2018 році [Електронний ресурс] : Анжеліка Юзькова. – Режим доступу: https://nachasi.com/2018/01/17/cbsc-in-2018/.

3. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій / І.М. Забара // Журнал європейського і порівняльного права. – 2017. - Вип.3. - С. 2-13.

4. Aliguliyev R.M., Hajirahimova M.Sh. "Big data" phenomenon: Challenges and Opportunities // Information Technology Problems, 2014, No 1, pp. 3-16.

5. Зануда А. Експерт: кіберзахист – це не параноя [Електронний ресурс] : Анастасія Зануда // Режим доступу : http://www.bbc.com/ukrainian/features-39364360.

6. Big data and machine learning: A perfect pair for cyber security? [Електронний ресурс]. – Режим доступу: https://blog.trendmicro.com/big-data-and-machine-learning-a-perfect-pair-for-cyber-security/.

7. Big Data Security Analytics: A Weapon Against Rising Cyber Security Attacks? [Електронний ресурс]. – Режим доступу: https://bi-survey.com/big-data-security-analytics.

8. Смирнов Д. Защита Big Data: проблемы и решения [Електронний ресурс] : Дмитрий Смирнов . – Режим доступу: http://www.it-weekly.ru/it-news/security/117831.html.

9. «Троянський кінь» Кремля: соцмережі визнали, що їх використали для маніпуляцій у США [Електронний ресурс] : Остап Яриш, Наталія Гуменюк . – Режим доступу: https://hromadske.ua/posts/rosiya-cherez-socmerezhi-manipulyue-amerikancyami.

10. Мацкевич Д. Мобильные операторы Украины или кого могут слушать спецслужбы РФ [Електронний ресурс]. – Режим доступу : https://stopterror.in.ua/info/2017/06/mobilnye-operatory-ukrainy-ili-kogo-mogut-slushat-spetssluzhby-rf/.

11.Панченко В.М. Загрози національній безпеці України в умовах впровадження BigData-технологій / В.М.Панченко // Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – Київ : Нац. акад. СБУ, 2018. – С. 127-131.

12. Тищенко К. GDPR – нові виклики для обробників персональних даних в Україні [Електронний ресурс]. – Режим доступу : http://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/gdpr--novi-vikliki-dlya-obrobnikiv-personalnih-danih-v-ukrayini.html.

Бондаренко І. Д.,
викладач спеціальної кафедри
Навчально-наукового інституту інформаційної безпеки
Національної академії Служби безпеки України

ШЛЯХИ ВДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ СБ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Із розвитком інформаційно-комунікаційних технологій та їх упровадженням у всі сфери життя суспільства «традиційні» виклики та загрози, яким має протидіяти правоохоронна система держави, зазнають змін. Кіберпростір починає використовуватись у деструктивних цілях і не лише злочинцями, але й іноземними спеціальними службами. Набувають поширення раніше невідомі явища «кібершпигунство», «кібертероризм», «кібердиверсія». Забезпечення державної безпеки в таких умовах передбачає необхідність вдосконалення роботи спецслужби, зокрема її організаційної структури, правового та матеріально-технічного забезпечення.

Для протидії новим викликам та загрозам державній безпеці в 2012 році в структурі Служби безпеки України було створено профільний департамент, який відповідає за забезпечення кібербезпеки: відповідно до Указу Президента України від 25 січня 2012 року № 34/2012, Закону України від 9 грудня 2011 року № 4157-VI «Про внесення змін до деяких законів України щодо структури та порядку обліку кадрів Служби безпеки України» створювався

Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

З 2014 року кібернетичні виклики та загрози, яким протидіє вищезазначений департамент, зазнали суттєвих кількісних та якісних змін. Вони стали одним з елементів гібридної війни, що ведеться проти України, переважно спрямовуються на, так звані, об'єкти критичної інформаційної інфраструктури, стале функціонування яких необхідне для нормального життя суспільства. Такі атаки часто здійснюються напередодні знакових національних свят, мають на меті дестабілізацію соціально-політичної обстановки в державі.

В 2014 році напередодні виборів Президента України мала місце перша масштабна кібератака, а саме атака на Єдину інформаційно-аналітичну систему «Вибори», призначену для оприлюднення попередніх даних про хід та результати виборів, пересилання між окружними виборчими комісіями і ЦВК електронних протоколів підрахунків голосів. Один з епізодів атаки мав наслідком знищення інформаційних масивів на сервері ЦВК, інший – оприлюднення на сайті проросійської хакерської групи «Киберберкут» внутрішніх файлів системи ЦВК, логінів та паролів доступу адміністраторів. Але найбільш провокаційний епізод зазначеної атаки – це несанкціоноване приховане розміщення хакерами на сайті ЦВК окремого підрозділу, який мав забезпечити висвітдення у визначений час на сайті ЦВК заздалегіть підготовленого графічного файлу із зфальшованою діаграмою результатів голосування, дані якої не відповідали реальним результатам волевиявлення (Д. А. Ярош – 37,13%, П. О. Порошенко – 29,63%, Ю. В. Тимошенко – 11,42% і т. д.). Попри той факт, що вказаний файл було своєчасно виявлено та знешкоджено українськими правоохоронцями і він не був висвітлений на сайті ЦВК, починаючи з 20:00 25 травня, тобто з часу, коли шкідливе програмне забезпечення мало б відобразити сфальшоване зображення, засоби масової інформації Російської Федерації почали оприлюднювати відповідні неправдиві дані щодо результатів президентських виборів – перемоги Дмитра Яроша. Така поінформованість російських ЗМІ щодо змісту відповідної діаграми чітко вказує на організаторів відповідної атаки. Слід також зазначити, що штатний ліцензійний антивірусний засіб «Касперський» не знешкоджував шкідливе програмне забезпечення, що використовувалося під час атаки на ЄІАС «Вибори».

В травні 2015 роціу мала місце масштабна кібератака на компаню «Київобленерго», в результаті якої було відключено 30 вузлових підстанцій електроживлення Київської області, знеструмлено близько п'ятдесяти населених пунктів у дев'яти районах Київської області, позбавлені електропостачання об'єкти Південно-Західної залізниці й низки важливих підприємств промисловості. Для атаки викоритсовувався експлойт «BlackEnergy».

В грудні 2016 року було здійснено атаку на комп'ютерну систему Державної казначейської служби України, виведено з ладу її офіційний

інтернет сайт, змінено налаштування мережевих маршрутизаторів, заблоковано обмін фінансовою інформацією Казначейства з регіональними підрозділами. Зазначені дії призвели до призупинення казначейського обслуговування одержувачів бюджетних коштів (в середньому – 150 000 електронних транзакцій за добу). Паралельно було виведено з ладу інформаційну систему Міністерства фінансів України.

В грудні 2016 року кібератаки зазнало ПАТ «Укрзалізниця». В результаті несанкціонованого втручанння в роботу Єдиної автоматизованої системи управління пасажирськими та вантажними перевезеннями, інформаційних систем Дніпропетровського, Одеського та Харківського відділень Головного інформаційно-обчислювального центру ПАТ «Укрзалізниця» було призупинено надання підприємством послуги онлайн бронювання квитків, компрометовано значну кількість облікових записів співробітників.

В грудні 2016 року мала місце кібератака на ДП «НЕК Укренерго», виведено з ладу інформаційно-телекомунікаційну мережу електропідстанції «Північна» та знеструмлено декілька районів Київської області та м. Києва.

В червні 2017 року була здійснено атаку за допомогою так-ваного вірусу Petya, який приховано перезаписував директорії дискового простору, чим порушував працездатність операційної системи. Атаки зазнали понад 800 об'єктів державної та приватної форми власності, вагома частина яких відноситься до критичної інфраструктури, зокрема, в сфері енергетики, комунального господарства, транспорту, зв'язку, логістики, торгівлі, фінансів, а також державної влади та ЗМІ. Масштабність поширення вірусу Petya пов'язана із самим механізмом атаки. Був використаний спосіб не лише адресної розсилки фішингових листів електронної пошти з шкідливим програмним забезпеченням, але й інфікування серверу оновлень популярного в Україні програмного продукту для документообігу та бухгалтерської звітності M.E.Doc. Тобто мала місце так-звана «Supply Chain Attack» через довірене джерело.

За результатами аналізу вищезазначених кібератак встановлено, що їм характерні спільні блоки шкідливого коду, об'єднаність за часом та метою. Подібні технології атак, зокрема:

1. Атаки були адресними, застосовувалися фішингові листи, а у випадку вірусу Petya – шкідливим програмним забезпеченням через можливості ураженого сервера M.E.Doc збиралися коди ЄДРПОУ та вибиралися конкретні цілі для атаки.

2. Атакам передувало тривале вивчення мережевої інфраструктури майбутніх об'єктів нападу, що здійснювалося із залученням високопідготовлених профільних спеціалістів.

3. Атаки проводилися не окремими хакерами, а певними організованими структурами, оскільки передбачали значну та тривалу (до року) підгтовчу роботу.

4. Всі атаки не мали на меті отримання фінансової винагороди. Що стосується вірусу Petya, то він лише імітував здирницьке програмне забезпечення для маскування. В дійсності ж не передбачалося навіть потенційної можливості розшифровування файлів. Жодний із постраждалих, який перевів грощі в біткоінах на вказаний зловмисниками гаманець, ключ дешифрування так і не отримав.

5. Зловмисники, які здійснювали кібератаки, мають високу кваліфікацію та гарно матеріально забезпечені. Ними використовувалися найновіші технології нейтралізації антивірусних засобів, актуальні вразливості системного програмного забезпечення, так-звані «бекдори», сукупна вартість яких на «чорному ринку» може сягати декілька сто тисяч долларів США.

6. Джерело атаки детально приховувалося. Використовувалися разгалужені багатонаціональні бот-мережі, мали місце факти видалення лог-файлів на уражених комп'ютерах.

Детальний аналіз вищезазначених кібератак свідчить про причетність до них російських хакерських угруповань (Sofacy, Fancy Bear), Cozy Bear, Кібер-Беркут, Спрут тощо, які безпосередньо пов'язані із спецслужбами РФ. Тенденційний вибір часу та цілей атак свідчить, що їх справжньою метою є дестабілізація соціально-політичної обстановки в Україні.

Актуалізація кібернетичних загроз державній безпеці України мала наслідком вжиття Службою безпеки України цілої низки заходів. В структурі спецслужби створено Ситуаційний центр забезпечення кібернетичної безпеки. Це відповідає визначеному в Стратегії кібербезпеки України напрямку розвитку сектору безпеки і оборони «розвиток підрозділів кібербезпеки та кіберзахисту Служби безпеки України». На центр покладено визначену в стратегії кібербезпеки функцію СБ України реагування на кіберінциденти у сфері державної безпеки.

За фінансової підтримки Трастового фонду Україна-НАТО Служба безпеки України за провідними світовими стандартами розпочала розгортати національну систему кібербезпеки. На об'єктах критичної інфраструктури встановлюються, так-звані, сенсори для глибокого моніторингу та своєчасного виявлення кібернетичних загроз. Інформація від них потрапляє до ситуаційного центру СБ України та автоматизовано аналізується. Найближчим часом буде забезпечено роботу такого центру в режимі 24/7. Ідентифікатори виявлених вразливостей заносяться до MISP (Malware Information Sharing Platform), що є міжнародною платформою обміну даними про атаки з метою їх попередження. Сама таку ідею розвитку сектору безпеки і оборони закладено в Стратегії кібербезпеки України «розроблення та впровадження протоколів спільних дій, зокрема інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки». На базі інформації про атаки, що вже мали місце як в Україні, так і за кордоном

в MISP формуються правила для оновлення програм-міжмережевих фільтрів на об'єктах критичної інфраструктури.

В поточному році набуває чинності Закон України «Про основні засади забезпечення кібербезпеки України», який вперше на рівні закону закріплює функції СБ України в сфері кібербезпеки, зокрема щодо: негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; реагування на кіберінциденти у сфері державної безпеки; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі.

Ефективна реалізація цих функцій перебачає необхідність розвитку законодавства в сфері захисту критичної інфраструктури, адже наразі відсутній як затверджений перелік об'єктів критичної інфраструктури, так і законодавчі вимоги щодо їх захисту. Одночасно існує необхідність і внесення змін до КК та КПК з метою розмежування кримінальної відповідальності та підслідності за злочини щодо приватних комп'ютерів та тих, що забезпечують функціонування критичної інфраструктури, державних електронних інформаційних ресурсів.

Толюпа С.В.,
доктор технічних наук, професор,
професор кафедри кібербезпеки та захисту інформації
Київського національного університету імені Тараса Шевченка

ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИЗНАЧЕННЯ

У сучасних умовах уряд жодної країни не може виключати можливість того, що ключові об'єкти критичної інфраструктури держави стануть прямими об'єктами кібератак, до яких зазвичай причетні розвідувальні й спеціальні служби інших держав та спеціальні підрозділи Збройних сил.

Останніми десятиріччями у світі спостерігається стійка тенденція до зростання кількості надзвичайних подій різного походження. Щодня світові ЗМІ повідомляють про природні й техногенні катастрофи, збройні конфлікти, терористичні акти, тяжкі злочини, вчинені і злочинними організаціями, і окремими особами, акти піратства на морі тощо. І дедалі частіше в результаті таких надзвичайних подій жертвами стає велика кількість людей, а життєво важливим для існування держав системам, об'єктам і ресурсам завдається серйозна шкода. З огляду на зазначені тенденції, у більшості провідних країн світу задля систематизації об'єктів, втрата або порушення нормального функціонування яких призведе до значних або навіть непоправних негативних

наслідків для національної безпеки, введено термін «критична інфраструктура». До критичної інфраструктури зазвичай належать транспортні й енергетичні мережі, системи міжбанківських розрахунків і телекомунікації, а також об'єкти, необхідні для функціонування органів державної влади, служби реагування на надзвичайні ситуації та екстреної допомоги населенню, системи життєзабезпечення мегаполісів.

Запровадження системного підходу до розв'язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише введення відповідного терміна. На першому місці – створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди вузловим елементам критичної інфраструктури внаслідок дії негативних чинників будь-якого походження: техногенного, природного, соціально-політичного або будь-якої їх комбінації.

Кібернетичні атаки, як правило, здійснюються через інформаційно-телекомунікаційні системи, особливо, автоматизовані системи управління, які необхідні для функціонування повсякденного життя людей, структур економіки чи органів влади. Джерелами таких атак можуть бути як «недружні» держави, терористичні або радикальні організації, так і невідомі угруповання або окремі фахівці з програмного забезпечення (так звані «хакери»). До того ж, кібератака на життєво важливу інфраструктуру може бути інструментом терору, акцією недружньої держави, помсти або навіть простого хуліганства.

Кібернетична безпека вже стала невід'ємною частиною національної оборонної стратегії України, тому виникає потреба створення фундаменту законодавчого врегулювання питань забезпечення кібернетичної безпеки. Так Верховна Рада України 05.04.2018 року затвердила у першому читанні проект закону №8068 про національну безпеку, який є необхідним, і на часі передбачає багато корисних нововведень в сфері безпеки та оборони, серед яких зокрема: розмежовуються посади начальника генерального штабу та головнокомандувача військами, а на посади міністра оборони та його заступників мають бути призначені цивільні особи. Така система управління відповідає нормам країн-членів НАТО і внесена в закон за рекомендаціями радників північноатлантичного Альянсу. Закон закріплює видатки на сектор оборони та безпеки не менше 5% від ВВП. Передбачається здійснення громадського та цивільного контролю за сектором безпеки та оборони, зокрема громадськими організаціями та активістами. Законом визначено створення та затвердження документів довгострокового планування, зокрема: Стратегія національної безпеки України, Стратегія воєнної безпеки України, Стратегія громадської безпеки та цивільного захисту України, Стратегія розвитку оборонно-промислового комплексу України, Стратегія кібербезпеки України, Національна розвідувальна програма.

Таким чином одним із основних завдань політичного керівництва будь-якої держави є забезпечення гарантованого функціонування відкритого, надійного та захищеного кіберпростору. Через відсутність кордонів у

кіберпросторі, а також відкритість, покладену в основу сучасних інтернет-технологій, та анонімність значно зростає кількість зовнішніх кібератак та кіберзагроз, що автоматично призводить до необхідності розробки чіткої стратегічної концепції як ідейної основи формування пріоритетів національної політики в кіберпросторі. Інакше кажучи, глобальний характер кіберпростору здатний підвищити ступінь ризику, впливаючи як на державний, так і на приватний сектор.

На сьогодні триває процес розбудови національної системи кібербезпеки і кіберзахисту, формування її організаційно-технічної моделі, здатної забезпечити оперативне і адекватне реагування на потенційні та реальні кіберзагрози.

Питання дослідження критичної інфраструктури стають пріоритетними в багатьох країнах світу, не є винятком і Україна, де рівень розвитку інформаційних технологій та можливості сучасних комплексів імітаційного моделювання постійно підвищуються. Серед цілей подібних досліджень виділяють захист національної критичної інфраструктури та організацію впливу на її об'єкти у супротивника. При цьому головне завдання полягає у виявленні ключових об'єктів (або їх сукупності), вплив на які може надати найбільш негативний ефект на галузь економіки, ключовий ресурс або всю інфраструктуру, а також в оцінці наслідків подібного впливу та розробці механізмів зниження таких ризиків.

Однією з основних труднощів при виявленні ключових об'єктів критичної інфраструктури до недавнього часу була відсутність чіткого математичного апарату, що не дозволяло сформувати кількісні показники вразливості об'єктів. Ймовірно, цим і можна пояснити те, що в основі більшості подібних досліджень лежав метод експертних оцінок, який передбачає обов'язкову наявність інформації про можливу шкоду «еталонного об'єкту» або розробку спеціальної шкали факторів ризикованості («небезпечності») таких.

Україні лише розпочинає формуватися розуміння масштабів та наслідків сучасних кіберзагроз, необхідності забезпечення максимально захищеного кіберпростору. Загрози критичної інфраструктури в разі їх реалізації проявлятимуться у вигляді припинення надання послуг та товарів, що є життєво важливими для населення, економіки, державного управління. Це забезпечення населення, суб'єктів господарювання та органів влади електроенергією, зв'язком, послугами з транспортних перевезень, водопостачання, водовідведення, каналізації тощо. Припинення надання таких послуг та товарів може призводити до соціально-політичної нестабільності, загострення внутрішньополітичних конфліктів, значних економічних втрат, послаблення інститутів влади.

Особливо небезпечними є комбіновані загрози й загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів критичної інфраструктури.

Напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність і суверенітет, характеризується значним зростанням рівня таких загроз зловмисних дій, як вчинення терористичних актів і диверсійних операцій на території України, спрямованих на об'єкти критичної інфраструктури. Безумовно, найсерйознішою може бути потенційна загроза використання з терористичною метою об'єктів ядерної енергетики.

За час проведення антитерористичної операції інфраструктурні об'єкти, що знаходяться на території Харківської, Донецької, Луганської та Запорізької областей неодноразово ставали ціллю атак з боку терористично-диверсійних формувань шляхом підривів залізничного полотна та опор мостів, ліній електропередач. Це говорить про недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій. Велика протяжність інфраструктурних об'єктів унеможливлює забезпечення їх повсюдної охорони, проте мають бути захищені вузлові об'єкти та ретельно сплановані та організовані дії із забезпечення та використання резервних можливостей інфраструктурних мереж.

Створення дієвої системи захисту об'єктів критичної інфраструктури в Україні є актуальним завданням, що має вирішуватись в рамках загального реформування сектору безпеки і оборони із врахуванням всього існуючого спектра загроз та забезпечення взаємопов'язаності різних систем, що неможливо без застосування науково обґрунтованих методологій. Без сумніву, моніторинг та прогнозування кризових ситуацій має здійснюватися із застосуванням сучасних інформаційних технологій та систем підтримки прийняття рішень.

Існуючі системи фізичного захисту об'єктів критичної інфраструктури, що охороняються, використовують радіолокаційні, оптоелектронні, інфрачервоні, контактні електронні і електромагнітні підсистеми контролю периметра і території, що охороняється, що в сукупності забезпечують процес управління надзвичайною ситуацією терористичного характеру на об'єкті критичної інфраструктури. Головне завдання цього управління – не допустити зловмисників на об'єкт, своєчасно виявляючи і припиняючи їх дії. Однак, функціонування цих засобів спостереження залежить від стану приземних шарів атмосфери, наявності природних і штучних завад та інших факторів.

Указом № 8 від 16.01.2017 року Президент ввів в дію рішення Ради національної безпеки і оборони «Про вдосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». Даним Указом він доручив Кабінету Міністрів протягом двох місяців розробити і прийняти концепцію створення державної системи захисту критичної інфраструктури і план заходів щодо її реалізації.

Протягом двох місяців після прийняття концепції повинна бути розроблена державна система захисту критичної інфраструктури, а на розгляд парламенту винесено законопроект про критичну інфраструктуру та її захист, в якому

повинні бути передбачені такі заходи: створення державної системи захисту критичної інфраструктури; визначення органу, відповідального за координацію діяльності щодо захисту критичної інфраструктури; визначення основ державно-приватного партнерства та ресурсного забезпечення в сфері захисту критичної інфраструктури; визначення основ міжнародного співробітництва в сфері захисту критичної інфраструктури. Службі безпеки України доручено протягом трьох місяців вжити заходи щодо вдосконалення контррозвідувального забезпечення та захисту критичної інфраструктури.

Хроніка надзвичайних ситуацій терористичного характеру показує, що терористична діяльність в сучасних умовах характеризується широким розмахом, відсутністю явно виражених державних кордонів, наявністю зв'язку і взаємодією з міжнародними терористичними центрами і організаціями. У розвитку тероризму простежується ряд більш-менш виразних тенденцій, вивчення яких має важливе значення і для розуміння ролі тероризму як глобальної загрози людству, багатьом країнам світу, і для наукової розробки системи заходів, необхідних для ефективної боротьби з ним.

Україна підтвердила свій євроінтеграційний вибір, і це передбачає, зокрема, її наближення до підходів ЄС у безпековій сфері. Також треба зважати на процеси реформування державного апарату в Україні, що закладають сприятливі організаційно-управлінські підвалини для запровадження концепції захисту критичної інфраструктури в нашій країні. Зважаючи на це, упровадження в Україні концепції захисту критичної інфраструктури стане важливим кроком до вдосконалення існуючих державних систем та інституцій у сфері безпеки. Заходи щодо захисту критично важливих об'єктів, систем і ресурсів в Україні здійснюються низкою відомств у межах їх завдань і компетенції, мають фрагментарний характер, що відбивається в паралельному функціонуванні систем, призначених для захисту об'єктів і населення від окремих типів загроз (техногенного, природного або соціально-політичного характеру), зокрема таких, як Єдина державна система запобігання та реагування на надзвичайні ситуації техногенного і природного характеру; Єдина державна система цивільного захисту населення й територій; Єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків.

Категоризація критично важливих об'єктів або елементів критичної інфраструктури України здійснюється на основі галузевих (відомчих) підходів, з огляду на міркування і критерії забезпечення безпеки за окремими складниками національної безпеки (економічної, державної, політичної, енергетичної, екологічної, гуманітарної тощо), результатом чого стали різні дефініції об'єктів: підприємства, що мають стратегічне значення для економіки та безпеки держави; важливі державні об'єкти; об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період; потенційно небезпечні та об'єкти підвищеної небезпеки; особливо важливі об'єкти

електроенергетики, нафтогазової галузі; нерухомі пам'ятки культурної спадщини.

Попри істотні досягнення у становленні (формуванні) системи захисту національної безпеки України, існує низка труднощів і проблем, пов'язаних із захистом критичної інфраструктури, що потребують розв'язання: невідповідність національної нормативно-правової бази положенням міжнародних документів, зокрема у частині, що регулює питання захисту критично важливих об'єктів та інфраструктури, на тлі декларування курсу на євроінтеграцію; обмеженість механізмів обміну інформацією та інформаційного забезпечення про загрози об'єктам критичної інфраструктури й відсутність механізмів надвідомчого управління та інвентаризації ресурсів, задіяних для попередження загроз техногенного і природного характеру, в умовах зростання їх рівня, що вимагає ліпшого забезпечення інженерними засобами, обладнанням, технікою, інформаційними та кадровими ресурсами; відсутність нормативних документів, вимог, методологій для оцінки загроз об'єктам, критичним для життєдіяльності держави; загальної методології оцінки ризиків для критично важливих об'єктів та інфраструктури, не зважаючи на щільну взаємозалежність критично важливих об'єктів (насамперед інформаційних, енергетичних і транспортних мереж), що створює небезпеку виникнення каскадних аварій; відсутність ефективної практики державно-приватного партнерства у сфері безпеки, що вимагає вдосконалення організаційних і правових основ такого партнерства; міждисциплінарний характер завдань захисту критичної інфраструктури, що потребують комплексних наукових досліджень, які через свою складність вимагають значних фінансових інвестицій.

Список використаних джерел

1. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2012. – 96 с.
2. Указ Президента України №8/2017 від 16 січня 2017 року. [Електронний ресурс] . Президент України Офіційне Інтернет-представництво – Режим доступу : http://www.president.gov.ua/documents/82017-21058
3. Порошенко усилил защиту объектов критической инфраструктуры. [Електронний ресурс]. – Режим доступу : http://news.liga.net/news/politics/14672613-poroshenko_usilil_zashchitu_ obektov_kriticheskoy_infrastruktury.htm
4. Бурячок В.Л., Толюпа С.В., Толубко В.Б., Хорошко В.О. «Інформаційна та кібербезпека: соціотехнічний аспект» // Навчальний посібник. – К.: Наш формат, 2015. – 288с.
5. Аварии и катастрофы природного характера в Украине. [Електронний ресурс] : Служба 101 - наша служба. – Режим доступу : http://service01. in.ua/index.php?/topic/91-avarii-i-katastrofy-prirodnogo-kharaktera-v-ukr/
6. Лазаренко С. В. Некоторые аспекты безопасности критической инфраструктуры государства / Ю. Ю. Гончаренко, М. М. Дивизинюк, Н. В. Касаткина, Г. В. Камышенцев, С. В. Лазаренко // Інформаційна безпека –

Науковий журнал Східноукраїнського національного університету імені Володимира Даля. – Северодонецьк: СУНУ ім. В. Даля, 2016. – № 4(24). – С. 135 – 140.

7. Безрук В.М., Баранник В.В., Толюпа С.В. и др. Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, инфомационная боротьба. Коллективная монографія. Харьков – Компания СМИТ – 2017. – с. 620.

Тимчук О.С.,
кандидат технічних наук, доцент,
в.о. декана фізико-технічного факультету,
доцент кафедри комп'ютерних технологій
Донецького національного університету імені Василя Стуса
(м. Вінниця)

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ В УМОВАХ ДЕФІЦИТУ ІНФОРМАЦІЇ ВІД ЕКСПЕРТІВ

Однією з пріоритетних задач інформаційних технологій є інтелектуальне об'єднання компонентів за допомогою Інтернет для формування нових економічних можливостей для окремих осіб, бізнесу та держав (Internet of Everything, IoE) [1]. У IoE виділено 4 компонента:

1. Люди, які підключаються і використовують Інтернет різними способами. У 2017 році всього було зареєстровано 1.24 млрд web-сайтів і 3.74 млрд користувачів Інтернет, які підключаються до мережі за допомогою пристроїв (наприклад, ПК, смартфон) і найчастіше використовують соціальні мережі (наприклад, Facebook, Twitter, LinkedIn) [2].
2. Речі, що складаються з фізичних елементів (наприклад, датчики, споживчі пристрої) і активів підприємства, які підключені як до Інтернет, так і один до одного. Ринок речей інтенсивно зростає: від 2 млрд об'єктів у 2006 році до прогнозованих 200 млрд до 2020 року, що складе близько 26 інтелектуальних об'єктів на кожну людину у світі [3].
3. Дані, що надходять від людей і речей. Основними проблемами забезпечення безпеки даних дослідники IDC вважають загрози втрати даних і загрози конфіденційності даних [4].
4. Процеси, що забезпечують взаємодію трьох компонент IoE – людей, речей і даних.

Повсюдне використання технологій IoE обумовлено розвитком і збільшенням доступності пристроїв з підтримкою IP, глобального широкосмугового зв'язку та появою IPv6. Разом з щорічно зростаючої залежністю від технологій IoE стрімко зростає і кількість кіберзлочинів в IT-інфраструктурах підприємств і держав. Згідно зі звітом Cybersecurity Ventures [5], в 2017 році найбільш піддані кібератакам були наступні галузі:

- охорона здоров'я;
- промисловість;

- фінансовий сектор;
- урядовий сектор;
- транспортний сектор.

У звіті також зроблено прогноз, що кіберзлочинність буде коштувати світу 6 трильйонів доларів на рік до 2021 року, в порівнянні з 3 трильйонами доларів в 2015 році.

Дослідниками виділені основні проблеми кібербезпеки в 2017 р. [4]:

1. Безпека хмарних технологій. Основні проблеми: втрата / витік даних, загрози приватності даних і порушення конфіденційності.

2. Аутсорсинг. Основні проблеми: треті сторони не забезпечують адекватний захист інформації або інформаційних систем.

3. BYOD (Bring Your Own Device). Основні проблеми: втрата / витік даних, установка небезпечних додатків, завантаження небезпечного контенту, проникнення шкідливих програм в IT-інфраструктуру підприємства.

4. Web- і mobile- безпека. Основні проблеми: втрата / витік даних, виявлення загроз / порушень, забезпечення вимог щодо дотримання відповідності.

5. Навчання і сертифікація. Основні проблеми: відсутність фахівців, які володіють навиками реагування на інциденти, виявлення ненормальної поведінки системи, інтелектуального аналізу і мають знання щодо критично важливих бізнес-процесів.

Реальність така, що побудувати абсолютно безпечний кіберпростір неможливо. Побудова ефективної системи захисту кіберпростору можлива тільки за умови якісної оцінки ризиків кібербезпеки, шляхом аналізу факторів ризиків і обліку доступного бюджету для зниження ризиків. Оцінка ризиків проводиться щорічно відповідно до плану оцінки ризиків кібербезпеки для інформаційних ресурсів критичних бізнес-процесів, а також при надходженні окремих запитів на проведення оцінки ризиків кібербезпеки, пов’язаних зі змінами в IT сервісах і бізнес-процесах. Оцінка ризику складається з процесу ідентифікації ризику, аналізу ризику і визначенні рівня ризику [6].

Оцінку ризиків виконують підприємства як великого і середнього, так і малого бізнесу. У всіх випадках для оцінки ризиків використовуються, як правило, моделі, що побудовані на якісній оцінці факторів ризиків. Основні проблеми, що виникають при оцінці ризиків з достатньою кількістю експертів (підприємства середнього і великого бізнесу):

- 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.

У даній роботі перераховані проблеми пропонується вирішувати за допомогою методу перцептивних міркувань, запропонований Wu і Mendel [7], а невизначеність, що виникає при перцептивних міркуваннях, враховувати за

допомогою методів теорії дискретних інтервальних нечітких множин другого типу [8]. Результати досліджень по даному питанню були представлені автором роботи на 23-й міжнародній конференції Soft Computing, м. Брно, Чеська республіка (2017 р.) [9].

Основною проблемою при оцінці ризиків з одним експертом (підприємства малого бізнесу) є дефіцит інформації від експертів, що призводить до суб'єктивної оцінки. У даній роботі для вирішення суб'єктивізму пропонується використовувати методи теорії нечітких множин першого типу та алгоритм мурашиної колонії. Кожну мураху колонії пропонується розглядати як окремого агента, який переміщається по заданій сітці за певними правилами. Основним завданням мурашки-агента є розмиття оцінки експерта, яка задається у вигляді нечіткої множини першого типу.

Використання методів перцептивних міркувань, теорії нечітких множин і систем, а також ройового інтелекту при оцінці ризиків кібербезпеки дозволяє вирішити проблему дефіциту інформації від експертів, що приводить до суб'єктивізму, та врахувати невизначеність, яка виникає під час вербальних оцінок.

Список використаних джерел

1 Dave Evans. The Internet of Everything. How More Relevant and Valuable [Електронний ресурс] : Connections Will Change the World. – Режим доступу : https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf

2 Simon Kemp. The global state of the internet in April 2017. – Режим доступу : https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/

3 A Guide to the Internet of Things. – Режим доступу : https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

4 2017 Cybersecurity trends report. – Режим доступу : https://www.cybersecurity-insiders.com/portfolio/cybersecurity-trends-report/

5 Steve Morgan. 2017 Cybercrime Report from Cybersecurity Ventures "Cybercrime damages will cost the world $6 trillion annually by 2021", 2017. 14 p.

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

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

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

9 Tymchuk O. Information security risk assessment model based on computing with words / O. Tymchuk, M. Iepik, A. Sivyakov // Mendel – Soft Computing Journal, Brno, Czech Republic – Vol. 23, No. 1, June 2017 – P. 119-124.

Ціон П.О.,
заступник начальника управління – начальник відділу протидії кіберзлочиннам Донецької області Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України, капітан поліції

КІБЕРПОЛІЦІЯ ТА БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ: ПРОТИДІЯ ЗАГРОЗАМ В УКРАЇНСЬКОМУ СЕГМЕНТІ МЕРЕЖІ ІНТЕРНЕТ

Враховуючи міжнародний характер кіберзлочинності, у боротьбі з нею життєво важливе значення має відповідність законодавчих та практичних заходів умовам сьогодення.

Виконуючи функції та завдання, покладені на кіберполіцію, інформування суспільства про будь-які кіберзагрози та їх попередження здійснюється за допомогою сайту кіберполіції України www.cyberpolice.gov.ua. Зокрема, використовуючи даний ресурс, можна перевірити інформацію про наявність кібератак, перевірити чи належить мобільний телефон, банківський рахунок шахрайським організаціям, зв'язатися з оперативними працівниками даного підрозділу та отримати допомогу чи консультацію. Нині проблеми протидії кіберзлочинності набувають все більшої актуальності та потребують нагального вирішення.

Тому забезпечення кібербезпеки особи, суспільства та держави входить до функціональних обов'язків структурного підрозділу Національної поліції – кіберполіції.

Метою кіберзлочинців є персональні та корпоративні дані, які самі по собі становлять цінність або за допомогою яких злочинці протиправним шляхом можуть заволодіти грошима, нематеріальними активами або майновими чи немайновими правами тощо. Сьогодні існує багато типів кіберзлочинів, серед яких найбільшу загрозу являють: онлайн шахрайство, DoS-атаки, розповсюдження шкідливих програм (Malware), кардерство, фішинг, комп'ютерне шпигунство, екстремізм у мережі (який все частіше кваліфікується як кібертероризм), особиста образа або наклеп тощо. Більшість із перелічених вище злочинів скоюються не лише на території або у віртуальному просторі однієї конкретної країни, вони можуть мати і більш глобальний міждержавний чи навіть міжнародний характер, тобто є по своїй суті трансграничними.

За підрахунками команди реагування на комп'ютерні надзвичайні події України в українському сегменті мережі Інтернет на поточний момент близько 2500 веб-сторінок, які презентують державний сектор України. З них приблизно половина має ознаки компрометації і це тільки вершина айсбергу, адже про «кіберзло» відомо далеко не все. Кібератаки мають серйозні наслідки, незважаючи на те, що практично кожна з постраждалих організацій володіє засобами антивірусного захисту. Загрози у кіберпросторі постійно змінюються.

Традиційні загрози набувають більш небезпечних, підступних та ефективних в дії типів, наприклад Advanced Persistent Threats (APT) – просунуті стійкі загрози.

Кіберполіція регулярно фіксує атаки на органи державної влади України які мають усі ознаки APT. Найчастіше джерелами APT є установи, що фінансуються з державних бюджетів та мають цілі, що виходять далеко за межі простої крадіжки: військова розвідка, економічний саботаж, технічний шпіонаж, фінансові махінації, політичні маніпуляції. У той час, коли організації все більше переводять свою діяльність у цифровий світ і створюють нові канали взаємодії з користувачами, постійні мутації кіберзагроз породжують нові ризики і нові питання.

Для організацій та підприємств сьогодні важливим є завдання визначення як використовувати проривні технології і тенденції, такі як Інтернет речей, хмарні технології, мобільні пристрої та контролювати ризики, що виникають в системах електронного урядування. Керівники все більше усвідомлюють необхідність забезпечення передових технологій кібербезпеки. Але щоб реагувати на інциденти тільки усвідомлення цього недостатньо ─ питання кібербезпеки повинні бути предметом постійної уваги. Та незважаючи на інформаційно-пропагандистську роботу, що проводиться засобами масової інформації, люди недостатньо комп'ютерно грамотні і досі не сприймають повною мірою загрози, не виконують необхідних дій з реалізації заходів кібербезпеки, не навчені культурі кібербезпеки. Сьогодні можна з упевненістю говорити, що кожна людина була, є, або буде жертвою кібератаки. Цього майже неможливо уникнути. Особливої уваги потребують ризики, пов'язані з соціальною інженерією.

Метод соціальної інженерії орієнтований не на інформаційну або технічну складову інформаційної системи, а на людину, як найбільш слабку ланку цієї взаємодії. Основне завдання цього методу – змусити користувача виконати дії, які необхідні зловмиснику для ураження його автоматизованого робочого місця. Саме цей метод ураження є сьогодні найбільш поширеним у інформаційному просторі. Люди повинні бути свідомі того, що вони самі є мішенню для фахівців соціальної інженерії і повинні бути спроможними самим захистити себе. Це, безсумнівно, вимагає обізнаності з цього питання. Еволюція кіберзагроз відбувається також паралельно з надзвичайно швидким розвитком мобільних та соціальних технологій, поширенням смартфонів і інших мобільних гаджетів. І якщо політика BYOD (Bring Your Own Device – свобода вибору терміналу) здається менш актуальною на вищому рівні, на місцевому рівні повинні керувати цим процесом, прививати культуру користування та здійснювати відповідні заходи із кібербезпеки. У цьому контексті культура мобільної кібербезпеки має формуватися, підтримуватися та бути пов'язаною з програмами підвищення кваліфікації і навчання користувачів, щоб залишатися на рівні реальних загроз.

Наслідки від кіберзлочинів стають все більш руйнівними і необхідно дотримуватися усе більш жорстких та обов'язкових правил кібербезпеки. Рекомендації та засоби, що надає кіберполіція, значно збільшують навантаження задля їх дотримання і не всі організації мають необхідні ресурси для їх запровадження у повній мірі. Безпека та стійкість інформаційних систем стають завданнями не тільки для фахівців і груп забезпечення безпеки персоналу. Якщо ІТ-відділ відповідає за безпеку мережі, то запобігання вторгненням стає справою кожного. Кібербезпека стає колективною відповідальністю і всі повинні нести особисту відповідальність. Такий розвиток подій неминуче вимагає формування в України культури кібербезпеки і розгляду цієї проблематики у значно ширшому контексті. Існує кілька сотень визначень поняття культури. Культури кібербезпеки потрібно дотримуватися усім, у тому числі керівництву та ІТ-персоналу. Керівники частіше стають мішенню тому, що мають доступ до додаткової та більш конфіденційної інформації, ніж інші, вони часто є більш уразливими, коли знаходяться далеко від місця своєї роботи. Співробітники ІТ-відділів більш уразливі через свої привілейовані права доступу до всієї мережі організації. Міцність ланцюга послідовних заходів кібербезпеки обмежується його найслабшою ланкою, а саме – персоналом. Необхідно потрібно постійно проводити навчання ─ обізнаність людей є одним з пріоритетів створення культури кібербезпеки.

Список використаних джерел

1. Рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України», затвердженого наказом Президента України від 14.03.2016 № 92/2016 // [Електронний ресурс] : База даних «Законодавство України»/Верховна Рада України. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/92/2016

2. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування / [Електронний ресурс] : Національний інститут стратегічних досліджень при Президентові України. – Режим доступу : http/www.niss.gov.ua/articles/454/

Страдний І.О.,
інспектор відділу протидії кіберзлочинності Донецькій області Донецького управління кіберполіції Департаменту кіберполіції Національної поліції України, старший лейтенант поліції

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ У СФЕРІ ВИКОРИСТАННЯ ПЛАТІЖНИХ СИСТЕМ

Стрімкий розвиток інформаційних технологій разом із позитивним впливом на ефективність економіки держави призвів до суттєвого росту кількості правопорушень у фінансово-банківській сфері України.

Розвиток мережі комерційних банків з великими обсягами банківських фінансових операцій щодо переказів значних сум грошей між державними і

комерційними структурами як в межах країни, так і за кордон, поставив питання про необхідність спрощення розрахунків шляхом впровадження в банківську систему електронної комп'ютерної мережі та інших технічних засобів комп'ютерної обробки інформації.

Науково-технічний прогрес та формування новітніх інтерактивних форм взаємодії банків з клієнтами (Інтернет-банкінг, Інтернет-трейдинг, мобільний банкінг) дозволили зменшити час доступу до банківських послуг та скоротити тривалість обслуговування у часі. В той же час поширення впровадження сучасних інформаційних технологій спричиняє зростання загроз хакерського втручання для державних комп'ютерних систем, компаній, організацій, приватних підприємців та окремих громадян.

До основних напрямів злочинної діяльності в сфері використання платіжних систем можна віднести: фішинг, вішинг та скімінг.

Концепція фішингу (англ. fishing – риболовля) полягає у тому, що шахрай будь-якими можливими способами намагається витягнути з власника картки інформацію. Це може бути підроблений лист, наприклад, від банку або платіжної системи, клієнтом якої є власник, із проханням так чи інакше повідомити інформацію, за допомогою якої шахрай може одержати доступ до коштів – запит PIN-коду, логіна, пароля. Найпростіший спосіб фішингу – підробка листа. Користувач одержує листа з пропозицією перейти за посиланням, адреса якого схожа на адресу відомої користувачу компанії. Якщо користувач перейде за посиланням та вкаже дані доступу, які звичайно використовує для доступу до Інтернет-банкінгу або особистого кабінету, його персональні дані стануть доступними шахраям.

Вішинг (від англ. voice – «голос»; fishing – «риболовля») – вид шахрайства з банківськими картками, що значно поширився в Україні протягом останніх років. Це один з методів шахрайства з використанням соціальної інженерії. Він полягає в тому, що зловмисники, граючи роль співробітника банку або покупця, випитують по телефону у власника платіжної картки конфіденційну інформацію або провокують до здійснення певних дій зі своїм картковим рахунком.

Одним із способів викрадення коштів з банківської картки є скіммінг (англ. skimming – «знімання вершків»). Скіммер – невелике пристосування для зчитування інформації з магнітної стрічки, яке вміщається в долоні і може вмістити в себе до 200 номерів карток. Зі скіммера дані перевантажуються на комп'ютер, а з нього за допомогою спеціального декодера – на магнітну стрічку викраденої, знайденої або незаконно виготовленої картки. Інформація, яка міститься на магнітній стрічці, потім витискається на картці і ніякого додаткового обладнання чи витрат ця операція не потребує. Скіммери використовуються, як правило, особами, що приймають картки до оплати – офіціантами, адміністраторами, касирами, які копіюють дані з картки два рази – один для оформлення платежу, другий – на скіммер для злочинців.

Як варіант, на банкомат прикріплюють мініатюрну відеокамеру, яка знімає руку, що вводить пін-код, і робить запис у модуль пам'яті або передає його дистанційно на комп'ютер шахрая. Загалом у випадку дистанційної передачі шахрай знаходиться недалеко та приймає відеодані за допомогою ноутбука.

Шиммінг є різновидом скіммінгу і останньою з вигадок викрадачів, одним із способів незаконного зняття грошей за допомогою використання тонкої плівочки, схожої на скотч. Така плівка наклеюється на клавіатуру, а потім із неї зчитується необхідна інформація. Незвичайна клавіатура банкомата не викликає підозри, що значно полегшує завдання злочинцям.

Таким чином, шахрайство з банківськими картками має значні негативні наслідки для стабільності фінансової системи держави, оскільки гальмує поширення безготівкової форми оплати, яка є визнаним пріоритетом розвитку світової фінансової системи, а також завдає значної економічної шкоди для різних суб'єктів господарських процесів. Тому активна боротьба із даним проявом кіберзлочинності – це нагальна вимога часу, що потребує консолідації зусиль банківських установ, правоохоронних органів, громадських організацій та, звичайно, користувачів банківських карток.

Список використаних джерел

1. Киберпреступность [Електронний ресурс] : Термины и определения. – Режим доступу : http://it-sektor.ru/kiberprestupnost.html.

2. Киберпреступность в Украине [Електронний ресурс]. – Режим доступу : http://z-filez.info/news/kiberprestupnost-v-ukraine.

3. Кіберзлочини проти банків: полювання на мільйон [Електронний ресурс]. – Режим доступу : http://ua.prostobankir.com.ua/it/statti/kiberzlochini_proti_bankiv_polyuvannya_na_milyon.

Пефтієв О.В.,
заступник начальника відділу супроводження та розвитку інформаційних систем і баз даних Головного управління Національної поліції у Донецькій області

ЗАХИСТ ВІД КІБЕРВТРУЧАНЬ: ОДНЕ ІЗ ЗАВДАНЬ УПРАВЛІННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ПІДТРИМКИ ГУ НП В ДОНЕЦЬКІЙ ОБЛАСТІ

Діяльність Національної поліції України значною мірою пов'язана з отриманням та використанням відомостей обмеженого доступу, розголошення яких може спричинити порушення конституційних прав громадян, а також зниження ефективності роботи поліції щодо превенції, розкриття та розслідування правопорушень.

У процесі здійснення своєї діяльності співробітники поліції отримують інформацію про режим і характер роботи підприємств, розташованих на території, що обслуговується, відомості, що стосуються особистого життя громадян, а також іншу інформацію (наприклад, службового характеру). Дана інформація, а також відомості про окремі методи, прийоми і результати роботи

поліції складають службову таємницю. Розголошення таких відомостей, а також витік інформації про плановані і проводяться органами внутрішніх справ заходи щодо охорони громадського порядку і боротьбі зі злочинністю порушує нормальну їх діяльність і значно знижує її ефективність.

У своїй діяльності, для службових цілей, Національна поліція використовує наступні види мереж, а саме:

1. Мережу Інтернет, затвердженою Наказом Національної поліції України від 21.02.2017 №141 «Про систему Інтернет у телекомунікаційній мережі Національної поліції України». Використання системи Інтернет є складовою частиною телекомунікаційного забезпечення Національної поліції України і надає можливість організувати обмін інформацією між сервісами, користувачами системи Інтернет Національної поліції України та глобальною мережею Інтернет.

2. Відомчу мережу, затвердженою Наказом Міністерства внутрішніх справ України від 04.07.2016 №596 «Про єдину цифрову відомчу телекомунікаційну мережу МВС» (далі - ЄЦВТМ). ЄЦВТМ є сучасною логічно цілісною мультисервісною багаторівневою інформаційно-телекомунікаційною мережею МВС, що здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв'язку та включає сукупність технічних засобів й обладнання мережі доступу і транспортної телекомунікаційної мережі для забезпечення передачі інформації (даних), яка (які) належить (належать) до державних інформаційних ресурсів регіонального районного та міського рівнів, для потреб користувачів, а також надає підключеним до неї віддаленим один від одного користувачам системи МВС весь різновид телекомунікаційних послуг і сервісів фіксованого телефонного, документального, радіозв'язку, аудіо- та відеоселекторного зв'язку тощо як у звичайних умовах, так і під час особливого періоду чи запровадження в державі надзвичайного стану.

Так Управлянням інформаційно – аналітичної підтримки Головного управління Національної поліції в Донецькій області створено ряд умов запобігання від загроз зовнішнього та внутрішнього периметру.

Для зниження ризиків компрометації критично важливих систем з боку зовнішніх порушників особлива увага приділяється ресурсам, доступним із зовнішніх мереж. Як показує практика, переважна більшість успішних атак засновані на експлуатації вразливостей не на неофіційних сайтів організацій та їх серверів, а будь-яких інших ресурсів компанії, які не повинні бути доступні на мережевому рівні.

Для захисту мережі Інтернет від атак на веб-додатки застосовуються міжмережеві екрани, а саме міжмережевий екран FortiGate, який забезпечує максимальний захист як проти мережевих загроз, так і проти загроз прикладного рівня, з ефективними настройками правил кореляції. Для контролю за ресурсами на мережевому периметрі забезпечуються регулярні сканування ресурсів, доступних з зовнішніх мереж.

Що стосується захисту відомчої мережі від атак з боку внутрішнього порушника, ведеться парольна політика, яка забороняє використання простих паролів, а також існують вимоги до регулярної зміни паролів (раз в 30 днів). Також необхідно звернути особливу увагу на застарілі версії ПЗ, на відкриті протоколи передачі даних і на зберігання важливої інформації у відкритому вигляді на серверах і робочих станціях співробітників. Крім базових заходів захисту інформації, на регулярній основі проводиться аудит безпеки інформаційних систем і тестування на проникнення з боку зовнішнього і внутрішнього порушника, а ради захисту персональних станцій співробітників поліції встановлюється якісний продукт ESET Endpoint Security та набори додатків до веб браузерів, наприклад AdGuard та захисту з'ємних носіїв, наприклад USB Protection & Recovery.

УІАП ГУНП в Донецькій області постійно ведеться оновлення застарілих версій ПЗ на актуальні.

Доцільним є питання поширення ноутбуків, нетбуків та планшетних комп'ютерів, що надало можливість користувачам працювати з інформацією не тільки безпосередньо на робочому місці, а і під час поїздок, командировок тощо. Але треба зазначити, що це дає не тільки можливості, а і породжую небезпеки. Однією з таких небезпек є втрата ноутбуку (нетбуку, планшетного комп'ютера), або його крадіжка. Якщо здійснити пошук в Інтернет, то ми легко знайдемо багато прикладів коли таким чином втрачалася вважлива та конфіденційна інформація. Основним завданням безпеки роботи з інформацією є, все ж таки, не збереження пристрою, а саме захист цієї інформації. Нажаль жоден з методів на забезпечує захист інформації у одному дуже простому випадку – коли зловмисник просто виймає жорсткий диск, або інший носій що використовується для збереження інформації і приєднує його до власного комп'ютера для отримання доступу до інформації. Якщо не зробити дій для шифрування інформації, то вся інформація буде доступна зловмиснику у відкритому вигляді тому. УІАП ГУНП в Донецькій області рекомендує проводити шифрування інформації. Якщо застосувати цей надійний метод захисту інформації у разі використання з'ємних носіїв немає можливості, то слід скористатися створенням зашифрованого розділу або зашифрованого віртуального диску. Єдине що можна зауважити, що для з'ємного носія краще скористатися варіантом створення зашифрованого розділу.

Існують ряд недоліків у використанні точок доступу і клієнтських пристроїв Wi-Fi, а також недоліків в архітектурі та організації бездротового доступу. Серед недоліків варто відзначити використання механізму WPS для спрощення процесу налаштування бездротової мережі. Для підключення до точки доступу використовується спеціальний PIN-код, що складається тільки з цифр. Порушник може підібрати PIN-код і підключитися до точки доступу, саме тому ГУНП в Донецькій області не використовує пристрої Wi-Fi.

УІАП ГУНП в Донецькій області постійно проводить аудит своїх систем а мереж на скомпроментрованість та її можливість такої бути, що надавало та надає певні привілеї до нових видів загроз.

Ткачук Т.Ю.,
кандидат юридичних наук, доцент,
заступник завідувача кафедри
організації захисту інформації з
обмеженим доступом
Навчально-наукового інституту
інформаційної безпеки
Національної академії Служби безпеки
України

ІНФОРМАЦІЙНИЙ ЧИННИК У ГІБРИДНІЙ ВІЙНІ

Цитуючи слова військового стратега Карла фон Клаузевіца, що *війна є продовженням політики іншими засобами* ця формула є прийнятною для будь-якої, у т.ч. гібридної, війни (*hybrid warfare*). Досить логічним продовженням цієї дуки є твердження генерал-майора у відставці, члена верхньої палати парламенту Нідерландів Франка ван Каппена про те, що держава, яка веде гібридну війну, укладає оборудку з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими формально повністю заперечується. Ці виконавці можуть робити такі речі, які сама держава робити не може, тому що будь-яка держава зобов'язана дотримуватися Женевської та Гаазької конвенцій про закони сухопутної війни, домовленості з іншими країнами.

Змістовні особливості гібридної війни були закладені ще у 1989 році американським експертом Вільямом Ліндом у теорії війн четвертого покоління[1]. Ідея «війни четвертого покоління» зародилася у часи Холодної війни, коли наддержавам в ході боротьби за свою присутність у різних точках світу стало зрозуміло, що широкомасштабне застосування танків, авіації і ракет в цих умовах малоефективне, і що роль партизанських і різних політичних, економічних, фінансових, а, особливо, інформаційних та психологічних підривних операцій кардинально зросла.

Важливим фактором гібридної війни є використання невійськових методів тиску на противника, передусім через політичний, економічний і гуманітарний елементи. Найактуальнішим сегментом такої війни є інформаційний вплив «на об'єкт нападу». Інформаційна складова «гібридної війни», за визначенням В. Горбуліна, структурується на кілька сегментів. Інформаційні атаки ведуться: «(1) серед населення в зоні конфлікту; (2) серед населення країни, проти якої здійснюється агресія, однак територія якої не охоплена конфліктом; (3) серед

[1] (англ. *Fourth generation warfare (4GW)*) — конфлікт, який характеризується стиранням відмінностей між безпосередньо війною і політикою, між залученими в неї військовими і цивільним населенням.

громадян країни агресора; (4) серед міжнародного співтовариства» [1, с. 10]. Як бачимо, інформаційний фронт охопив всю Україну та вийшов далеко за її межі. До того, ж, розпочалася ця війна задовго до подій 2014 р. Складовою частиною війни став, крім іншого, релігійний фактор, який виступає одним із потужних інструментів інформаційного чиннику гібридної війни. Як стверджує Н. Кочан, релігійний чинник суттєво вплинув на підготовку, розв'язання й ведення військової агресії РФ. Більше того, після переходу війни з «гарячої» у «холодну» фазу, його роль як складової гібридної війни, відіграватиме не менш важливу та помітну роль [2, с. 71]. Тому вивчення цієї проблеми набуває ще більшої актуальності в умовах стрімкої зміни інформаційних потоків та масованої пропагандистської навали з боку країни-агресора. Тим паче, що «гібридна війна пов'язана не стільки з окупацією території противника, скільки з прагненням підірвати структуру його управління зсередини, зруйнувати інфраструктуру, придушити волю до опору» [3, с. 4].

Інформаційна боротьба здійснюється протягом усієї «гібридної війни», починаючись задовго до її «гарячої» фази. В основі цієї боротьби лежить теорія симулякрів Жака Бодрйіяра. Ж. Бодрійяр позначає поняттям «симулякр» «імітацію і заміну реального, одиницю підробленого сенсу, ірреферентний знак» [4, с. 46]. При цьому він наділяє симулякри такими властивостями як: виробництво реального знаками гіперреального; перетворення реальності в гіперреальність; антиципація подій; ірреферентність; вибух, що спрямований всередину, і нерозрізнюваність складових опозиційної пари. Яскравими прикладами симулякрів є «плата двома рабами», «розіп'ятий хлопчик», «візитка Яроша» тощо.

Оперуючи наведеними фактами можна констатувати надважливий вплив інформаційного чинника, а зрештою й інформаційної безпеки, на національну безпеку держави в цілому. При цьому, зауважимо, що основними рушійними силами системи національної безпеки є національні цінності, інтереси і цілі – зазначені елементи визначають зміст, характер, конфігурацію та спрямованість системи. З урахуванням того, що пріоритетність того або іншого виду національної безпеки визначається об'єктивними факторами: ступенем потреби людей, соціальних груп, суспільства, держав, світового співтовариства у безпеці для збереження й розвитку себе, а також життєво важливих об'єктів і цінностей (природних і соціальних); зростаючою уразливістю людей і життєво важливих об'єктів і цінностей (природних і соціальних) без зосередження зусиль на зміцненні безпеки; наявністю широкого кола надзвичайних небезпек, яким повинна протистояти система безпеки, – інформаційна безпека закономірно виходить на перший план у системі національної безпеки.

Отже, з урахуванням викладеного, інформаційну безпеку держави слід визначати як постійний процес діяльності компетентних органів, направлений на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Оскільки

під дією інформаційних впливів може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуватися чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [5], інформаційна безпека держави включає в себе не тільки захист, а й вміння та здатність створювати інформаційні загрози противнику. На нашу думку, таке визначення базується на комплексному функціональному визначенні національної безпеки та врахуванні особливостей інформаційної сфери, а також акцентує увагу не лише на пасивній (протидія інформаційним загрозам) [6], але й на активній складовій (створення інформаційних загроз) інформаційної безпеки. Останнє є особливо актуальним у світлі завдань, визначених Стратегією національної безпеки, щодо протидії інформаційній війні, що ведеться проти України [7].

Створення належних умов для реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України, гарантування безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз у всіх сферах життєдіяльності, потребує формування сучасних ефективних механізмів забезпечення національної безпеки держави, які відповідатимуть характеру і масштабам викликів сьогодення. Складна воєнно-політична, оперативно-стратегічна та економічна ситуація, яка склалася внаслідок збройної агресії Росії проти України, окупації і анексії частини суверенної території України, проведенням антитерористичної операції в окремих регіонах Донецької та Луганської областей, де триває інспірований та підтриманий Російською Федерацією збройний конфлікт, набуває загрозливих проявів також у інформаційному просторі. У сукупності зі стратегічним значенням інформаційної сфери для сталого розвитку сучасного суспільства це зумовлює пріоритетний характер інформаційної безпеки у системі національної безпеки України. Відповідно, надзвичайно важливим є вірне усвідомлення змісту категорії «інформаційна безпека», яке неможливе без її визначення. То ж проаналізувавши різні підходи до визначення категорії «інформаційна безпека», які дають можливість зрозуміти це явище комплексно і системно, пропонуємо розглядати інформаційну безпеку як постійний процес діяльності компетентних органів, направлений на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час.

Список використаних джерел

1. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу // Стратегічні пріоритети. – 2014. – № 4(33). – С. 9-12.

2. Кочан Н. Деякі особливості використання релігійного чинника в гібридній війні Російської Федерації на Сході України // Культурні цінності Криму і Донбасу в умовах війни та окупації: Матер. круглого столу «Історико-

культурний та науковий потенціал Півдня та Сходу України в умовах окупації та воєнних дій: загрози, втрати, перспективи збереження», Київ, 12 листопада 2015. – К.: І-тут історії України НАНУ, 2016. – С. 70-73.

3. Магда Є. Гібридна війна: вижити і перемогти / Є. Магда. – Х.: Віват, 2015. – 304 с.

4. Бодрийяр Ж. Симулякры и симуляция / Жан Бодрийяр ; [пер. с фр.О. А. Печенкина]. – Тула : Тульский полиграфист, 2013. – 204 с.

5. Шамрай В.О. Інформаційна безпека як складова національної безпеки України/ В.Шамрай. – 12.06.2016 [Електронний ресурс]. – Режим доступу: http:// www.crime-research.org/ articles.html

6. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України/ О.Довгань// Інформаційна безпека людини, суспільства, держави. – 2015, № 3 (19). – С. 6-17.

7. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287/2015 – 28.07.2017 [Електронний ресурс]. – Режим доступу: www.rada.gov.ua

Пальчик М.Л.,
кандидат юридичних наук,
провідний науковий співробітник науково-організаційного центра
Національної академії Служби безпеки України

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК ПРИНЦИП ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Сфера персональних даних та їх захисту є актуальною в повсякденному житті для кожного із нас. А нещодавні події навколо соціальної мережі Facebook, яка не змогла забезпечити належного захисту персональних даних, внаслідок чого дані близько 2,7 млн мешканців Європейського союзу були незаконно передані британській компанії Cambridge Analytica, ще раз підтвердили крайню уразливість та фактичну незахищеність основоположного права на недоторканість приватного життя.

Законом України «Про основні засади забезпечення кібербезпеки України» встановлено, що забезпечення захисту прав користувачів комунікаційних систем та споживачів послуг електронних комунікацій щодо захисту персональних даних, є одним із принципів застосування законодавства у сфері кібербезпеки та прийняття рішень суб'єктами владних повноважень.

Визначений принцип забезпечення кібербезпеки реалізується в межах правового регулювання захисту персональних даних. Зазначимо, що основоположним нормативним актом у сфері захисту персональних даних є Закон України «Про захист персональних даних», який створено на основі положень Директиви 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. Вказаний нормативно-правовий акт встановлює досить детальні

вимоги щодо організації загальнодержавної системи захисту персональних даних.

Водночас, незважаючи на детальну регламентацію Уповноважений Верховної Ради України з прав людини, який здійснює Парламентський контроль за дотриманням законодавства про захист персональних даних у сфері кібербезпеки, констатує відсутність змін на краще ситуації навколо оброки персональних даних.

Основними підставами, що призводять до порушень у сфері оброки та захисту персональних даних є недотримання законодавства про захист персональних даних, його нерозуміння і неправильне застосування володільцями та розпорядниками персональних даних.

За результатами аналізу щорічних доповідей Уповноваженого з прав людини можна стверджувати, що основними порушеннями принципу захисту персональних даних є: порушення при отриманні згоди на обробку персональних даних; порушення права особи на доступ інформації про неї; порушення поширення персональних даних.

Підсумовуючи викладене вище можемо зазначити, що принцип захисту персональних даних фактично є правозастосовним принципом, що слугує відповідним орієнтиром реалізації правових основ забезпечення кібербезпеки. Він реалізується в межах правового регулювання захисту персональних даних і є критерієм правомірності діяльності суб'єктів відносин, пов'язаних із персональними даними, зокрема володільців та розпорядників персональних даних. Основні повноваження щодо контролю над дотриманням права на захист персональних даних як принципу забезпечення кібербпезпеки покладено на Уповноваженого Верховної Ради України з прав людини, яким констатується системність недотримання принципу захисту персональних даних через низку комплексних порушень, що допускаються володільцями та розпорядниками персональних даних.

Неласа Г.В.,
кандидат технічних наук, доцент,
доцент кафедри захисту інформації,
Запорізького національного технічного університету
Козіна Г.Л.,
кандидат фізико-математичних наук,
доцент кафедри захисту інформації
Запорізького національного технічного університету

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СХЕМ ЦИФРОВОГО ПІДПИСУ

Одна з особливостей сучасного етапу розвитку систем електронного документообігу полягає в тому, що існуючі системи підтримують лише двоточковий варіант протоколу електронного цифрового підпису, до якого прив'язаний і український стандарт ДСТУ 4145 – 2002 [1].

Однак існує велика кількість різних схем електронного цифрового підпису, що допускають участь у протоколі більше двох сторін [2]. На практиці часто виникає необхідність мати колективний підпис. Колективний підпис [3] дозволяє відмовитися від використання кратного підпису при одноразовому підписанні документа групою відповідальних осіб. Концепція групового підпису [4] реалізує метод, що дозволяє членам групи анонімно підписати повідомлення від імені всієї групи. Кільцевий підпис [5] уможливлює специфікувати набір можливих осіб, що підписують, без викриття, хто саме з них дійсно зробив підписання. Схема підпису із призначеним одержувачем [6] – це схема підпису, де підпис може бути перевірений тільки єдиним «призначеним одержувачем», обраним підписувачем. Незаперечний цифровий підпис [7] може бути перевірений тільки в присутності підписувача. Схема підпису на ідентифікаторах [8] дозволяє будь-якій парі користувачів перевіряти підпис один одного без обміну особистими або відкритими ключами, без зберігання ключів у каталогах, без використання послуг третьої сторони. Сліпий електронний підпис [9] запропоновано для захисту від підробки електронних грошей. За допомогою використання так званого «цифрового конверта» у такій системі одночасно з рішенням задач ідентифікації, автентифікації й авторизації претендента вирішена задача забезпечення анонімності останнього, інакше кажучи, невідстежуваності електронних документів, зокрема електронних грошей. В схемі мультипідпису із груповою перевіркою чинності можливо перевіряти цифрові мультипідписи із використанням лише однієї перевірки замість декількох [10]. Схеми розподілення секрету [11] дозволяють розділити секрет проміж групи учасників, кожен з яких володіє тільки своєю часткою секрету. Секрет може бути відтворений тільки за умови одночасної присутності всіх або певної кількості учасників протоколу.

На сьогодні в Україні прийнято низку стандартів на криптографічні алгоритми серед яких, окрім стандарту цифрового підпису [1], прийняті стандарт на алгоритм симетричного блокового перетворення ДСТУ 7624:2014 та стандарт на функцію гешування ДСТУ 7564-2014. Однак, незважаючи на те, що розглянуті схеми цифрового підпису [3-11] мають вже поважний вік, їх математичний апарат та доказ криптографічної стійкості є недостатньо опрацьованими для прийняття відповідних державних стандартів, що надає широке поле для наукових досліджень.

В доповіді висвітлюються особливості використання схем цифрового підпису різного призначення на практиці. Аналізуються можливі варіанти архітектури програмного забезпечення для реалізації розглянутих схем. Напрямком подальших досліджень є аналіз математичного апарату та криптографічної стійкості розглянутих схем цифрового підпису, пошук можливих областей використання та розробка відповідного програмного забезпечення.

Список використаних джерел

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

2. Козіна Г.Л. Криптопротоколи: схеми цифрового підпису : навч. посіб. / Г.Л. Козіна, М. А. Молдов'ян, Г. В. Неласа. – Запоріжжя : ЗНТУ, 2014. – 158 с.

3. Способ генерации и проверки подлинности электронной цифровой подписи, заверяющей электронный документ / А. А. Молдовян, Н. А. Молдовян. Пат. заявка № 2007130982, 13.08.2007.

4. Chaum D. (1991). Group signatures / D. Chaum, E. van Heyst // Advances in Cryptology, EUROCRYPT'91. – 1991. – volume 547 of Lecture Notes in Computer Science. – P. 257-265.

5. Rivest R. How to leak a secret [Електронний ресурс]/ R. Rivest, A. Shamir, Y. Tauman . – 2001. – 13 с. – Режим доступу: http://people.csail.mit.edu/rivest/RivestShamirTauman-HowToLeakASecret.pdf.

6. Jakobsson M. Designated Verifier Proofs and their Applications [Электронный ресурс] / M. Jakobsson, K. Sako, R. Impagliazzo // Proc. of Eurocrypt'96, Springer LNCS. – 1996. – Vol. 1070. – P. 142–154. – Режим доступу: http://www.informatics.indiana.edu/markus/dvp.pdf.

7. Chaum D. Undeniable signatures / D. Chaum, H. van Antwerpen // CRYPTO'89, LNCS 435. – Springer-Verlag. – 1989. – P. 212-216.

8. Adi Shamir, Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7, 1984. – P. 47 – 53.

9. Chaum D. Blind signatures for untraceable payments / D. Chaum // Advances in Cryptology, Crypto '82. – Springer-Verlag. – 1983. – P. 199-203.

10. Hawng M. Research issues and challenges for multiple digital signature / M. Hawng, C. Le // International Journal of Network Security. – 2005. – Vol. 1. – No 1. – P. 1-7.

11. Shamir A. How To Share a Secret / A. Shamir // Comm. ACM. –1979. – Vol. 22. – P. 612–613.

Івохін Є.В.,
доктор фізико-математичних наук,
професор, професор кафедри системного аналізу
Київського національного університету імені Тараса Шевченка

ДОСЛІДЖЕННЯ ПРОЦЕСІВ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ НА ОСНОВІ ГІБРИДНИХ ДИФУЗІЙНИХ МОДЕЛЕЙ

Сучасні інформаційні потоки, котрі розраховані на конкретного споживача, мають, як правило, чітко визначену предметну або цільову

спрямованість, що характеризується областю інтересів людини. Для дослідження впливу інформації на соціум потрібно використовувати принципово новий інструментарій, який здатний адекватно відображати стан динамічної складової процесу розповсюдження інформації [1]. При цьому, розробка нових підходів не відміняє методики застосовування класичних способів аналізу та обробки інформаційних процесів, що реалізується у вигляді механістичного підходу та методів біоаналогій.

В рамках даного підходу розглянемо один з варіантів формалізації процесів розповсюдження інформації. Позначимо через $u(x,t)$ функцію рівня розповсюдження інформації в межах визначеної частки x, $0 \le x \le 1$, групи населення, обсяг якої не перевищує наперед заданої величини A.

Будемо моделювати зміну рівня (концентрації) інформації у соціальній або регіональній групі населення за допомогою рівняння дифузії [2]. Цей процес аналогічний розповсюдженню деякої речовини протягом конкретного часового інтервалу $t \in [0,T]$ і може бути описаний скалярним рівнянням:

$$\partial u / \partial t = -k(t) \partial^2 u / \partial x^2 , \qquad (1)$$

з початковою умовою $u(x,0) = 0$, $0 \le x \le 1$, та крайовою умовою $u(0,t) = 0$, $t \in [0,T]$, де $k(t)$ - коефіцієнт, що характеризує швидкість проникнення інформації (аналог коефіцієнта дифузії) і є пропорційним швидкості зміни частки населення, яка вважається чутливою до впливу зовнішньої інформації.

Склад населення розбивається на 3 підгрупи: частка чутливих до впливу інформації y_1, частка тих, що вже знаходяться під впливом інформації y_2, і частка байдужих до інформаційного впливу y_3. На основі моделі Кермана-Маккендріка [3] можна записати систему диференціальних рівнянь, що описує процес розповсюдження інформації у загальній групі населення, а її розв'язки, відповідно, визначають величини часток окремих підгруп:

$$\begin{aligned} \dot{y}_1(t) &= -y_1(t) y_2(t), \\ \dot{y}_2(t) &= y_1(t) y_2(t) - y_2(t), \\ \dot{y}_3(t) &= y_2(t), \end{aligned} \qquad (2)$$

з початковими умовами $y_1(0) = y_2(0) = 0; y_3(0) = 1$.

За таких припущень граничне значення частки населення, що відчуває вплив інформації, x_Γ, $0 \le x_\Gamma(t) \le 1$, буде залежати від часу, тобто маємо $0 \le x \le x_\Gamma(t)$, $x_\Gamma(t) = (y_1(t) + y_2(t))/A$, $y_1(t), y_2(t)$ - компоненти розв'язку системи (2). Крім цього, можна покласти $k(t) = \mu \dot{x}(t)$.

Шукаємо функцію $u(x,t)$ у вигляді $u(x,t) = X(x(t))$. Тоді для будь-якого моменту часу $t \in [0,T]$ отримуємо розв'язок рівняння (1) $u(x,t) = \mu(1 - e^{-x(t)/\mu})$, що визначає рівень розповсюдження інформації в межах підгрупи, частка якої складає $x_\Gamma(t)$ від загальної кількості A, $0 \le x(t) \le x_\Gamma(t)$.

Цей розв'язок може бути узагальнений за умов припущення, що частина населення, яка має імунітет до впливу інформації, може через деякий час його

втратити. Частина населення при цьому стає чутливою до впливу інформації, збільшуючи групу $y_1(t)$, і процес періодично повторюється.

Розглянемо процес розповсюдження інформації на базі дифузійного підходу з двовимірним (площинним) поданням групового контингенту. Припустимо, що існують два різні типи споживачів інформації, що відрізняються сприйняттям зовнішнього інформаційного впливу та своїм ставленням до змісту інформаційних потоків. Подібне припущення абсолютно коректно вписується в рамки викладеного вище підходу, який базується на представленні контингенту споживачів у формі трьох окремих за ставленням до інформаційного впливу підгруп.

У цьому випадку просторові координати x_1, x_2 будуть використовуватися для позначення частин споживачів інформації, які є чутливими до впливу зовнішньої інформації. Сформулюємо модель на основі рівняння дифузії (3), описуючи за допомогою функції $u(x_1, x_2, t)$, $t \geq 0$, рівні розповсюдження і сприйняття інформації в межах двох підгруп, що сприймають її вплив. Будемо шукати функцію $u(x_1, x_2, t)$ у вигляді $u(x_1, x_2, t) = =(X_1(x_1(t)) + X_2(x_2(t)))/2$. Граничні величини $x_1^{\Gamma}(t)$, $x_2^{\Gamma}(t)$ часток населення, в межах яких враховується розповсюдження інформації, визначатимемо на основі компонент $y_1(t), y_2(t)$ розв'язку системи (1): $0 \leq x_1(t) \leq x_1^{\Gamma}(t)$, $0 \leq x_2(t) \leq x_2^{\Gamma}(t)$, $x_1^{\Gamma}(t) = y_1(t)$, $x_2^{\Gamma}(t) = y_2(t)$, а коефіцієнт, що характеризує швидкість проникнення інформації, вважаємо однорідно пропорційним швидкостям змін обсягів підгруп, тобто $k(t) = \mu \dot{x}_1(t) = \mu \dot{x}_2(t)$.

Тоді для довільного моменту часу $t \in [0, T]$ отримаємо розв'язок дифузійного рівняння (1):

$$u(x_1, x_2, t) = 0.5\mu((1 - e^{-x_1(t)/\mu}) + (1 - e^{-x_2(t)/\mu})), \qquad (3)$$

яке дозволяє визначити рівень проникнення інформації в межах чутливих до впливу підгруп, чисельність яких задається величинами часток $x_{\Gamma}^1(t)$, $x_{\Gamma}^2(t)$ від загальної кількості населення.

Розглянемо також альтернативний варіант моделі розповсюдження інформаційних процесів. Позначимо $y_1(t)$ - частка населення, що сприймає вплив інформації, $y_2(t)$ - частка тих, хто вже знаходиться під інформаційним впливом. Динаміка процесу зміни величин цих груп описується першим та другим рівняннями системи (2). Рівні розповсюдження інформації можна формалізувати за допомогою вектор-функції $u(x_1, x_2, t) = =(u_1(x_1, t), u_2(x_2, t))^T$, де функції $u_1(x_1, t)$, $u_2(x_2, t)$, $0 \leq u_i(x_i, t) \leq 1$, $i = 1,2$, $t \geq 0$, визначають інформаційний вплив у середовищі категорій $y_1(t)$, $y_2(t)$ відповідно та задовольняють скалярним дифузійним рівнянням $\partial u_i(x_i, t) / \partial t = -k_i(t) \partial^2 u_i(x_i, t) / \partial x_i^2$, $i = 1,2$, з функціями $k_i(t)$, $i = 1,2$, - що визначають швидкості проникнення інформації в межах розглянутих груп (як і раніше, вважаємо їх пропорційними швидкостям зміни конкретних частин населення з коефіцієнтами пропорційності μ_i, $i = 1,2$).

Максимальні граничні величини $x_1^{\Gamma}(t)$, $x_2^{\Gamma}(t)$ частин населення, в межах яких можливе розповсюдження інформації, визначаються на основі компонент $y_1(t), y_2(t)$: $0 \le x_1(t) \le x_1^{\Gamma}(t)$, $0 \le x_2(t) \le x_2^{\Gamma}(t)$, $x_1^{\Gamma}(t) = y_1(t)$, $x_2^{\Gamma}(t) = y_2(t)$. Повторюючи викладки, проведені для скалярного випадку, отримуємо розв'язок $u(x_1, x_2, t)$ з компонентами вигляду $u_i(x_i, t) = \mu_i(1 - e^{-x_i(t)/\mu_i})$, $i = 1,2$, що задають розповсюдження інформації на основі гібридного дифузійного підходу.

В якості іншої цікавої моделі, що дозволяє вивчати розповсюдження інформаційних потоків на основі гібридних процесів, можна розглядати модель на основі використання опису процесів кінетики хімічних реакцій, в яких каталізатором служить фермент (ензим). Характерним проявом життєвої активності організмів є їх здатність кінетично регулювати хімічні реакції, пригнічуючи прагнення до досягнення термодинамічної рівноваги. Ферментативна кінетика займається дослідженням закономірностей впливу хімічної природи реагуючих речовин (ферментів, субстратів) і умов їх взаємодії (концентрації, температури, присутність інгібіторів) на швидкість ферментативної реакції. Головною метою вивчення кінетики ферментативних реакцій є отримання інформації, яка може сприяти з'ясуванню молекулярного механізму дії ферменту.

Якщо розглянути ланцюг реакцій вигляду $I \to z_1 \underset{\gamma}{\to} z_2 \to z_3 \to z_4 \to$

$\uparrow$_____$\downarrow$

де I - зовнішній субстрат, запас якого підтримується постійним, спільна дія кінцевого продукту $z_4(t)$ пригнічує (затримує перебіг ферментативного процесу) стадію реакції $z_1 \to z_2$, так, що величина її швидкості має вигляд $\gamma = 1/(1 + \alpha(z_4(t))^2)$.

Вважається, що молекули інгібітора переміщаються в місце розташування регулюючого ензиму шляхом процесу дифузії, що дозволяє отримати математичну модель процесу у вигляді [4]:

$$\begin{aligned} z_1(t) &= I - \gamma z_1(t), \\ z_2(t) &= \gamma z_1(t) - z_2(t), \\ z_3(t) &= z_2(t) - z_3(t), \\ z_4(t) &= z_3(t) - z_4(t)/2. \end{aligned} \qquad (4)$$

У цьому випадку можна провести аналогію між процесом кінетики даної реакції та процесом розповсюдження інформації, в якому величини $z_1(t)$, $z_2(t)$, $z_3(t)$, $z_4(t)$ будуть асоціюватися с частинами деякої популяції заданого обсягу $I = 1$ і які описують пропорційні складові на різних стадіях процесу проникнення.

І, нарешті, окремої уваги заслуговує випадок врахування у дифузійній моделі агентів (нонкомформістів) [5]. Наявність у цільовій групі населення частини нонконформістів може радикально змінити процес розповсюдження інформації. Формально його схема залишається аналогічною описаній вище, однак поведінка агентів передбачає стійкий імунітет до інформаційного впливу

(ігнорування будь-яких нових ідей, крім визначених) з можливістю передачі суб'єктивної інформації у процесі розповсюдження інформаційного потоку в межах популяції. При цьому дифузійна модель ускладнюється, потребує розгляду і врахування додаткових факторів, що впливають на динаміку процесу. Одним з варіантів подальших досліджень у цьому напрямку може бути запропоновано залстосування для формалізації, наприклад, автоматних реалізацій.

Висновки. Моделі на основі рівняння дифузії для дослідження розповсюдження інформації були використані в процесах вивчення і оптимізації потоків рекламної інформації. Дифузійна модель впливу реклами розглядалась також з урахуванням показників динаміки товарів, одержуваних на основі статистичних звітів за результатами діяльності торгових підприємств. Аналіз результатів процесів впливу рекламної інформації на основі запропонованого походу і проведених числових експериментів дозволив зробити висновок про адекватність отриманих розрахунків параметрам реальних процесів зміни рівнів сприйняття інформації в межах конкретно заданих груп населення, що мають місце внаслідок зовнішнього інформаційного впливу.

Список використаних джерел

1. Брайчевський С.М. Сучасні інформаційні потоки: актуальна проблематика /С.М. Брайчевський, Д.В. Ланде //Науково-технічна інформація. – Сер.1. – Вип.11. – 2005. – С. 21-33.
2. Араманович И.Г. Уравнения математической физики / И.Г.Араманович, В.И. Левин. – М.: Наука, 1969. - 288 с.
3. Kermack W. O. A Contribution to the Mathematical Theory of Epidemics / W. O. Kermack, A. G. McKendrick // Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character, 1927. – Vol. 115. – Iss.772. – P.700-721.
4. Хайрер Э. Решение обыкновенных дифференциальных уравнений / Э.Хайрер, С. Нерсетт, Г.Ваннер. –М: Мир, 1990.-512 с.
5. Федотов А.М. Модель самоорганизации в агентных системах с передачей сообщений/ А.М.Федотов, С.Г.Ломакин // Математическое моделирование и вычислительно-информационные технологии в междисциплинарных научных исследованиях: Материалы IV Всероссийской конференции. - 2014. - Иркутск: Институт динамики и теории управления СО РАН. - С.42.

Нікітін А.В.,
кандидат фізико-математичних наук, доцент,
доцент кафедри математичної і прикладної статистики
Київського національного університету імені Тараса Шевченка

АНАЛІЗ МАТЕМАТИЧНОЇ МОДЕЛІ РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ ІЗ ЗОВНІШНІМ ІМПУЛЬСНИМ ВПЛИВОМ

З технологічним розвитком суспільства, дедалі більшої ваги набуває можливість інформаційного впливу на соціальні спільноти. З кінця XX століття низка провідних науковців з різних країн вважають поширення інформації однією з провідних ролей у внутрішніх та зовнішніх соціально-економічних процесах. З'явились публікації, які описують процес поширення інформації, можливості використання її у власних інтересах, як для поширення «потрібної» інформації, так і для протидії небажаним тенденціям у суспільстві. Надзвичайно важливим питанням, що виникли для даної сфери, є побудова та системний аналіз математичних моделей, які б адекватно описували цей процес. Перспективним напрямком для даної проблематики є математичні моделі, записані у вигляді стохастичних еволюційних рівнянь з імпульсним впливом.

Основні положення. Стохастична еволюційна система в ергодичному марковському середовищі задається стохастичним диференційним рівнянням [4]

$$du^{\varepsilon}(t) = C(u^{\varepsilon}(t), x(t/\varepsilon^2))dt + d\eta^{\varepsilon}(t), \quad u^{\varepsilon}(t) \in \mathrm{R} \tag{1}$$

де $u^{\varepsilon}(t)$ – випадкова еволюція, $t \geq 0$;

$\varepsilon > 0$ – малий параметр серій;

$C(u,\cdot) \in C^2(\mathrm{R}^d)$ – функція регресії;

$x(t)$ – рівномірно ергодичний марковський процес у стандартному фазовому просторі $(X, \mathbf{X})$, який визначений генератором [2]

$$\mathbf{Q}\varphi(x) = q(x)\int_X P(x,dy)[\varphi(y) - \varphi(x)], \tag{2}$$

на банаховому просторі $B(X)$ дійснозначних обмежених функцій $\varphi(x)$ з супремум-нормою $\|\varphi\| = \sup_{x \in X} |\varphi(x)|$ [3].

Стохастичне ядро $P(x,B)$, $x \in X$, $B \in \mathbf{X}$, визначає рівномірно ергодичний вкладений ланцюг Маркова $x_n = x(\tau_n)$, $n \geq 0$, зі стаціонарним розподілом $\rho(B)$, $B \in \mathbf{X}$. Стаціонарний розподіл $\pi(B)$, $B \in \mathbf{X}$, марковського процесу $x(t), t \geq 0$ визначається співвідношенням [3]

$$\pi(dx)q(x) = q\rho(dx), \; q = \int_X \pi(dx)q(x).$$

Позначимо R_0 – потенціальний оператор генератора $\mathbf{Q}$, який визначається рівністю [3]: $R_0 = \Pi - (\Pi + \mathbf{Q})^{-1}$, де $\Pi\varphi(x) = \int_X \pi(dy)\varphi(y)\mathbf{1}(x)$ – проектор на підпростір $N_Q = \{\varphi : \mathbf{Q}\varphi = 0\}$ нулів оператора $\mathbf{Q}$.

Імпульсный процес збурень $\eta^\varepsilon(t),\ t \ge 0$, у схемі апроксимації Леві визначається співвідношенням

$$\eta^\varepsilon(\mathrm{t}) = \int_0^t \eta^\varepsilon(ds, x(s/\varepsilon^2)); \tag{2}$$

де сукупність процесів з незалежними приростами $\eta^\varepsilon(t,x), t \ge 0, x \in X$, визначається генераторами

$$\mathbf{\Gamma}^\varepsilon(x)\varphi(\omega) = \varepsilon^{-2}\int_R (\varphi(\omega+v) - \varphi(\omega))\Gamma^\varepsilon(dv, x), x \in X \tag{3}$$

та задовольняють умовам апроксимації Леві:

L1: *Апроксимація середніх:*

$$\int_R \mathrm{v}\,\Gamma^\varepsilon(d\,\mathrm{v}, x) = \varepsilon a_1(x) + \varepsilon^2(a_2(x) + \theta_a(x)),\ \theta_a(x) \to 0, \varepsilon \to 0,$$

та

$$\int_R \mathrm{v}^2\,\Gamma^\varepsilon(d\,\mathrm{v}, x) = \varepsilon^2(b(x) + \theta_b(x)),\ \theta_b(x) \to 0, \varepsilon \to 0.$$

L2: *Умова на функцію розподілу:*

$$\int_R g(\mathrm{v})\Gamma^\varepsilon(d\,\mathrm{v}, x) = \varepsilon^2(\Gamma_g(x) + \theta_g(x)),\ \theta_g(x) \to 0, \varepsilon \to 0$$

для всіх $g(\mathrm{v}) \in C_3(R)$ (простір дійснозначних обмежених функцій таких, що $g(\mathrm{v})/|\mathrm{v}|^2 \to 0, |\mathrm{v}| \to 0$). Тут міра $\Gamma_g(x)$ обмежена для всіх $g(\mathrm{v}) \in C^2(R)$ і визначається співвідношенням (функції з простору $C_3(R)$ розділяють міри [1])

$$\Gamma_g(x) = \int_R g(\mathrm{v})\Gamma_0(d\,\mathrm{v}, x),\ g(\mathrm{v}) \in C_3(R).$$

L3: *Рівномірна квадратична інтегровність:*

$$\lim_{c\to\infty} \int_{|\mathrm{v}|>c} \mathrm{v}^2\,\Gamma_0(d\,\mathrm{v}, x) = 0.$$

Модель (1) перепишемо у наступному вигляді

$$dL^\varepsilon(t) = C(L^\varepsilon(t), x(t/\varepsilon^2))dt + d\eta^\varepsilon(t) \tag{4}$$

Тут $C(L,x) = \alpha_1(x)L_0(x) + \alpha_2(x)L_0(x)L(t) - \alpha_2(x)L^2(t)$,

$\alpha_1(x) = \alpha_{11}(x)\alpha_{12}(x)$ – зовнішній канал;

$\alpha_2(x) = \alpha_{21}(x)\alpha_{22}(x)$ – внутрішній канал;

де $\alpha_{11} > 0$ $\alpha_{21} > 0$ – інтенсивність (число рівноцінних інформаційних контактів на одиницю часу ;

$\alpha_{12} > 0,\ \alpha_{22} > 0$ – ймовірність бути завербованим (схильність до сприйняття інформації).

$L(t)$ – число «завербованих» адептів;

$L_0(x) - L(t)$ – число ще не «завербованих» адептів;

$\eta^{\varepsilon}(t)$ моделює імпульсні впливи, це можуть бути, наприклад, чужі інформаційні канали, які з'являються на території спільноти;

Твердження1. *При виконанні умови балансу*

$$\hat{a}_1 := \int_X \pi(dx)\hat{a}_1(x) = 0 \ ,$$

справедлива слабка збіжність

$$L^{\varepsilon}(t) \to \hat{L}(t) \ , \ \varepsilon \to 0$$

Граничний процес визначається генератором

$$\mathbf{L}\varphi(w) = \hat{C}(L)\varphi'(w) + \Gamma\varphi(w)$$

де

$$\hat{C}(L) = \Pi\mathbf{C}(x) = \int_X \pi(dx)(\alpha_1(x)L_0(x) + \alpha_2(x)L_0(x)L(t) - \alpha_2(x)L^2(t))$$

$$\Gamma\varphi(\omega) = \hat{a}_2\varphi'(\omega) + \frac{1}{2}\sigma^2\varphi''(\omega) + \int_R [\varphi(\omega + \mathrm{v}) - \varphi(v)]\hat{\Gamma}_0(d\,\mathrm{v})$$

$$\hat{a}_2 = \int_X \pi(dx)(a_2(x) - a_0(x)), \qquad \sigma^2 = \int_X \pi(dx)(b(x) - b_0(x)) + 2\int_X \pi(dx)a_1(x)R_0a_1(x),$$

$$a_0(x) = \int_R \mathrm{v}\Gamma_0(d\,\mathrm{v}, x), \qquad b_0(x) = \int_R \mathrm{v}^2\Gamma_0(d\,\mathrm{v}, x), \ \hat{\Gamma}_0(\mathrm{v}) = \int_X \pi(dx)\Gamma_0(d\,\mathrm{v}, x)$$

$$V(L) \in C^3(\mathbf{R}^d)$$

Твердження2. *Нехай існує функція Ляпунова системи*

$$\frac{dL}{dt} = \beta(L)$$

де

$$\beta(L) = \hat{C}(L) + \hat{a} = \int_X \pi(dx)(\alpha_1(x)L_0(x) + \alpha_2(x)L_0(x)L(t) - \alpha_2(x)L^2(t)) + \hat{a}$$

яка задовольняє умовам

C1: $|\Gamma_L^1(x)R_0\hat{\mathrm{L}}V(L)| < \mathrm{M}_1V(L), \ M_1 > 0;$

C2: $|\Gamma_L^1(x)R_0\Gamma_L^1(x)V(L)| < \mathrm{M}_2V(L), \ M_2 > 0;$

C3: $|\Gamma_L^1(x)R_0\mathbf{C}(x)V(L)| < \mathrm{M}_3V(L), \ M_3 > 0;$

C4: $|\mathbf{C}(x)R_0\hat{\mathrm{L}}V(L)| < \mathrm{M}_4V(L), \ M_4 > 0;$

C5: $|\mathbf{C}(x)R_0\Gamma_L^1(x)V(L)| < \mathrm{M}_5V(L), \ M_5 > 0;$

C6: $|\mathbf{C}(x)R_0\mathbf{C}(x)V(L)| < \mathrm{M}_6V(L), \ M_6 > 0.$

Крім того, нехай виконуються нерівності

$$\alpha(L)V'(L) < -c_1V(L);$$

$$\sup_{y \in R^d} \| \sigma(y) \| < c_2(x);$$

$$|\int_R \mathrm{v}^2\Gamma_0(d\,\mathrm{v}, x)| < c_3(x);$$

де $c_1 > 0, c_2 > 0$ *та* $\hat{c}_3 = \int_X \pi(dx)c_3(x) > 0$

Тоді система (4) асимптотично дисипативна.

Твердження 1 демонструє поведінку схожих соціальних систем, які піддаються інформаційним впливам. Зрозуміло, що будуть флуктуації. Твердження 2 показує, чи буде система близька до усередненої. Даний підхід необхідно використовувати для побудови та системного аналізу більш загальних моделей інформаційного протистояння, а також для розробки алгоритмів знаходження гарантованих прогнозних оцінок для даної моделі при неповних спостереженнях.

Список використаних джерел

1.Jacod J. Limit theorems for stochastic processes / J. Jacod, A.N. Shiryaev // Springer-Verlag, Berlin. – 2003. – 601 p.

2.Korolyuk V.S. Stochastic Models of Systems / V.S. Korolyuk, V.V.Korolyuk // Kluwer, Dordrecht. – 1999. – 185 c.

3.Koroliuk V.S. Stochastic Systems in Merging Phase Space / V.S. Koroliuk, N. Limnios // World Scientific, Singapore, 2005. – 330 c.

4.Koroliuk V.S. Lévy and Poisson approximations of switched stochastic systems by a semimartingale approach / V.S. Koroliuk, N.Limnios, I.V. Samoilenko // Comptes Rendus Mathématique, 354, 2016, 723-728.

5.Samoilenko A.M. Qualitative and asymptotic analysis of differential equations with random perturbations / A.M. Samoilenko O.M. Stanzhytskyi // World Scientific, Singapore, 2011. - 323 p.

6. Nikitin A.V. Asymptotics of normalized control with Markov switchings / A.V. Nikitin, U.T. Khimka // Ukrainian Mathematical Journal, 2017, Vol.68, №8, P. 1252 – 1262.

7. Nikitin A.V. Asymptotic properties of a stochastic diffusion transfer process with an equilibrium point of a quality criterion / A.V. Nikitin // Cybernetics and Systems Analysis, 2015, Vol.51, №4, P. 650 – 656.

Kolyada Yu.,
Doctor of Physical and Mathematical Sciences, Professor
Mariupol State University

RISK ANALYSIS FOR THE PROTECTION OF INFORMATION ENTERPRISES ACTIVITIES

The assessment of risks to protect the information activities of the company is currently an urgent problem. The reason is that the sources of loss and leakage of information are difficult to identify, hidden objects and subjects from direct contact. As illegal sources of information leakage, we will consider some hidden factors. In this connection, for their establishment, it has been proposed to use a mathematical model based on a multivariate statistical analysis of seemingly chaotic observable values and the formation on their basis of a correlation matrix [1]. It is assumed that there is a multiple correlation between the observed values, which is due not only to their mutual relations, but also through invisible, hypothetical factors in the form of

sources of information leakage that cannot be directly observed and measured. In this case, it is necessary to identify and identify the sources of information leakage based on statistical observations. The number of factors can be much smaller than the number of observed values. This will make it possible to order the apparent chaos of the ongoing processes by compressing information and help to create a more adequate model of the phenomena and connections that take place in the system and better understand their essence. Production indicators are apparent chaotic observables, or variables.

The algorithm for processing variables was carried out in accordance with the methodology of factor analysis, described in [2]. In particular, the input data can be represented as a matrix of variables $Y = (y_{i,j})$, where $i = 1,2,...m$ refers to the production variables, and $j = 1,2,...n$ - to the units. Then the elements of the matrix Y must be transformed to standardized or normalized variables in the form of a matrix $Z = (z_{ij})$, the elements of which have the form: $z_{ij} = \frac{y_{ij} - \overline{y_i}}{s_i}$. Here $\overline{y_i} = \frac{1}{n}\sum_{j=1}^{n} y_{ij}$ and $s_i = \sqrt{\frac{1}{n-1}\sum_{j=1}^{n} (y_{ij} - \overline{y_i})^2}$ is the standard deviation. The purpose of any method of factor analysis is the representation of quantities z_{ij}, i.e. elements of the matrix Z, as a linear combination of several hypothetical variables, or factors. In our case, it can be assumed that hypothetical factors are represented as sources of information leakage, the number of which is equal to r.Then the following relation holds: $z_{ij} = a_{i1}p_{1j} + a_{i2}p_{2j} + ... + a_{ir}p_{rj}$. This equality expresses the basic model of factor analysis. Here are a_{il} - the constant coefficients to be determined; p_{lj} - the values of factors in the j subdivision, which are also unknown. This relationship in matrix form can be represented as the basic equation of factor analysis:

$$Z = AP \qquad (1)$$

It should be recalled that Z it is a matrix of standardized variables - the initial data, the order $m' n$. $A = (a_{il})$ is an unknown order matrix $m' r$. It is called a factor mapping, and its elements (coefficients a_{il}) are factor loads. I.e. A is a matrix of regression coefficients factors by variables. $P = (p_{lj})$ is an unknown matrix of the order $r' n$ for the values of all factors for all units, or factor values. In this case, there is one matrix equation with two unknowns. However, by carrying out certain mathematical transformations, as was done in [2], for the given problem the solution was obtained one equation with one unknown

$$R = AA¢ \qquad (2)$$

Here *R* is the correlation matrix, *A* is the matrix of coefficients regression factors for production indicators, and *A¢*-is the transposed matrix of these quantities. The relations (1) and (2) are called the fundamental theorem of factor analysis. She argues

that the correlation matrix can be reproduced using factor mapping and correlations between factors, if any. In what follows we assume that the factors are orthogonal. Thus, relations (1) and (2) allow finding unknown matrices A and P, reproducing the correlation matrix by compressing information, which will allow to determine the influence of hidden factors on specific units of the enterprise and its operation as a whole.

It should be noted that this mathematical apparatus has been successfully used to evaluate and explain the dynamics of the development of states in time [3].

This communication explores the procedure for the exchange of information between the main divisions of a large enterprise in the form of the Mariupol seaport while performing the next production tasks. There are considered *n* leading units that operate with *m* most important production indicators. In our case, the number of units observed is n = 15, and the number of production indicators is m = 11. Then the matrix of the observed quantitative elements (quantitative characteristics of the system) has a dimension $n' \ m$. The task was solved numerically using the program "Statistics. Factor analysis". Further, hidden factors were introduced, establishing a connection between the apparent chaotic observed indicators. For this purpose matrices A and P - matrices of factor loads and values of the corresponding factors were determined. For greater clarity, only two factors were considered. These factors are common (the factor is considered general if at least two of its loads are nonzero). Next, a correlation matrix obtained by factor mapping is reproduced. Her analysis yields important results. Below is the result of processing the specified correlation matrix:

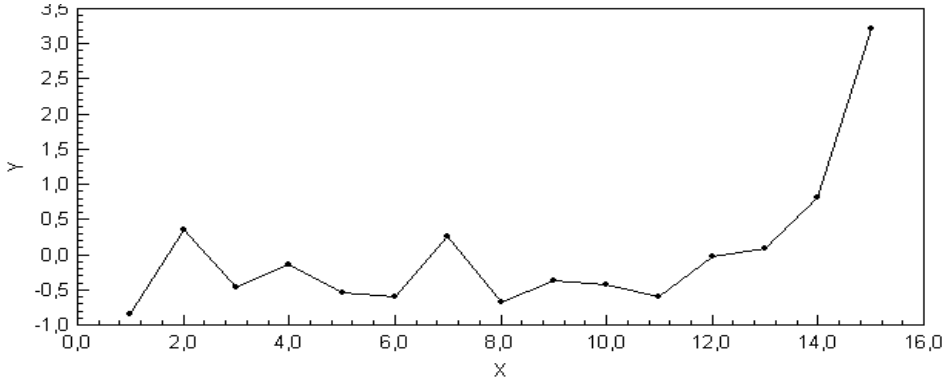
	Eigenvalues (Port_1.sta) Extraction: Principal components			
Value	Eigenvalue	% Total variance	Cumulative Eigenvalue	Cumulative %
1	7,607646	69,16042	7,607646	69,16042
2	1,370707	12,46097	8,978353	81,62139

This implies that more than 81% of the information on production processes and phenomena can leak with the help of the two concealed factors under consideration. Moreover, due to the presence of the first factor, more than 69.1% of the total information leak, and at the expense of the second - more than 12.4%.

The most important is the question of the connection of factors (that is, sources of obtaining production information) precisely with the departments of the enterprise.

This result is shown in the graph. The meaning of the graph can be interpreted as follows. Subdivisions 1, 14 and especially 15 have maximum connections with factor 1. Exactly these subdivisions are due to the main flow of information loss.

Graph. Relationship between factor 1 and enterprise subdivisions.



As follows from table (matrix of production indicators), the maximum information leakage is due to the number of employees. Subdivisions 1, 14 and 15 contain the maximum number of employees: 36, 75 and 192 people respectively.

Thus, the proposed mathematical model for assessing the sources and causes of information leakage made it possible to estimate the loss of information for enterprise divisions.

In conclusion, it should be noted that in this paper we propose and demonstrate a method based on multidimensional statistical analysis and factor analysis, in particular. This method can be used and further developed in assessing the risks to protect the information activities of the enterprise.

Literature

1. Anderson T. W. Au introduction to multivariate statistical analysis. N.Y.- 1958.

2. Überla K. Faktoreuanalyze. Eine systematische Einführung für Psychologen, Mediziner, Wirtschafts-und Sozialwissenschaftler. Springer-Verlag Berlin Heidelberg New-York.- 1977.

3. Kolyada Yu., Klebanova T. The Influence Factors of Economic Indicators of State Development / Journal L Association 1901 «SEPIKE» /Osthoven, Deutschland; Poitiers, France/ 2013.-Part 2.-P.148-153.

Zaitseva E.,
Candidate of Technical Sciences
Mariupol State University

SOME PRACTICAL ASPECTS OF EU GENERAL DATA PROTECTION REGULATION REQUIREMENTS IMPLEMENTATION

Recently data privacy have become a popular topic far beyond IT-related community not just in blog news but also as matter for lawsuits, e.g. EU Court of Justice case Google Spain SL and Google Inc. vs Agencia Española de Protección de Datos and Mario Costeja González in 2014 [1]; government hearings like late Facebook/Cambridge Analytica data breach scandal; and serious fines that companies can be issued by regulatory bodies, like it was for Flybe and Honda Motors, that have been fined £70,000 and £13,000 respectively by the UK's Information

Commissioner's Office (ICO) for breach of the Privacy and Electronic Communications Regulations [2].

For the last two years almost every article concerning data privacy mentions EU General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [3] – that becomes into force on May 25, 2018 and will replace the existing 1995 Data Protection Directive (Directive 95/46/EC). This two-years transition period was granted for organizations mostly outside the European Union so they could prepare for the Regulation.

Key principles of data privacy are not changed in GDPR, though many amendments to the regulatory policies and new requirements were proposed and adopted, some examples include

- Increased territorial scope – organizations that process personal data outside of the European Union (EU) but also offer their services to individuals (referred to as data subjects) residing in the Union are to be subject to GDPR.
- Large penalties – tired approach to fines is adopted. Maximum fine of 20 millions Euro or 4% of annual worldwide turnover (whichever is greater) can be imposed for the most serious infringements like violating data subject's rights (GDPR Article 83.5.b), though organization can be fined up to 10 millions Euro or 2% of annual worldwide turnover (whichever is greater) for not carrying out impact assessment of the processing risks to personal data or not having records in order (GDPR Article 83.4.a).
- Conditions for consent – clear affirmative action should be taken by individual and pre-ticked checkboxes or inactivity should not be sufficient to constitute consent. Moreover, it must be as easy to withdraw consent, as it is to give it.
- Change in data subject rights, for example added right to data portability and the right to not be subject of automated decision-making.
- Appointment of Data Protection Officers (DPO) – organizations should consider whether they are required to designate DPO with necessary level of expert knowledge who takes responsibility for data protection compliance and acts as contact point between organization, individuals and authorities.
- Accountability includes mandatory documentation to demonstrate compliance, like keeping records of processing activities and personal data register.

Since GDPR is law technical aspects are not explicitly covered by the Regulation, for example GDPR does not contain strict requirements regarding security controls on data protection. Article 32 states that "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" [3], and names encryption of data as one of possible, and not mandatory measures. With that if data is not being protected with encryption in case of data breach organization must be ready to prove that existing security controls such as access controls, configuration and change

management, incident response, etc. were sufficient for managing security and privacy risks. Also, some GDPR requirements like those regarding data subject rights do not necessarily have to be automated, however for organizations that run web applications, the rights may be fulfilled with the help of the following features.

1. Right to be informed (Articles 13,14). When sending individual a notification email at the first time add information block describing why person get this notification, what rights does he have under GDPR, are there any transfers of his data to countries outside EU/EEA, who has access to his data, what data organization keeps, contacts of organization and DPO.
2. Right to access (Article 15). Add user profile section where user's data can be seen at once. Obviously, this section must be secured with some sort of authentication process.
3. Right to rectification (Article 16). Add "Edit data" functionality where possible e.g. except for system-derived information or payment transactions, but certainly user should be able to change information he entered himself.
4. Right to be forgotten (Article 17). Add "Delete" button, and erase or anonymize user's data.
5. Right to data portability (Article 20). Add "Export data" button, and use commonly recognized machine-readable formats like CSV or JSON (approved by Article 29 Working Party). Data export functionality or, equivalently, notification about right to data portability should be available at the system interface where user can delete his data.
6. Right to object (Article 21). Add working "Unsubscribe" link/button to all marketing and promotional emails.
7. Right to withdraw consent (Article 7). If organization asks for consent to use cookies, add opt-out options to all public sites.

EU Member States regulatory bodies like the UK's ICO as well as European Commission Article 29 Working Party have published a number of guidelines [4,5] to explain GDPR requirements and to help organizations to implement them. However, there are still many challenges for organizations that act as data controllers and/or data processors.

List of references

1. Case Google Spain and Google (C-131/12). Judgment of the Court (Grand Chamber), 13 May 2014. URL: http://curia.europa.eu/juris/liste.jsf?num=C-131/12
2. ICO warns UK firms to respect customers' data wishes as it fines Flybe and Honda. URL: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/03/ico-warns-uk-firms-to-respect-customers-data-wishes-as-it-fines-flybe-and-honda/
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

URL:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

4. Guide to the General Data Protection Regulation (GDPR). URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

5. Article 29 Working Party Guidelines. URL: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

Меркулова К.В.,
кандидат технічних наук, доцент,
доцент кафедри математичних методів
та системного аналізу
Маріупольського державного університету

ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ У МАРІУПОЛЬСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ

Стрімкий розвиток інформаційних технологій, активізація інтеграційних процесів у вищій освіті, глобалізація світової економіки, динамічні зміни на ринку праці зумовлюють потребу у фахівцях-професіоналах нової генерації в галузі інформаційних технологій, та ставлять принципово нові вимоги до їхньої професійної підготовки. На сучасному етапі розвитку науки і техніки кібербезпека кожної розвинутої держави перетворюється на одну з найважливіших галузей високотехнологічного суспільства. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування, стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як об’єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об’єднаннями. Потоки інформації, що передаються, зберігаються та обробляються в кіберпросторі постійно зростають, що вимагає їх належного захисту від несанкціонованого доступу зі злочинною метою. Тому потреба у фахівцях з кібербезпеки є актуальною і з подальшим розвитком високотехнологічного суспільства буде ще більше зростати.

Підготовка фахівців з кібербезпеки вимагає належної технологічної оснащеності вищого навчального закладу, залучення висококваліфікованих спеціалістів. У підготовці такого роду спеціалістів зацікавлені підприємства та організації України. Ефективність їх підготовки значною мірою пов’язана з реформуванням системи вищої освіти в Україні на всіх рівнях, що здійснюється у напрямі створення гнучкої системи доступу до неперервної освіти, та розробки перспективних моделей підготовки висококваліфікованих, конкурентоздатних фахівців у галузі інформаційних технологій, зокрема бакалаврів з кібербезпеки, відповідно до світових стандартів. Тому у Маріупольському державному університеті за участю провідних фахівців було

розроблено освітньо-професійну програму «Кібербезпека», відповідно до якої майбутні бакалаври повинні вміти:

- виявляти і оцінювати ознаки стороннього кібернетичного впливу, а також моделювати можливі ситуації такого впливу та прогнозувати їх можливі наслідки;
- організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної і кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізуємості та економічної доцільності, можливих внутрішніх і зовнішніх впливів, імовірних загроз та рівня розвитку технологій захисту інформації;
- проводити дослідження у напрямах забезпечення інформаційної і кібербезпеки національних інтересів України та обґрунтовувати шляхи підвищення їх ефективності;
- протидіяти несанкціонованому проникненню протиборчих сторін до власних ІТ систем і мереж, забезпечити стійкість їх роботи, а також відновлення їх нормального функціонування після здійснення кібернападів;
- забезпечити криптозахист власного інформаційного ресурсу, тощо.

Це обумовило впровадження у Навчальному плані підготовки фахівців за спеціальністю 125 Кібербезпека таких дисциплін, як: Управління інформаційною безпекою, Захист інформації в комп'ютерних системах та мережах, Комплексні системи захисту інформації, Теорія і практика інфраструктури відкритих ключів, Кібернетичний простір, Захищені банківські технології, Інформаційна безпека держави, Системи технічного захисту інформації, Кібернетична безпека підприємства та інші. Структурно-логічна схема підготовки бакалаврів зі спеціальності 125 Кібербезпека наведено на рисунку 1.

З метою поліпшення практичної складової навчання на кафедрі створено лабораторію «Кібернетичної безпеки», яка дозволяє студентам:

- опановувати знання з проблем функціонування кібернетичного простору і кіберправа;
- проводити практичні заняття з криптології та розробки криптографічних механізмів інформаційної і кібербезпеки;
- будувати захищені IP та TCP мережі та обслуговувати сертифікати відкритих ключів;
- досліджувати особливості сучасних операційних систем і баз даних,
- вивчати мови програмування високого рівня (C++), сучасні математичні пакети MatLab та пакети прикладних програм типу MathCad;
- вирішувати задачі моделювання процесів підтримки необхідного рівня захищеності інформаційних активів та оптимізації процесів, тощо.

Важливу роль у системі підготовки спеціалістів із кібербезпеки в Маріупольському державному університеті грає дуальне навчання. В основі підготовки закладено, насамперед, практично орієнтовані предмети, посилена підготовка з іноземної мови, а вже потім – загальні дисципліни. Також, для

отримання практичних навичок з метою наближення до практичних потреб галузі, МДУ заключено договори про співпрацю з правоохоронними органами, органами державної влади та іншими провідними установами та організаціями, досвід яких може бути передано студентам у процесі проведення майстер-класів, практичних занять та інших комунікативних заходах.

Як результат, випускники кафедри, як еліта у сфері забезпечення інформаційної та кібербезпеки, будуть здатні працювати в освітніх та наукових установах, підрозділах інформаційної і кібербезпеки державних установ та структур спеціального призначення (СБУ, ДССЗЗІ, МВС, Кіберполіції, ЗС та СЗР України), у центрах і службах захисту інформації підприємств та банківських установ різних форм власності й зможуть обіймати такі первинні посади: програміст/тестувальник програмного забезпечення систем ІКБ; адміністратор комп'ютерних систем і мереж; адміністратор інформаційної та кібербезпеки; аудитор безпеки ІКС; розробник засобів захисту інформації; інженер служби ТЗІ тощо.

Список використаних джерел

1. Рудь І. Закон про кібербезпеку: основні положення, оцінки експертів та розвиток вітчизняного інформаційного простору[Електронний ресурс] / І. Рудь // Україна: події, факти, коментарі. – 2017. – № 19. – С. 42–48. – Режим доступу:http://nbuviap.gov.ua/images/ukraine/2017/ukr19.pdf.

2. Бурячок В. Л. Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології» / В. Л. Бурячок, І. П. Пархомей, М. М. Степанов, В. Б. Толубко // Сучасний захист інформації. – 2016. – № 2. – С. 4–9.

3.Підготовка фахівців з кібербезпеки має бути практично орієнтованою [Електроний ресурс]. – Режим доступу: http://mon.gov.ua/usi-novini/novini/2016/10/04/kruglij-stil-1016/.

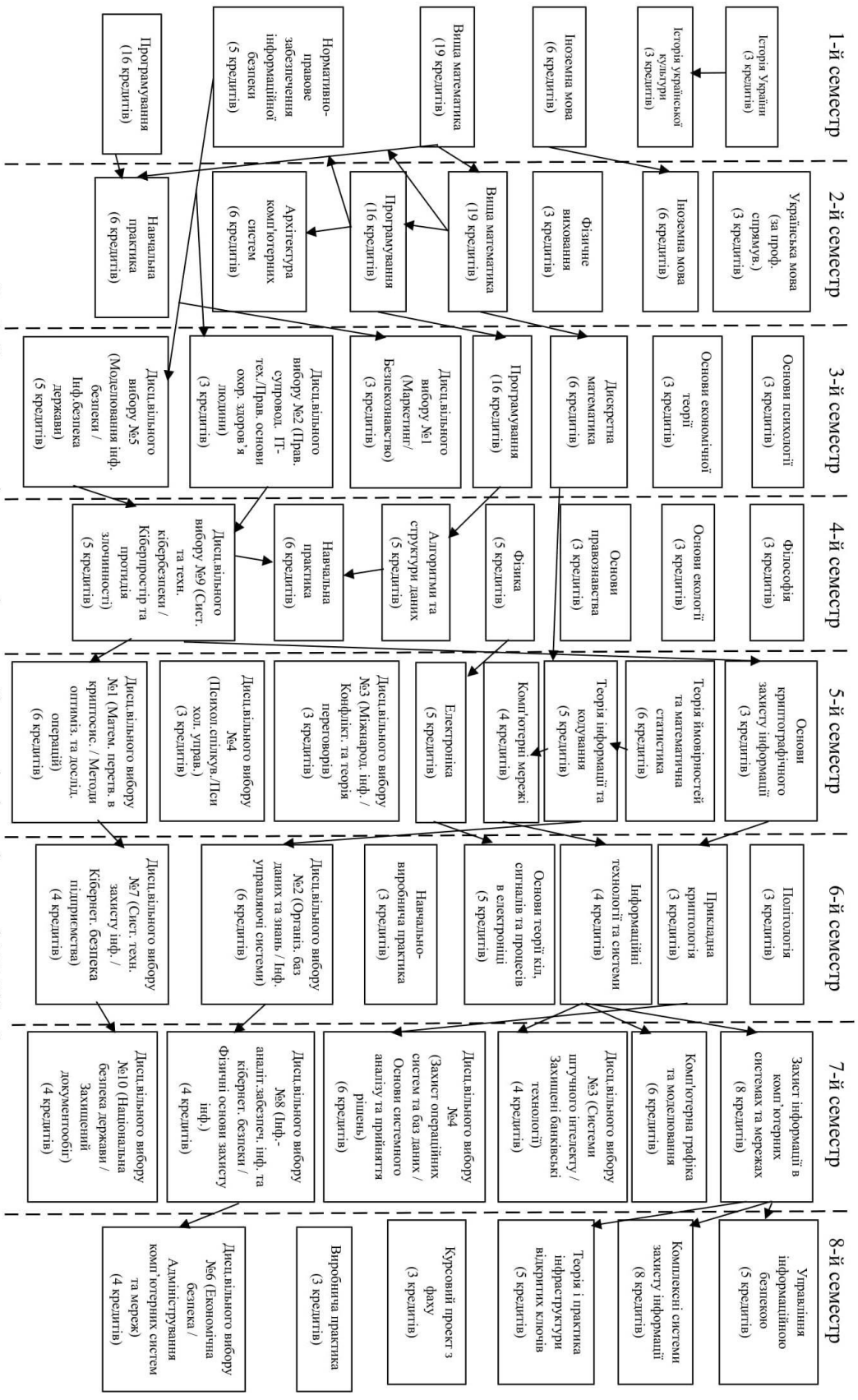


Рис.1. Структурно-логічна схема підготовки бакалаврів зі спеціальності 125 Кібербезпека

Барибін О.І.,
доцент,кандидат технічних наук,
в.о. зав кафедри радіофізики та кібербезпеки
Донецького національного університету імені
Василя Стуса
(м. Вінниця)

СУЧАСНІ МЕТОДОЛОГІЇ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Забезпечення інформаційної безпеки, як для бізнес-організацій, так і для державних установ є досить важливою – якщо не критичною – складовою нормального функціонування. Однією з відомих форм для оцінки стану безпеки та зменшення ризиків безпеки є тестування на проникнення (penetration testing або pentest). Тестування на проникнення – це контрольований експеримент з метою проникнення в систему або мережу для виявлення вразливостей. Тестування на проникнення застосовує ті ж методи, які використовуються при звичайному нападі зловмисника. Такий підхід дозволяє застосовувати відповідні заходи для усунення вразливостей, перш ніж вони будуть вивчені неавторизованими людьми.

У роботі [1] зазначено чотири основні проблемні напрями досліджень, що пов’язані з тестуванням на проникнення:

1. Основні інструменти, що використовуються для тестування на проникнення.
2. Сценарії атак.
3. Методології та стандарти тестування на проникнення.
4. Проблемні питання та напрямки досліджень.

Слід зазначити, що інструментарію та сценаріям атак в літературі присвячено досить багато уваги. Зокрема можна згадати такі публікації як [2-4], у яких досить докладно викладені вищезазначені два питання.

У той же час третє питання не може бути викладене у вигляді підручника або докладного аналітичного звіту у зв’язку з тим, що існуючі методології, як правило, можуть бути порівняні лише в рамках загальних положень. Окрім цього в Україні відсутня єдина затверджена методологія тестування на проникнення. Відповідно, аналіз сучасного стану сформованих методологій тестування на проникнення є актуальним питанням.

Методологія – це схема, яка використовується для досягнення мети. Відмова від використання методології для тестування на проникнення може призвести до неповного випробування, високих витрат часу, невдач та неефективності тестування [5]. Незважаючи на велику кількість і неможливість виділити "правильну методологію" її дотримання має результатом професійне та ефективне тестування на проникнення.

Актуальний перелік сучасних та чинних методологій тестування на проникнення можна сформувати наступним чином:

1. Open Source Security Testing Methodology Manual (OSSTMM). Джерело для ознайомлення: http://www.isecom.org/research/osstmm.html.

2. OWASP testing guide. Джерело для ознайомлення: https://www.owasp.org/index.php/OWASP_Testing_Project.

3. Information Systems Security Assessment Framework (ISSAF) Джерело для ознайомлення: www.oissg.org/issaf.html.

4. Penetration Testing Execution Standard (PTES) Джерело для ознайомлення: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.

5. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). Джерело для ознайомлення: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

OSSTMM може бути використаний практично для будь-яких типів інспекцій, у тому числі тестування на проникнення, етичне хакерство, оцінка безпеки та визначення вразливостей; він складається з тестових модулів для кожної галузі. До методології входять такі методи, як:

1. Тестування інформаційної безпеки (Information Security Testing);
2. Тестування безпеки процесів (Process Security Testing);
3. Тестування безпеки Інтернет-технологій (Internet Technology Security Testing);
4. Тестування безпеки комунікацій (Communications Security Testing);
5. Тестування безпеки бездротового зв'язку (Wireless Security Testing);
6. Тестування фізичної безпеки (Physical Security Testing).

OWASP Testing Guide може бути використаний на різних етапах життєвого циклу розробки програмного забезпечення як складова частина фреймворку, що використовується, та пропонує конкретне керівництво для слідування в рамках цього процесу. У першу чергу методологія OWASP рекомендується для використання при тестуванні веб-застосувань та включає п'ять етапів:

1. Збір інформації (Information Gathering);
2. Тестування управління конфігурацією (Configuration Management Testing);
3. Тестування автентифікації (Authentication Testing);
4. Тестування управління сесіями (Session Management Testing);
5. Тестування авторизації (Authorization Testing).

Методологія ISSAF розроблена як структурований фреймворк для оцінки різних інформаційних систем. Вона передбачає стандарти оцінки та тестування для різних галузей та включає оцінку безпеки, що відображає реальні сценарії. Процедури тестування на проникнення є такими:

1. Збір інформації (Information Gathering)
2. Побудова мережевих карт (Network Mapping)
3. Ідентифікація вразливостей (Vulnerability Identification)
4. Проникнення (Penetration)

5. Отримання доступу та підвищення прав (Gaining Access and Privilege Escalation)

6. Подальше перерахування (Enumerating Further)

7. Компрометація віддалених користувачів/сайтів (Compromise Remote Users/Sites)

8. Підтримання доступу (Maintaining Access)

9. Приховання слідів (Cover the Tracks)

PTES є методологією, яка повністю зосереджена саме на тестуванні на проникнення та включає практичні технічні керівництва для того, що і як тестувати, настанови щодо раціоналізації тестування та рекомендації щодо інструментарію з тестування на проникнення. У PTES тестування на проникнення визначено в рамках семи етапів:

1. Попередні взаємодії (Pre-engagement Interactions);
2. Збір інформації (Intelligence Gathering);
3. Моделювання загроз (Threat Modeling);
4. Аналіз вразливостей (Vulnerability Analysis);
5. Експлоітація (Exploitation);
6. Пост-експлоітація (Post Exploitation);
7. Звітування (Reporting).

NIST SP 800-115 направлена скоріше не на надання вичерпної інформації щодо тестування безпеки та прогами перевірок, а на огляд ключових елементів тестування та перевірки безпеки з акцентом на специфічні технічні методики.

Одним із найважливіших факторів успішності тестування на проникнення є наявність на підприємстві або установі методології. Відсутність формальної методології означає відсутність послідовності у процесах, пов’язаних із підтвердженням того чи іншого рівня інформаційної безпеки. Формальна методологія повинна забезпечувати чітко визначену структуру для проведення повного і точного тесту на проникнення, але не повинна бути обмежувальною – вона повинна дозволяти тестувальнику повною мірою реалізувати свої навички.

Хоча назва чи кількість етапів у різних методологіях відрізняються і можуть складати від 5 до 9, і кожна з розглянутих методологій має різне наповнення та галузі застосування, можна виділити три загальних блока у послідовності тестування на проникнення:

1. збір інформації та її аналіз;
2. підготовка до тестування та проведення тестування;
3. звітування та переведення системи у початковий стан.

Список використаних джерел

1. Bertoglio D. D. Overview and open issues on penetration test / D. D. Bertoglio, A. F. Zorzo. // Journal of the Brazilian Computer Society. – 2017. – №23. – С. 1–16.

2. Penetration Testing: A Survival Guide / [W. Halton, B. Weaver, J. A. Ansari та ін.]. – Birmingham: Packt Publishing Ltd, 2016. – 1045 с.

3. Mohit R. Python Penetration Testing Essentials / Raj Mohit. – Birmingham: Packt Publishing Ltd, 2015. – 178 с.

4. Oriyano S. Penetration testing essentials / Sean-Philip Oriyano. – Indianapolis: John Wiley & Sons, Inc., 2017. – 349 с.

5. Mirjalili M. A survey on web penetration test / M. Mirjalili, A. Nowroozi, M. Alidoosti. // Advances in Computer Science: an International Journal. – 2014. – №3. – С. 107–121.

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

ЗАХИСТ ПРОМИСЛОВИХ МЕРЕЖ У ЦЕНТРІ ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ ДОННТУ

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 FLсервер 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).

Список використаних джерел

1. Билл Лайдон, для InTech. Промышленная автоматизация и «Интернет Вещей» [Електронний ресурс] : 2013. – Режим доступу: 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: https://www.phoenixcontact.com/online/portal/ua/

4. Phoenix Contact. Industrial Ethernet [Електронний ресурс] : Phoenix Contact. – 2017. – Режим доступу: https://www.phoenixcontact.com/online/portal/ua/

5. Phoenix Contact. Ethernet Basics Rev. 02 [Електронний ресурс] : Phoenix Contact. – 2017. – Режим доступу: https://www.phoenixcontact.com/online/portal/ua/

Свірський Б.М.,
кандидат юридичних наук, професор кафедри права та публічного адміністрування, в.о. завідувача кафедри права та публічного адміністрування Маріупольського державного університету

ВДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОГО ІНСТИТУТУ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКА)

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 чимало загроз.

Конституція України (ч.1 ст. 17) визначає – захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. [1]

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 комплексу проблеми нейтралізації або мінімізації цієї нової сукупності загроз в тому числі з допомогою такого інструментарію, як вдосконалення кримінально-правових норм регулюючих спектр відносин в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку.

Розвиток методів обробки інформації за допомогою комп'ютерів призвів до застосування цих машин в усіх галузях національної економіки та інших сферах суспільного життя. Значна кількість таких машин об'єднана комп'ютерними мережами, деякі з них набули інтернаціонального характеру. За цих умов виникли і набули суспільної небезпеки різні діяння, що заподіюють шкоду нормальній роботі комп'ютерів та комп'ютерних мереж, яка поряд зі встановленим порядком використання ЕОМ та комп'ютерних мереж.

Важливим і своєчасним було прийняття 5 жовтня 2017 року парламентом - закону України «Про основні засади забезпечення кібербезпеки України» (далі Закон).[2]

Предметом закону 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 Закону такі як – кібератака; кібербезпека; кіберзагроза; кіберзахист, кібероборона, кібертероризм тощо.

Разом з тим, шляхи до вдосконалення вищезазначенного інституту були зроблені ще у 2014-2015 роках, коли законодавець вніс зміни до розділу XVI КК, але вони були більш косметичними та апріорі не могли відреагувати на Закон який був прийнятий у 2017році.[3]

Системний аналіз понятійного апарату Закону дає підстави стверджувати на необхідність розширення переліку статей розділу з метою реалізації вимог Закону та приведення їх до відповідності чинного законодавства.

Так, на думку автора розділ XVI КК необхідно розширити низкою нових кримінально-правових норм різного спрямування, а саме: доповнити розділ статтями які дають - а) визначення поняття *кіберзлочин* (за аналогом ст. 364 КК); б) визначити такий склад злочину як *кібертероризм* та встановити кримінальну відповідальність; в) визначити такий склад злочину як *кібершпигунство* та встановити кримінальну відповідальність; г) визначити такий склад злочину як *кібершатака* та встановити кримінальну відповідальність.

Наприклад, відповідно до ст. 2 Закону до Кримінального Кодексу України необхідно внести поняття (а також сконструювати нові склади злочинів) у наступній редакції:

Кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням, а також передача або збирання за допомого засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання). з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю.

Кібертероризм - терористична діяльність тобто діяльність що здійснюється у кіберпросторі або з його використанням із закликами застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою.

Кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні

та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

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.Конституція України від 28.06.1996р // Відомості Верховної Ради України (ВВР), 1996 № 30 ст. 141

2. «Про основні засади забезпечення кібербезпеки України» Закон України від 05.10.2017р //Відомості Верховної Ради України (ВВР), 2017 № 45 ст. 403

3. Кримінальний кодекс України. Закон України від 05.04..2001р //Відомості Верховної Ради України (ВВР), 2001 № 25-26 ст. 131

Хараберюш І.Ф.,
доктор юридичних наук, професор,
професор кафедри права
та публічного адміністрування
Маріупольського державного університету

ПРОТИДІЯ ЗЛОЧИНАМ В ГЛОБАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ: КРИМІНОЛОГІЧНІ ОСОБЛИВОСТІ

Глобальні мережі та мережні інформаційні технології створили умови як для суттєвої зміни способів здійснення «традиційних» злочинів, так і для появи нових видів злочинної діяльності, які обумовлюють проведення звичайних та специфічних процесуальних та оперативно-розшукових заходів.

У цьому зв'язку важко переоцінити важливість формалізованого представлення про сутність і властивості щодо відносно нового для юридичної науки феномена, яким є глобальні комп'ютерні мережі. Останні все частіше виступають не тільки предметом злочинних зазіхань або інструментом злочинної діяльності, але і джерелом цінної інформації (у тому числі доказової) про скоєні або плановані злочини. Розуміння суті і відповідних якісних характеристик явищ, пов'язаних з функціонуванням глобальних комп'ютерних мереж у сучасному суспільстві, необхідно для правильної кваліфікації відповідних протиправних діянь, відповідного вибору методів і прийомів ведення процесуальних та оперативно-розшукових заходів. У той же час багато проблем сучасних глобальних комп'ютерних мереж вимагають проведення

міждисциплінарних досліджень, заснованих на застосуванні різних підходів, моделей і теорій. У цілому систематизація знань у даній області повинна сприяти становленню кримінологічної теорії протидії злочинам в глобальних комп'ютерних мережах, розробці на цій основі ефективних правових механізмів, удосконалюванню нормативної бази [1, с. 145-162, 194-229].

Нам би хотілося звернути особливу увагу на деякі кримінологічні особливості глобальних комп'ютерних мереж з метою визначення напрямків ефективної протидії злочинам процесуальними та оперативно-розшуковими засобами. Виділимо і розглянемо найбільш важливі з обставин, які безпосередньо пов'язані із сутністю сучасних глобальних комп'ютерних мереж і мають кримінологічне значення:

1) *можливість анонімної діяльності в глобальних мережах.* Однієї з основних проблем, характерних для сучасного етапу розвитку Інтернету, є практично повна відсутність достовірних ідентифікаторів особистості при роботі в мережі. Простота забезпечення анонімної активності в мережі приводить до психологічного відчуття безкарності і, як наслідок, створенню кримінальних груп у мережі, об'єднанню навколо них осіб, схильних до протиправної діяльності, можливості ведення пропаганди з метою залучення нових учасників, що ми і бачимо сьогодні.

Для зміни ситуації пропонуються різні способи, наприклад, введення до Інтернету стандарту, що вимагає жорсткої ідентифікації користувача при входженні до мережі. Однак усі подібні пропозиції вимагають для своєї реалізації колосальних капіталовкладень;

2) *технологічна незахищеність глобальних мереж.* Більшість проблем технологічної незахищеності глобальних мереж пов'язане з тим, що Інтернет будувався як відкрите середовище комунікації незначного за сьогоднішніх масштабів числа дослідницьких і військових комп'ютерних центрів. До нинішнього часу досягнута така стадія розвитку Інтернету, коли закладені при його створенні принципи функціонування частково суперечать розв'язуваним задачам;

3) *складність інфраструктури сучасних мереж і мережних процесів.* Для сучасних глобальних мереж характерна надзвичайна розгалуженість комунікацій, наявність значної кількості проміжних вузлів зв'язку, кожний з яких являє собою уразливу ланку з погляду безпеки інформації, яка через нього проходить, а також збільшується обсяг інформаційних ресурсів. Усе це утруднює виявлення випадків злочинної діяльності у мережах;

4) *вплив глобальних комп'ютерних мереж на стан національної безпеки.* У більшості технологічно розвинених держав застосування глобальних комп'ютерних мереж у різних галузях досягло такого рівня, що їх нормальне функціонування стало одним з факторів національної безпеки. При цьому глобальні мережі значною мірою забезпечують роботу об'єктів, що безпосередньо впливають на благополуччя суспільства.

Формування єдиного інформаційного простору України, інтеграція його зі світовими комунікаційними системами також приводять до появи нових погроз національній безпеці нашої країни. Одним з напрямків такої протидії є використання автоматизованих систем забезпечення оперативно-розшукових заходів. Прикладом такої системи є, наприклад, американська система забезпечення оперативно-розшукових заходів, які проводяться у мережі Інтернет, «DCS-1000». Ця система дозволяє правоохоронним органам здійснювати моніторинг електронної пошти і ftp-трафіка. Аналогічна система діє й у країнах Євросоюзу – система «RES»;

5) *відсутність єдиної організації, яка повністю координує діяльність Інтернету.* Інтернет являє собою децентралізовану структуру, яку утворюють різі мережі. Вони розрізняються за своїми задачами, джерелами фінансування, вимогами до клієнтів цих мереж. Рішеннями технічних питань, пов'язаних з управлінням Інтернетом, займаються міжнародні громадські організації.

У більшості держав, у тому числі і в Україні, система регулювання і контролю Інтернету знаходиться в стадії становлення. Варто підкреслити, що, незважаючи на велику кількість відомств, які мають відношення до Інтернету, відсутня єдина організація, що здійснює контроль над ним, з якою правоохоронні органи могли б ефективно співпрацювати;

6) *наддержавний характер сучасних глобальних мереж.* Складна інфраструктура мереж, які територіально охоплюють не одну державу, забезпечує передачу інформації за рахунок погодженого функціонування пристроїв, що належать організаціям і фізичним особам у межах різної юрисдикції. Сайти, що фізично знаходяться на території якої-небудь держави, можуть обслуговуватися закордонним провайдером. При мережному обміні даними географічне місцезнаходження суб'єктів практично не має значення. Кіберпростір не має територіально визначених границь, а виникаючі тут процеси можна вважати наддержавними.

Серйозні правові проблеми постійно виникають щодо того, відповідно до законодавства якої держави повинна нести відповідальність особа, що вчинила злочин, знаходячись в одній державі, у той же час як об'єкт посягання був в іншій. Світова спільнота поки не виробила норм, що вказують, яким законом варто користуватися в тих чи інших обставинах (наприклад, lex loci actus – закон місця здійснення дії або lex patrie – закон країни, громадянином якої є правопорушник).

Таким чином, аналіз окремих особливостей глобальних комп'ютерних мереж досить чітко вказує на присутність обставин, що дозволяють відносити глобальні мережі до свого роду криміногенних об'єктів. У глобальних мережах концентрується значний обсяг процесуальної та оперативно-значимої інформації, функціонують канали обміну інформацією між учасниками злочинних груп, що забезпечують підвищену скритність і мобільність. До глобальних комп'ютерних мереж підключені об'єкти, у відношенні яких можливі злочинні прояви підвищеної суспільної небезпеки. Усе це робить

необхідним адекватно протидіяти новим формам злочинної діяльності, що, як показала зарубіжна практика та досвід протидії цим злочинам з боку правоохоронних органів нашої держави, неможливо без проведення процесуальних та оперативно-розшукової заходів в цій сфері, які спрямовані не тільки на пасивний але і на активний пошук важливої інформації, а в окремих випадках і на її ефективну реалізацію.

Список використаних джерел

1. Злочини в сфері використання комп'ютерної техніки: кваліфікація, розслідування та протидія: монографія / [І.Р. Шинкаренко, В.О. Голубєв, М.В. Карчевський, І.Ф. Хараберюш]. – Донецьк: Донецький юридичний інститут ЛДУВС, 2007. – 268 с.

Українцев О. А.,
кандидат юридичних наук,
начальник відділу економічної безпеки ПАТ «ММК ім.Ілліча»,
м. Маріуполь

КРІПТОВАЛЮТА – ЯК ЗАГРОЗА ЦІЛІСНОСТІ ДЕРЖАВИ?

Однією з основних умов стабільного функціонування держави є надходження грошових коштів та покриття поточних зобов'язань. Відповідно, відсутність такого мінімально необхідного запасу грошових коштів свідчить про фінансові труднощі держави. В той же час надмірна величина грошових коштів свідчить про збитки, пов'язані з інфляцією і знеціненням грошей. В зв'язку з цим виникає необхідність аналізу і оцінки раціональності управління грошовими коштами держави. Аналіз грошових потоків допомагає з'ясувати причини, які вплинули на збільшення (зменшення) припливу грошових коштів та збільшення (зменшення) їх відпливу. Це можна робити як за довгостроковий період (декілька років), так і за короткостроковий (квартал, рік). Також за допомогою аналізу грошових потоків держави можливо з'ясувати причини надмірного витрачання грошових коштів, фактори впливу на процес припливу чи відпливу грошових коштів та вчасно прийняти міри для подолання вказаних причин.[1]

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» Національний банк України визначається як регулятор з кібербезпеки в банківській сфері. Для цього він буде мати право на встановлення в цій сфері власних стандартів і організацію перевірки їх дотримання [13]. У той же час можливо спостерігати тенденцію до збільшення використання при розрахунках різного роду операцій, замість традиційних платіжних засобів криптовалют, при цьому роль держави як безпосереднього регулятора в даному випадку нівелюється.

Що ми знаємо о кріптовалютах? Сатоши Накамото (англ. Satoshi Nakamoto) - псевдонім людини або групи людей, які розробили протокол кріптовалюти біткоїн і створили першу версію програмного забезпечення, в

якому цей протокол був реалізований [2] за допомогою поштової розсилки в листопаді 2008 року. Після цього, в 2009 році, він випустив першу версію програмного клієнта біткоїни і разом з іншими програмістами - знову ж за допомогою поштової розсилки, а до кінця 2010 року поступово зник з поля зору криптовалютної спільноти. Незважаючи на таку співпрацю з іншими розробниками, Накамото ніколи нічого не розповідав про себе особисто. В останній раз про нього чули навесні 2011 року, коли він повідомив, що "перемикається на інші речі" [3].

Ось одна з тез висунутих Сатоши: «Традиційна банківська модель підтримує необхідний рівень приватності, надаючи доступ до інформації лише сторонам-учасницям і довіреній третій особі. Необхідність відкритої публікації транзакцій виключає такий підхід, однак приватність як і раніше можна зберегти, якщо публічні ключі будуть анонімними. Відкритою буде інформація про те, що хтось відправив комусь певну суму, але без прив'язування до конкретних особистостей » [4].

У 2017 році в статті колишнього стажера SpaceX була підтримана точка зору, що безпосередньо CEO Tesla і SpaceX Ілон Маск може бути справжнім Сатоши. Підозри були засновані на проведеної Маском технічній експертизі програмного забезпечення та історії опублікованих білих книг. Однак, сам Маск спростував цю інформацію 28 листопада 2017 року. [5] В умовах зростаючої популярності криптовалюта до цифрової валюті стали придивлятися і держави. Одні країни заборонили використовувати криптовалюту, інші ввели обмеження на її оборот, а треті взагалі визнали офіційним платіжним засобом. Але всі вони зрозуміли, що, якщо криптовалюта таки візьме гору над звичайними грошима, єдиним варіантом виживання для офіційних грошових знаків стане перехід в формат криптовалюти [6].

В цей час можна констатувати що криптовалюта для держави невигідна за наступними причинами:

- загроза для національної валюти
- втрата контролю над грошовими потоками
- створення кращих умов для обігу нелегальних товарів

При цьому криптовалюта ніяк не може поповнювати скарбницю держави, так як комісія за транзакції не йде ні в які банки, способу обкладання податком криптовалютних капіталів на даному етапі немає. Анонімність криптовалюти дозволяє громадянам уникати повсюдного контролю за грошовими операціями. Відносна швидкість переміщення криптовалют від однієї людини до іншої - в перебігу декількох хвилин. (В той же час деякі міжбанківські перекази можуть займати до декількох днів). І вже тільки ці гідності криптовалют за фактом негативно впливають на національну валюту за допомогою якої державна влада може контролювати багато сфер суспільства. Так при зростанні популярності криптовалюти, знижується державний контроль і відбувається втрата контролю за грошовими потоками. Рух криптовалют є анонімним, що заважає державі контролювати переміщення фінансів. Це робить можливим безперешкодно

виводити гроші з країни. Дізнатися від кого саме і до кого переводилася криптовалюта дуже важко. Тому торгувати забороненими товарами всередині країни стає набагато простіше. Слід враховувати те, що під заборону можуть потрапити не тільки наркотики і зброя, а цілком звичайні товари - технічні засоби, література і багато іншого, що не вписується в політику, яка проводиться країни. У зв'язку з цим існування такої системи не вигідно для держави і будь-яка країна буде намагатися або заборонити, або шукати методи регулювання криптовалюти [7].

Так, в документі під назвою "Цифрові валюти: відповідь на запит інформації" центральний апарат Великобританії вказав, що використання цифрових валют представляє мінімальні ризики для фінансової стабільності і кредитно-грошової системи держави. Деякі країни всіляко їх заохочують (Австралія, Німеччина, Нідерланди, Нова Зеландія, Сінгапур), деякі - встановлюють для цифрових грошей серйозні обмеження (Індонезія, Китай, Росія). Прямі заборони на сьогоднішній день встановлені тільки в Болівії, Еквадорі, Таїланді і В'єтнамі. А більшість урядів вибрали лінію нейтралітету, уникаючи будь-яких рішень щодо віртуальної валюти. У деяких країнах, наприклад, в Японії, криптовалюта визнається фінансовим активом. При цьому електронні гроші не вважаються законним платіжним засобом, а розглядаються як засіб обміну. У Канаді ж, навпаки, можна навіть отримати цифрову заробітну плату. А криптовалюта, отримана в результаті майнінга, обкладається прибутковим податком. Іспанія ще в 2014 році визнала біткойн офіційною платіжною системою. Ця ініціатива виходила від податкової інспекції країни, яка провела аналіз використання криптовалют в країні і прийшла до висновку, що цей процес необхідно легалізувати і оподаткувати [8].

У березні 2017 року голова Ради Національного банку України Богдан Данилишин підтвердив незмінність раніше прийнятого рішення, промовив в інтерв'ю, що біткоїни і інші криптовалюти «є грошовими сурогатами, які не забезпечені реальною вартістю і не можуть використовуватися на території нашої країни, як засіб платежу, оскільки це суперечить нормам українського законодавства» [9].

Але поки биткоїн офіційно не визнаний в Україні, то й адмініструвати операції з криптовалютою, фактично, неможливо. Але так чи інакше, незалежно від думки уряду, віртуальні гроші існують і використовуються в Україні.

У той же протягом 6 лютого 2018 р. у Вашингтоні комісія з цінних паперів і бірж США (SEC) і Комісія з торгівлі товарними ф'ючерсами США (CFTC) підтримали впровадження криптовалют в фінансову систему США. Це сталося під час відкритого засідання Комітету з банківським, житловим та міським питань. Голова CFTC Крістофер Джанкарло у своїй промові перед Комітетом з банківських, житловим та міським питань заявив, що криптовалюти можуть значно поліпшити глобальну фінансову систему: платежі здійснюватимуться швидше, прозоріше і надійніше, а децентралізована фінансова система, швидше за все, виявиться централізованою. Також голова

SEC Джей Клейтон висловився оптимістично щодо майбутнього ринку криптовалют. Він пояснив, що криптовалюти і ICO поліпшать процес функціонування фінансових потоків [10].

Основний інструмент регулювання bitcoin - криптовалютние біржі, тому що bitcoin рідко використовується як пряме засіб платежу і відразу після здійснення транзакції обмінюється на необхідну валюту. Ухвалення статусу криптовалюти як товар, надасть можливість обкладати всі операції податками, зокрема біржові торги і прибуток за проведення операцій, як збирається вчинити уряд Японії. Національні державні влади можуть вимагати від криптовалютних бірж, зареєстрованих на території їх країн, вимагати від клієнтів біржі підтвердження особи, шляхом надання копій паспортів та інших документів. Або біржі самі можуть вводити таку функцію. В цей час одна з таких бірж - Bitstamp, вимагає підтвердження особи для доступу до всіх можливостей біржі. [11]. В опублікованому документі під назвою "Цифрові валюти: відповідь на запит інформації" центральний апарат Великобританії вказав, що використання цифрових валют представляє мінімальні ризики для фінансової стабільності і кредитно-грошової системи держави [12].

Виходячи з такої статистики, напрошується висновок, що визнання цифрової валюти багато в чому залежить від ступеня розвитку країни. Держави зі слабкою економікою не готові до впровадження подібних платіжних систем. І навпаки, високорозвинені країни все ж прагнуть врегулювати електронні платежі, взявши їх під свій контроль.

Список використаних джерел

1. В.М.Вареник, [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua
2. Офіційний сайт свобідної енциклопедії Вікіпедії. -[Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/
3. Утмагазин [Електронний ресурс]. – Режим доступу https://utmagazine.ru/posts/21076-satoshi-nakamoto-chto-izvestno-o-sozdatele-bitkoin
4. Перевод статьи Сатоши Накамото «Биткоин: цифровая пиринговая наличность» [Електронний ресурс]. – Режим доступу: https://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/
5. Musk: I Am Not Bitcoin’s Satoshi Nakamoto [Електронний ресурс]. – Режим доступу: https://www.bloomberg.com/news/articles/2017-11-28/elon
6. Национальные криптовалюты: возможность или риск для рынка криптовалют [Електронний ресурс]. – Режим доступу: https://cryptonet.biz/ru/natsionalnye-kriptovalyuty-vozmozhnost-ili-risk-dlya-rynka-kriptovalyut/
7. Офіційний сайт свобідної енциклопедії Вікіпедії [Електронний ресурс]. – Режим доступу https://ru.m.bitcoinwiki.org/wiki/Bitcoin
8. Законны ли биткоины в Украине [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/rus/publications/2017/08/11/627993/

9. Минфин [Електронний ресурс]. – Режим доступу: https://minfin.com.ua/2017/03/24
10. Американские регуляторы поддержали биткоин и внедрение криптовалют в финансовую систему США [Електронний ресурс]. – Режим доступу: https://investfuture.ru/articles/id/amerikanskie
11. Новости [Електронний ресурс]. – Режим доступу https://securenews.ru/exchange/
12. Чи законні біткоіни в Україні Наталя Мисник [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/publications/2017/08/11/627993/
13. Офіційний веб-портал Верховної ради України [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua

Крівенко С. В.,
кандидат технічних наук, доцент,
доцент кафедри математичних
методів та системного аналізу
Маріупольського державного університету

СТРЕС-ТЕСТ МЕРЕЖІ НА DOS І DDOS АТАКИ

У комп'ютерній термінології атака на відмову в обслуговуванні (DoS) або атака розподілена відмова в обслуговуванні (DDoS) – це спроба зробити ресурси машини або мережі недоступними для користувачів. Хоча засоби, мотиви і цілі DoS розрізняються, головна її суть залишається незмінною – на час або на невизначений строк припинити або призупинити послугу хоста, з'єднаного з Інтернетом. Як відомо, DDoS – це атака, яка здійснюється двома або більше особами, або ботами, а DoS атака робиться однією особою чи системою. На 2014 рік, частота розпізнаних DDoS атак досягла в середньому 28 за кожну годину. Звичайною метою виконавців DoS атак є сайти і послуги на серверах, які привертають увагу, на зразок банківських, платіжні шлюзи кредитних карт і навіть кореневі сервери імен. Загроза відмови в обслуговуванні також поширені в бізнесі відносно веб-сайтів. Ця техніка тепер широко застосовується в певних іграх, що використовується власниками серверів або незадоволеними конкурентами в таких іграх як популярні сервера Minecraft. Зростає застосування DoS як форми «Вуличних Інтернет Протестів». Цей термін зазвичай застосовується до комп'ютерних мереж, але не обмежується цим; наприклад, він також відноситься до управління ресурсами CPU.

Один із загальних методів атаки – це насичення цільової машини зовнішніми запитами зв'язку, у зв'язку з чим вона не може відповісти на легітимний трафік чи відповідає так повільно, що є по суті недоступною. Такі атаки зазвичай ведуть до перевантаження сервера. Узагальнено кажучи, в результаті DoS атаки виявляються зайнятими ті чи інші ресурси сервера і він

більше не може виконувати діяльність, для якої він призначений, або відбувається перешкоджання зв'язку між користувачами і жертвою таким чином, що вони не можуть адекватно обмінюватися інформацією. DoS атаки незаконні. Їх організатори і рядові виконавці переслідуються за законами багатьох країн. Стрес-тест власної мережі не є протизаконним. Стрес-тест чужих мереж/серверів при отриманні їх згоди також дозволений, але необхідно враховувати інтереси третіх осіб. Цими третіми особами можуть бути власники хостингу (якщо ви тестуєте чужий сайт, віртуальний сервер, що знаходяться на хостингу), інтернет-провайдери (оскільки значний потік трафіку може створювати навантаження на їх комунікації) і т. д. Вкрай бажано погоджувати стрес-тести і з цими третіми особами щоб уникнути всіх можливих проблем. Інакше, мимоволі, ви станете заподіювачем шкоди тим, на кого стрес-тест не був націлений.

Є агентства і корпорації, які практично в реальному часі відстежують DDoS атаки по всьому світу і відображають карту DoS в реальному часі: http://www.digitalattackmap.com/; http://map.norsecorp.com/; http://map.ipviking.com/.

Утиліта hping3 Kali Linux добре відпрацьовує якщо у вас ще є інші запущені DoS інструменти на зразок GoldenEye (використання декількох інструментів, які атакую один і той же сайт/сервер/послугу, збільшує шанси на успіх). hping3 це безкоштовний генератор і аналізатор пакетів для TCP/IP протоколу. Hping, де факто, один з обов'язкових інструментів для аудиту безпеки і тестування фаєрволів і мереж, він використовувався для виконання експлойта техніки сканування Idle Scan, яка зараз реалізована в сканері портів Nmap. Нова версія hping3 – написана на скриптах з використанням мови Tcl. В ній реалізується движок для зручного опису рядками TCP/IP пакетів, отже, програміст може за дуже короткий час написати скрипт, що відноситься до низькорівневої маніпуляції пакетами TCP/IP і аналізувати їх. Як і більшість інструментів, що використовуються в комп'ютерній безпеці, hping3 корисний для експертів з безпеки, але існує безліч додатків, пов'язаних з тестуванням мережі і системним адмініструванням. hping3 слід використовувати для

- Traceroute/ping/probe (трасування/пінгу/зондування) хостів за файерволом, які блокують спроби використовувати стандартні утиліти.
- Виконання сканування простою (в даний час реалізується в nmap з легким призначеним для користувача інтерфейсом).
- Тестування правил брандмауера.
- Тестування IDS (систем виявлення вторгнення).
- Експлуатації відомих залежностей в стеках TCP/IP.
- Мережевих дослідженнях
- Вивченні TCP/IP (hping була використана в мережевих курсах AFAIK).
- Написанні реальних програм, пов'язаних з TCP/IP тестуванням і безпекою.
- При автоматизованих тестах по фільтрації трафіку.

• Створення робочої моделі експлойтів.

• Досліджень у сфері мереж і безпеки, коли потрібно емулювати комплексне TCP/IP поведінку.

• Прототипах систем виявлення вторгнень (IDS).

• Простих у використанні утиліти з інтерфейсом Tk.

Існує також утиліта Low Orbit Ion Cannon (LOIC) – це інструмент стрес-тесту мережі, тобто він створений для перевірки, як багато трафіку мета може обробити. Щоб ґрунтуючись на цих даних зробити оцінку запасу потужності ресурсів. Ця програма надихнула створення інших подібних програм, у неї існує безліч клонів, деякі з яких дозволяють проводити стрес-тест прямо з браузера. Ця програма з успіхом використовувалася групою Anonymous, для полегшення їх DDoS атак проти кількох веб-сайтів, у тому числі деяких дуже відомих громадських організацій. Противники заборони цієї програми вказують, що те, що вона робить, аналогічно зайти на веб-сайт кілька тисяч разів; тим не менш, деякі американські правоохоронні групи розцінюють використання LOIC як порушення комп'ютерної безпеки та шахрайське дію.

Також можна здійснювати тестову DoS-атаку з використанням GoldenEye та інші інструменти для стрес-тесту мережі.

Висновок. Будь-які нові та сучасні фаєрволи будуть блокувати перевантаження мережі, і в наші дні більшість ядер Linux побудовані з захистом від SYN флуду. Інструкція hping3 призначена для цілей дослідження і навчання. Для тих, у кого проблеми з TCP SYN або TCP Connect флудом, треба використовувати IPTables і способи налаштування для блокування DoS-атак, що використовують hping3 або будь-які інші інструменти.

Тимофєєва І.Б.,
кандидат педагогічних наук,
старший викладач кафедри математичних методів
та системного аналізу
Маріупольського державного університету

АНАЛІЗ РИЗИКІВ ПІДКЛЮЧЕННЯ СТОРОННІХ ХМАРНИХ ДОДАТКІВ

Хмара є новою областю для хакерів, які активно освоюють його, щоб отримати нові потенційні можливості для своїх атак. Зловмисники розуміють, що хмарні системи є життєво необхідними для багатьох сучасних організацій. Вони також розуміють, що можуть швидше проникнути в корпоративні системи, якщо зуміють зламати хмарну систему.

За визначення стандарту ISO/IEC 27005 під ризиком розуміється вплив невизначеності на цілі, що характеризується комбінацією ймовірності подій та їх наслідків [1].

Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року (Cisco® 2017 Midyear Cybersecurity Report, MCR) вказує на швидку еволюцію

загроз і зростання їх масштабів, а також на поширення атак типу «переривання обслуговування» (destruction of service, DeOS), які здатні знищувати резервні копії і страхувальні системи (safety net), необхідні організаціям для відновлення систем і даних після атаки. З появою Інтернету речей (Internet of Things, IoT) все більше операцій в ключових галузях переводиться в режим online, що розширює горизонт атак, збільшує їх масштаби і посилює наслідки.

Нами було обрано за основу аналіз-звіт компанії Cisco щодо інформаційної безпеки у 2017р. Компанія Cisco створює інтелектуальні системи кібербезпеки для реального світу. Пропонований нею комплекс рішень є одним з найбільш повних в галузі і захищає від широкого спектра загроз. Підхід Cisco до інформаційної безпеки, орієнтований на нейтралізацію загроз і відновлення працездатності, спрощує систему безпеки, робить її більш цілісною, надає можливості детального моніторингу, узгодженого управління і вдосконаленої захисту від загроз до, під час і після атаки [2].

З кінця 2016 року компанія Cisco спостерігає зростання хакерської активності, спрямованої на хмарні системи. У січні 2017 р. дослідники Cisco виявили хакерів, що полюють за діючими скомпрометовані корпоративними обліковими даними. Використовуючи атаки методом грубої сили, хакери створили бібліотеку облікових даних (імен і паролів) корпоративних користувачів, можливо, використовуючи для цього відомі списки зламаних облікових записів в мережі. Вони намагалися проникнути в кілька корпоративних хмарних систем, використовуючи для цього сервери з 20 вкрай підозрілими IP-адресами.

У період з грудня 2016 р. по середину лютого 2017 р. дослідники компанії Cisco за допомогою аналізу поведінки та інших інструментів проаналізували тисячі корпоративних хмарних середовищ клієнтів. Після аналізу компаній виявили схожі патерни підозрілих спроб входу в системи більш ніж 17% організацій, які вивчались. Хакери в довільному порядку перебирали 20 IP-адрес, щоб уникнути виявлення [2].

Як хакери збиралися використовувати бібліотеку облікових даних корпоративних користувачів, невідомо. Один з можливих варіантів – підготовка цільової фішингової кампанії або соціальна інженерія. Також можливо, що Зловмисники хотіли продати діючі поєднання імені користувача і пароля або використовувати облікові дані самостійно, щоб увійти в облікові записи користувачів і добути конфіденційну інформацію або зламати їх колег. Що точно відомо, так це те, що облікові дані, за допомогою яких хакери намагалися отримати доступ до корпоративних хмарним мереж, були пов’язані з корпоративними обліковими записами, скомпрометовані в ході попередніх порушень.

За допомогою відкритої авторизації OAuth підвищуються можливості хмари, але також породжується ризик підключених сторонніх хмарних додатків, що використовуються співробітниками на підприємстві. Ці додатки взаємодіють з корпоративної інфраструктурою і корпоративними хмарними

ISaaS-платформами, якщо користувачі отримують доступ за допомогою відкритої авторизації (OAuth).

Як видно на рис. 1, за даними дослідження компанія Cisco, кількість підключених хмарних додатків на одну організацію серйозно зросла в порівнянні з 2014 р. У середовищі середньостатистичного підприємства на сьогоднішній день налічується понад 1000 різних додатків і більше 20 000 різних установок цих додатків [2].

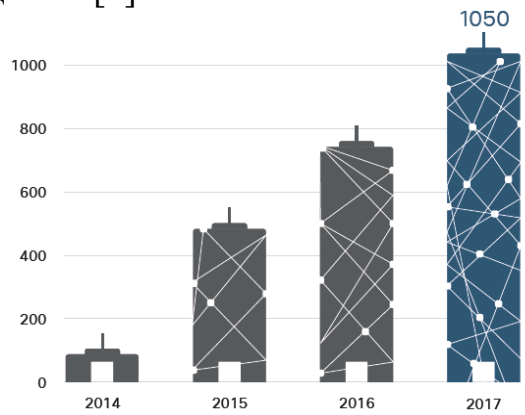


Рис.1 - Кількість унікальних підключень хмарних додатків на одну організацію URLзображення: https://www.cisco.com/c/dam/assets/prod/sec/mcr2017/images/1080/figure-52-cloud-apps.png

Остання фішингова кампанія, націлена на користувачів Gmail і намагалася використовувати інфраструктуру OAuth, продемонструвала ризик безпеки, пов'язаний з OAuth. Зловмисники намагалися отримати контроль над обліковими записами електронної пошти користувачів і розіслати фішингових хробака по їх контактам. За оцінками Google, кампанія торкнулася близько 0,1% від мільярда користувачів Google. За найскромнішими підрахунками дослідників Cisco, черв'як інфікував понад 300 000 організацій [2].

На хмару не звертають уваги: єдиний привілейований хмарний користувач створює величезний ризик. Найсучасні найбільші компрометації системи безпеки починаються з захоплення і використання в злочинних цілях єдиною облікового запису привілейованого користувача. Доступ до привілейованого облікового запису може дати хакерам можливість встановити повний контроль, провести масштабне розкрадання інформації і завдати серйозної шкоди. Однак більшість організацій залишають цей ризик без належної уваги.

Щоб краще представляти масштаби цієї проблеми, дослідники Cisco вивчили 4410 привілейованих облікових записів в 495 організаціях і виявили, що шість з кожних ста кінцевих користувачів хмарної платформи мають привілейовані облікові записи. При цьому в більшості організацією велика частина адміністративних завдань (88%) виконувалася в середньому лише двома привілейованими користувачами. Також виявили, що організації могли б скасувати привілеї «Суперадміністратора» для 75% адміністраторських облікових записів без будь-яких наслідків або з мінімальним збитком для бізнесу [2].

Захист персональних даних – проблема, яка вже достатньо давно є актуальною не лише для українських компаній. Але в поточному році це питання повинно стати справжнім викликом для українців, які в своїй економічній діяльності використовують персональні дані громадян та жителів Європейського Союзу. Справа в тому, що починаючи з 25 травня 2018 року в юридичному полі Європейського Союзу вступає в силу новий нормативний акт – Загальний Регламент Захисту Даних, більш відомий як GDPR (General Data Protection Regulation). Євросоюз переходить на нові правила поводження з персональними даними, а Регламент стосується будь-якої роботи з персональними даними, зокрема збору, зберігання, передачі.

Аналіз загроз, показав, що найбільшу небезпеку становлять загрози управління хмарою та її безпекою, а також загрози гіпервізору. Інформаційна безпека стає ключовим чинником, що визначає стабільне функціонування бізнесу й успіх цифрових перетворень.

Список використаних джерел

1. Аулов І. Ф. Дослідження моделі загроз ключових систем хмари та пропозиції захисту від них / І. Ф. Аулов // Восточно-Европейский журнал передовых технологий. – Том 5. № 2 (77). - 2015. – С. 4-11.

2. Отчет Cisco по информационной безопасности за первое полугодие 2017 г. прогнозирует появление новых атак типа «прерывание обслуживания», а также рост масштабов и усугубление последствий атак [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/ru_ru/about/press/press-releases/2017/07-21.html

Дяченко О. Ф.
старший викладач кафедри математичних методів та системного аналізу Маріупольського державного університету

ІНТЕГРАЦІЯ МАТЕМАТИЧНИХ ДИСЦИПЛІН З ДИСЦИПЛІНАМИ ЦИКЛУ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ БАКАЛАВРІВ СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА

Інтеграції, як провідній тенденції розвитку національних систем освіти й багатогранному освітньому явищу, присвячено чимало наукових праць останнього часу, у значній частині яких розглядаються питання, пов’язані з міждисциплінарним аспектом (Т. Голубенко, Л. Демчина, В. Кірвас, Т. Коженовська, А. Лісневська, В. Прошкін, П. Ситнікова, С. Чечотіна та ін.). Цими та іншими вченими наголошується на тому, що при реалізації єдиної стратегії професійної підготовки студентів інтеграція особистісних, соціальних і діяльнісних аспектів сприяє формуванню загальних і спеціальних компетентностей майбутнього фахівця засобами координації, уникнення дублювання змісту навчальних дисциплін, встановлення горизонтальних і вертикальних, біпредметних і мультипредметних зв’язків, забезпечення єдності

теоретичної і практичної підготовки, університетської освіти та науки. Завдяки цьому створюються умови для усвідомлення студентами задач майбутньої діяльності та шляхів їх автономного вирішення на основі здобутих знань і навичок оперативного пошуку, обробки та плідного використання інформації у складних, не алгоритмізованих ситуаціях [1 та ін.].

Аналіз освітньо-професійних програм та навчальних планів підготовки бакалаврів зі спеціальності 125 Кібербезпека дозволив зробити висновки, що математична підготовка є фундаментом для більшості професійно-орієнтованих дисципліни. Оскільки математичні знання виконують роль методологічної основи наукового знання та базової складової більшості профілюючих дисциплін. Математичні дисципліни вивчаються студентами даної спеціальності на першому та другому курсах.

Визначимо, які конкретно знання та вміння з математичних дисциплін необхідні при вивченні дисциплін циклу професійної підготовки. Так, вивчаючи дисципліни «Теорія інформації та кодування», «Основи криптографічного захисту інформації», «Прикладна криптологія», «Комплексні системи захисту інформації» для вдалого шифрування даних студент повинен знати алгебру висловлень та алгебру множин, вміти виконувати дії над множинами, знати поняття однозначного відображення, оберненого відображення, сюр'єктивного та ін'єктивного відображення, знати малу теорему Ферма та теорему Ейлера, вміти розв'язувати конгруенції, створювати та аналізувати розподіли випадкових величин, тощо.

У дисципліні «Теорії ризиків» для виконання моделювання ризику використовуються знання з «Теорії ймовірностей» та «Математичних методів і моделей», зокрема використовують лінійне та стохастичне програмування, теорію ігор; теорію нечітких множин та ін.

Дисципліна «Основи теорії кіл, сигналів та процесів в електроніці» базується на знаннях лінійної та векторної алгебри, диференціального числення та його застосування, інтегрального числення та його застосування, рядів, диференціальних рівнянь. Для більш глибоко вивчення даної фахової дисципліни необхідні також знання з теорії функцій комплексної змінної, рядів Фур'є й розклад функцій за ортогональними базисами [2].

Інтеграція математичних та профільних дисциплін виступає чинником забезпечення освітніх вимог до професійної підготовки бакалаврів з кібербезпеки та сприяє подоланню головного недоліку та парадоксу сучасної освітньої системи – засвоєнню зростаючого об'єму знань за обмежений час навчання.

Список використаних джерел

1. Прошкін В.В. Зміст інтеграції університетської науки та освіти / В.В. Прошкін // Вісник Дніпропетровського університету імені Альфреда Нобеля. Серія «Педагогіка і психологія». Педагогічні науки, 2014. – № 2 (8). – С. 108-114.

2. Шевченко С.М. Математичні компетенції майбутніх фахівців інформаційної безпеки / С.М. Шевченко, Ю.Д. Жданова // Сучасний захист інформації. – 2016. – №4. – С. 90-96.

Черновол В.С.,
курсант 4-го курсу факультету №4 (кіберполіції)
Харківського національного університету внутрішніх справ

ШАХРАЙСТВО ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННО-ОБЧИСЛЮВАНОЇ ТЕХНІКИ: ЗЛОЧИНИ З КРИПТОВАЛЮТОЮ

Криптовалюта за своєю суттю це цифрові гроші, випуск та облік яких заснований на технології блокчейн.

Відповідно до проекту Закону України «Про стимулювання ринку криптовалют та їх похідних в Україні» криптовалютою слід вважати децентралізований цифровий вимір вартості, що може бути виражений в цифровому вигляді та функціонує як засіб обміну, збереження вартості або одиниця обліку, що заснований на математичних обчисленнях, є їх результатом та має криптографічний захист обліку [1., п.1, ч.1, ст.1].

Блокчейн - являє собою вибудований за певними правилами безперервний послідовний алгоритм з блоків, що містять певну інформацію про видобуток та транзакції, пов’язані з криптовалютою. Тобто вся інформація зберігається не в одному централізованому місці, а на безлічі електронних засобів, сполучених мережею Інтернет.

Історія транзакцій в блокчейні відкрита всім учасникам системи і незмінна, всі користувачі залишаються анонімними і мають рівні статуси Технологія блокчейну базується на спеціальних алгоритмах шифрування, що потребує відповідного програмного забезпечення та комп’ютерного обладнання.

В Україні статус криптовалют до теперішнього часу залишається не визначеним. Національний банк України офіційно розглядає криптовалюту як грошовий сурогат, що не має забезпечення реальною вартістю. Звідси витікає неможливість її використання фізичними і юридичними особами на території України як засоби платежу. Незважаючи на чітку позицію національного регулювальника економіки заперечувати світовий досвід і розвиток криптовалюти в практиці міжнародних валютних розрахунків вважаємо недоцільним. Відмовлятися від використання криптовалюти зважаючи на її потенційну небезпеку і можливість шахрайських дій також не розумно. Єдиним рішенням проблеми, на наш погляд, являється створення ефективної системи контролю обігу криптовалюти в Україні. Технології сьогодні розвиваються швидше, ніж держава встигає адаптувати законодавство щодо їх регулювання.

Проблеми та ризики, пов’язані з використанням криптовалюти, умовно можна поділити на три категорії.

Перша - уразливості безпеки самої системи блокчейну і побудованої на ній інфраструктури послуг, включаючи послуги-посередників, таких, як

криптовалютні біржі і торгові платформи, сервіси електронних гаманців та ін. Експлуатація цих вразливостей обумовлює ризики, перш за все пов'язані з можливістю втрати контролю над криптовалютними рахунками і гаманцями, для самих учасників криптовалютної екосистеми. Більш актуальною проблемою для самих учасників екосистеми є злом криптовалютних гаманців, торгових майданчиків і платформ сервісів-посредників з метою розкрадання активів в криптовалюті.

Друга група ризиків, пов'язаних з використанням криптовалюти, має фінансову природу. В першу чергу мова йде про їх високу волатильність. Оскільки біткоін не був визнаний офіційним платіжним засобом де-небудь в світі, не існує його офіційного курсу по відношенню до інших національних валют. Курс визначає ринок в ході торгів на віртуальних біткоін-біржах і обмінних майданчиках.

Третя група ризиків і загроз включає використання криптовалюти в протидії законним цілям, в тому числі для торгівлі кримінальними послугами, відмивання грошей і фінансування тероризму. Особливості криптовалюти при проведенні операцій з ними дозволяють уникати деяких форм контролю, які використовуються для транзакцій зі звичайними грошима. Оскільки операції з тим же біткоіном, як правило, анонімні, неможливо простежити, чи не є відправник і одержувач коштів однією і тією ж особою. Крім того, в силу відсутності централізованого регістра транзакцій державним регуляторам важко простежити походження коштів на рахунки власників біткоінів.

У Листі НБУ від 08.12.2014р., зазначається, що діяльність з купівлі-продажу Bitcoin за долари США або іншу іноземну валюту має ознаки функціонування так званих «фінансових пірамід» та може свідчити про потенційну залученість у здійсненні сумнівних операцій відповідно до законодавства про протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансуванню тероризму [2].

Слід зазначити, що при операціях з криптовалютами існують суттєві ризики. Доступ до криптовалютного гаманця може буде скомпрометовано, а операція із переказу криптовалюти є неповоротною. Відсутність прямої вказівки держави на закон, який потрібно застосовувати до операцій з криптовалютами створює дуже високі ризики їх використання. Правоохоронні органи завдяки невизначеності статусу криптовалют в Україні істотно обмежені у виборі засобів і методів протидії злочинам які вчиняються з використанням криптовалют та злочинів де криптовалюта є об'єктом протиправного посягання. Зловмисникам поточний стан справ навпаки розв'язує руки і надає безліч можливостей, особливо в незаконному заволодінні криптовалютою. Існує велика кількість шахрайських схем щодо незаконного заволодіння криптовалютою такі як фейкові сайти відомих ресурсів, піраміди, онлайн казино, фішингові інструменти, продаж неіснуючих товарів та послуг тощо.

Список використаних джерел

1. Про стимулювання ринку криптовалют та їх похідних в Україні: проект закону 7183-1 від 10.10.2017. // База даних «Законодавство України» / [Електронний ресурс] : Верховна Рада України – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710

2. Лист Національного Банку України «Щодо віднесення операцій з "віртуальною валютою/криптовалютою "Bitcoin" до операцій з торгівлі іноземною валютою, а також наявності підстав для зарахування на поточний рахунок в іноземній валюті фізичної особи іноземної валюти, отриманої від продажу Bitcoin» від 08.12.2014 // База даних «Законодавство України» / [Електронний ресурс] : Верховна Рада України – Режим доступу : http://zakon3.rada.gov.ua/laws/show/v2889500-14.

3. Биткойн - это инновационная сеть платежей и новый вид денег! [Електронний ресурс] . – Режим доступу : https://bitcoin.org/ru/

Авдєєнко В.,
студентка ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

СПОСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Кому і навіщо потрібен ваш акаунт?

Найчастіше користувач навіть не припускає, що його акаунт зламаний. Шахраї діють обережно, щоб людина нічого не запідозрила.

Зламані профілі використовують для здійснення цільових дій: вступу в групи, додавання лайків і коментарів. Це безпечний для шахраїв спосіб монетизації чужого акаунта, так як більшість людей не пам’ятають, в які групи вони вступали, а перевіркою коментарів і лайків у всіх незліченних спільнотах в Facebook і «ВКонтакте» взагалі ніхто не займається.

Послуга вступу в різні групи і додавання лайків з коментарями зараз масово пропонується реальним користувачам. Але ви нічого не зможете за допомогою неї продати, оскільки хакери залучають в групи замовників нецільову аудиторію, а розсилка спаму від невідомого спільноти тільки дратує людей, що негативно позначається на іміджі компанії.

Існують ще два поширених кошти монетизації зламаних акаунтів:

- розсилка спаму на стіну акаунта і в особисті повідомлення друзям; спам розсилається у вигляді рекламних повідомлень, промоакцій і т. д .;
- розсилка індивідуальних SMS-повідомлень з проханням проголосувати або терміново допомогти; в таких SMS повідомляється, що вони будуть коштувати 30 коп., а насправді людина платить 5 $.

Як зрозуміти, що вас зламали?

Перелічимо основні ознаки зламаного облікового запису, щоб ви змогли

своєчасно змінити контактні дані:

- Друзі пишуть, що ви були online, коли ви точно знаєте, що не виходили в Інтернет.
- З вашого облікового запису почалася розсилка підозрілих листів, посилань і т. д.
- Ви знаходите в акаунті групи, в які не вступали, і френдів, яких не заводили.
- Коли ви заходите в аккаунт, і ваш пароль не підходить.

Якщо ви розумієте, що ваш профіль зламаний, необхідно поміняти пароль не тільки від соціальної мережі, але і від вашого e-mail-ящика.

Гігієна для акаунта

Щоб ваш акаунт не виявився в руках зловмисників, необхідно дотримуватися запобіжних так званої мережевої гігієни:

- Реєструйте акаунти на корпоративну пошту. Пошту на поширених доменах частіше зламують і так отримують доступ до індивідуальних акаунтів.
- Використовуйте спеціальні програми, які не дозволять троянам і інших вірусних системам красти паролі. Приділіть особливу увагу тому, щоб ваша антивірусна програма блокувала роботу шпигунів клавіатури. Адже часто за допомогою таких додатків отримують доступ до приватної інформації (логіни та паролі від електронної пошти і соціальних мереж, паролі від кредитних карт і т. д.).
- Змінюйте паролі, використовуйте якомога більше символів, щоб ускладнити автоматичний підбір.
- Не переходьте за посиланнями, які вам надсилають на пошту і в соціальні мережі. Кожна з них може бути використана для злому вашої сторінки.

Але мережева гігієна, як і будь-яка інша, не зможе повністю захистити вас від вірусного захворювання. Навіть якщо враховувати, що соціальні мережі захищені безпечними протоколами: на жаль, на даний момент не існує стовідсоткових способів захисту облікового запису.

Це пов’язано з тим, що соціальна мережа - це непідконтрольна нам середовище, і захистити її можуть тільки її співробітники за допомогою додаткових внутрішніх систем безпеки. Тому існують лише базові поради щодо дотримання запобіжних заходів.

До злому акаунта практично неможливо визначити його вразливість, але після злому можна поміняти логін і пароль, що закриє доступ зловмисникам до ваших особистих даних. У соціальній мережі набагато легше усувати проблеми за фактом їх появи, ніж прагнути передбачити можливі варіанти атаки, тому що поліпшити заходи безпеки чужорідної середовища ми не зможемо.

Список використаних джерел

1. Мамєдов Р. Захист персональних даних в соціальних мережах. [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah/

2. Халілов Д. Способи захисту персональних даних в соціальних мережах. [Електронний ресурс]. – Режим доступу: http://www.praima.ru/node/351

3. Хачатурова С.С. Зберігання та захист інформації. Міжнародний журнал прикладних і фундаментальних досліджень. 2016. № 2-1. С.63-65.

Арапова А.,
студентка ОС «Магістр» спеціальності «Право»
Маріупольський державний університет

СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ЯК НЕОБХІДНА СКЛАДОВА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Кібербезпека охоплює широкий спектр практик, інструментів та концепцій, які тісно пов'язані з безпекою інформаційних та оперативних технологій (ОТ). Кібербезпека відрізняється тим, що вона включає в себе наступальне використання інформаційних технологій для атаки противників. Термін «кібербезпека» використовується лише для позначення безпеки, що стосується оборонних дій, пов'язаних із інформаційними технологіями та / або середовищами та системами ОТ.

Широкий спектр різних заходів, пов'язаних з кіберзахистом може включати зменшення привабливості середовища до можливих зловмисників, розуміння критичних місць та конфіденційної інформації, введення превентивного контролю, щоб атаки були дорогими, здатність виявлення атак, реагування та можливості реагування. Кіберзахист також проводить технічний аналіз, щоб виявити шляхи та райони, на які можуть нападати.

Ключ до посилення кібербезпеки - це зниження рівня вразливості. Незважаючи на важливість усвідомлення загрози, зменшення вразливості, всі напади ускладнюються [1].

Кібернетика включає в себе три комплементарних категорії: «проактивний», «активний» та «реактивний». «Проактивні» заходи посилюють кібернетичне середовище та забезпечують максимальну ефективність для кіберінфраструктури. «Активні» заходи зупиняють або обмежують шкоду, заподіяну кібер-активності супротивника. «Реактивні» дії відновлюють ефективність після вчиненого кібернападу. Ці категорії утворюють цикл інформаційної діяльності, що відбувається безперервно та одночасно в мережах, інтегрованих за спільною системою автоматизації [2, с. 46-55].

Кібернапади унікальні у відсутності необхідності фізичної близькості виконувати атаку (тобто кожен, хто має підключення до Інтернету, є потенційним учасником цього всесвітнього бойового простору) та в значно скороченому часі, необхідному для здійснення атаки.

Директор Агентства національної безпеки та голова Кібернетичного командування Сполучених Штатів адмірал Майк Роджерс говорить: « річ не в тому, чи атакує вас, а в тому – коли саме» [3].

Існує нагальна потреба організаціям по-справжньому зрозуміти свій статус кібербезпеки та, де це необхідно, негайно вжити заходів щодо виправлення недоліків. Якщо немає розуміння статусу кібербезпеки, організації не зможуть керувати ризиками кібербезпеки, і вони майже напевно зазнають атаки.

Управління ризиками в галузі кібербезпеки, яке раніше було просто щорічним процесом, як частина планування та складання бюджету, зараз є критичним фасилітатором у режимі реального часу в боротьбі проти кібер-порушень [3].

Порушення в галузі кібербезпеки виникають, коли люди, процеси, технології або інші компоненти системи управління ризиками системи кібербезпеки відсутні, неадекватні або певним чином не виконуються. Отже, ми повинні розуміти всі важливі компоненти та те, як вони взаємопов'язані. Система управління ризиками повинна знати, що всі кінцеві точки в мережі були (і в даний час) ідентифіковані і що критичні вразливості вирішуються швидко. Успіх кібербезпеки по суті є результатом ефективного процесу управління ризиками.

У стані великого обсягу подій важливою є кібернетична стійкість - це здатність системи, організації, місії передбачати, протистояти, відновлювати та адаптувати свої можливості в суперечливих умовах, кібернападів на ресурси.

В цілому, аналіз стану забезпечення інформаційної безпеки показує необхідність удосконалення системи регулювання інформаційної безпеки. Постає потреба у виробленні нових засобів, методів і способів забезпечення інформаційної безпеки, моніторинг інформаційного середовища, наявності загроз та небезпек [4].

Через розміри, складність та постійну еволюцію векторів атаки немає простого, єдиного підходу до управління ризиками, пов'язаними з кібербезпекою. Тим не менш, важливо почати десь встановити базову лінію для ідентифікації критичних компонентів. Наступні п'ять важливих атрибутів є ефективними в управлінні ризиками кібербезпеки.

Атрибут перший: ефективна структура. Ефективна та відповідна основа є важливим місцем для початку. Центральна частина будь-якої програми управління ризиками кібербезпеки - це стандарт кібербезпеки, призначений для управління конфіденційністю, цілісністю та доступністю даних.

Другий критичний атрибут програми кібербезпеки – його сфера застосування. Ефективна програма повинна бути всеосяжною за своїм обсягом, тобто програма повинна звертатись до всіх критичних елементів, які необхідно захистити в компанії.

Наприклад, у більшості організацій програма управління ризиками буде включати мережі, особисті комп'ютери та різні мобільні пристрої, адже ми живому в епоху зростання «Інтернет речей». З автомобілів до приладів, від термостатів до складу двері, все більше і більше пристроїв підключені до

мережі і доступні через Інтернет. Всі ці пристрої створюють більше потенційних векторів атак.

Крім того, що охоплюється широкий масив підключених пристроїв, сфера повинна бути всеосяжною у своєму підході. Наприклад, виявлення вторгнення та системи профілактики працюють на периферії організації, регулярно проводячи моніторинг зовнішніх загроз для виявлення будь-якої незвичайної діяльності.

Третій атрибут: оцінювання та моделювання загрози. Щоб запобігти кібератакам організація повинна оцінювати ризики та визначати пріоритети. Спостерігаючи за новими загрозами та оцінюючи як їх вірогідність, так і збиток, який вони можуть завдати, служба кібербезпеки зможе розробити теплову карту типової оцінки ризику кібербезпеки, на якій розташовуються потенційні ризики проти витрат і зусиль, які будуть потрібні для захисту від них.

Процес оцінки ризиків показує, чому наявність правильної структури є таким важливим; оскільки більшість загроз кібербезпеки зачіпають більше, ніж один домен, тому єдиний набір засобів керування може не забезпечити належний захист від загрози. Хоча важливо захищати від відомих погроз, служба кібербезпеки повинна бути в змозі захистити від невідомих погроз.

Коли цінні дані будуть ідентифіковані, наступним кроком буде визначення потенційних векторів атаки для цих даних. Одним з основних джерел ризику практично для всіх типів даних є фішинг-атака. Після того, як хакери фінішують свої повноваження, вони використовуються для входу в базу даних, що містить велику кількість конфіденційних даних.

Слабкі або повторно використані паролі є постійною проблемою, оскільки паролі залишаються відкритими або зберігаються в документах, які не є захищеними. Це означає, що просто використання імені користувача та пароля для безпеки більше не достатньо. Багаторівнева безпека - тобто вимога до окремої перевірки через повідомлення про смартфон або інший токен перед наданням доступу - все частіше рекомендований спосіб підтвердження особи, кому потрібен доступ.

Ще однією зростаючою загрозою є ransomware, тип зловмисного програмного забезпечення, який уникає типових антивірусних програм. Вірус ransomware зашифровує вміст на систему користувача, яка вимагає від жертви купувати ключ розблокування за допомогою банківського переказу, віртуальної валюти або інші засобів. Новіші варіанти цього зловмисного програмного забезпечення також є здатними шифрувати вміст інших систем, прив’язаних до зараженої системи, включаючи резервну копію системи та хмарних сервісів, ефективно шифруючи всі версії виробничих даних і залишаючи жертву без інших варіантів.

Четвертий атрибут: проактивне планування реагування на інциденти. За більшу частину своєї історії кіберзберігаючі галузі зосередили свою увагу на запобіганні атак і контролю доступу з брандмауерами, паролями та подібними

заходами. Але сьогодні, хоча запобігання залишається ключовим, основна увага переміщується від профілактики до питань, як реагувати на вторгнення та обмежити шкоду, яку воно викликає.

Початок такого проактивного планування реагування на інциденти - це виявлення порушень, виявлення регіону реєстрації та моніторингу домену. Більшість систем мають численні пристрої для різних видів діяльності. Журнали брандмауера та журнали додатків реєструють хто входить до системи, хто змінює дані, які записи вони переглядають та іншу інформацію. Дисципліна в цій області в останні роки суттєво покращилася, і зараз питання полягає в тому, як зробити так, щоб переконатись, що всі дані журналювання збираються та аналізуються централізовано.

Після виявлення виникає питання, як організація відновлює роботу після інциденту? Ще більш терміновим є питання, як організація обмежує збиток та зупиняє будь-яку незаконну діяльність, що продовжується в мережі? Ці питання є критичними елементами плану реагування на інцидент, який також охоплює інформування безпосередньо постраждалих сторін; інших зацікавлених сторін, таких як продавці та клієнти; і, нарешті, зовнішній світ.

П’ятим критичним атрибутом є наявність достатніх ресурсів - зокрема, команд, служб кібербезпеки. Багато організацій часто не приділяють належної уваги цій вимозі, нехтуючи призначенням відповідних посад та розподілом обов’язків або не встановлюють необхідні структури управління, що вимагаються в рамках використовуваної системи.

У більшості компаній щоденна увага IT-команд зосереджена, перш за все, на тому, щоб система безперебійно працювала і це зрозумілий пріоритет. Адже сервісні переривання помічаються негайно, і ефекти очевидні майже всім. З іншого боку, порушення безпеки менш помітні, принаймні на перших порах, і переваги профілактики та планування нападів не є настільки очевидними.

Крім того, у багатьох організаціях IT-команда має мало безпосередньої підготовки з питань безпеки або недостатньо досвіду. Практично в кожному випадку зусилля з кібербезпеки повинні бути покладені на досвідченого лідера команди, для якого IT-безпека є його головним обов’язком, а не додатковою функцією [5].

Зрештою, незалежно від того, як організовані зусилля з кібербезпеки, результат процесу планування повинен бути дієвою дорожньою картою - планом дій, який визначає пріоритети для конкретних людей, процесів та технологічних питань.

Іншими словами, дорожня карта може включати необхідне нове програмне забезпечення та інструменти, можливі настройки системи та технології, що забезпечують більший захист, і кадрові зміни, які дають змогу організації реагувати ефективним способом у разі порушення. Як приклад, дорожня карта кібербезпеки може включати в себе п’ять стандартних етапів:

1. Визначення критичних даних. Тип даних буде відрізнятися залежно від галузі.

2. Карта зберігання даних і потоків. Включити зовнішню маршрутизацію та зберігання даних.

3. Виконання аналізу ризику контролю. Визначення як ризиків, так і пом'якшення контролю.

4. Оцінка терміну контролю безпеки. Використання структури домену безпеки для
виявлення слабких місць.

5. Створення короткострокових та довгострокових планів по відновленню. Визначення пріоритетів шляхом збалансування ймовірності і ступеню ризику відносно часу та витрат на відновлення.

Звичайно, для різних організацій ризики різні. І саме в цьому полягає складність вирішення питання, як допомогти тій чи іншій організації. Не можна зовні прийти й діяти, адже у кожної свої проблемні питання і ніхто краще самої організації, її керівництва не знає, які саме ризики їй загрожують, які дані їм потрібно захистити та які в них можливості. Дуже важливо, щоб у самій організації ці дані були структуровані та впорядковані. Захист кіберпростору – це дуже складний процес системного розвитку, зміни різноманітних процедур в організації, встановлення нових правил, технічних змін, який допоможе запобігти кібератакам та обмежити їх негативних вплив на діяльність різноманітних структур.

Список використаних джерел

1. Pescatore, J.: Toward a National Cybersecurity Strategy, G00167598,. Gartner, Inc., 2009
2. Herring MJ, Willett KD. Active cyber defense: a vision for real-time cyber defense. J Inform Warfare. 2014;13(2):46–55.
3. Marvell S. The real and present threat of a cyber breach demands real-time risk management. Acuity Risk Management; 2015.
4. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці: [Електронний ресурс]. Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=747
5. Chaudhary R., Hamilton J.: The Five Critical Attributes of Effective Cybersecurity Risk Management - A White Paper. Techocal report, Crowe Horwath LLP (2015): [Електронний ресурс]. – Режим доступу: http://www.scadahackr.com/library/Documents/Risk_Management/Crowe%20Horwath%20-%205%20Critical%20Attributes%20of%20Effective%20Cybersecurity%20Risk%20Management.pdf

Герасименко Я.,
студент ОКР «Магістр» спеціальності «Журналістика (журналістика)»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Мережа Інтернет давно стала глобальною як за принципами організації, так і за кількісними показниками. При цьому права людини на анонімність тривалий час вважалися філософією Інтернету. Водночас повноцінне користування всіма його вигодами неможливе без розміщення персональних даних на віддалених серверах. Користувачам доводиться залишати дані про себе, коли вони здійснюють покупки, завантажують контент чи реєструються в соціальних мережах. Користувача можна ідентифікувати навіть за деякими технічними даними, якими пристрій обмінюється з віддаленими серверами в автоматичному режимі.

Актуальність роботи зумовлена тим, що використання комп'ютерних технологій призвело до загострення проблеми захисту персональних даних від несанкціонованого доступу. Специфіка захисту персональних даних у мережі Інтернет пов'язана з тим, що інформація не прив'язана жорстко до носія, а може швидко копіюватися та передаватися різними каналами.

Мета цієї роботи – виявити найпоширеніші загрози витоку персональних даних, а також розглянути програми та методи, що розширюють безпеку інформації в мережі Інтернет. Мета дослідження досягається наступними завданнями:

- визначити основні способи несанкціонованого доступу до персональних даних в Інтернеті;
- розглянути основні програмні методи захисту персональних даних.

Статтею 32 Конституції України проголошено право людини на невтручання в її особисте життя. Крім того, не допускається збирання, зберігання, використання поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1].

З метою визначення механізмів захисту персональних даних 1 червня 2010 року Верховною Радою України було прийнято Закон України «Про захист персональних даних», який набрав чинності з 1 січня 2011 року. Предметом правового регулювання цього Закону є правовідносини, пов'язані із захистом персональних даних під час їх обробки. Визначення поняття персональні дані наводиться в абзаці восьмому статті 2 Закону, відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2]. Спроба удосконалити захист осіб у зв'язку з автоматизованою обробкою персональних даних осіб здійснена в Законі України «Про внесення змін до деяких

законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року [3].

На сьогодні відома дуже велика кількість загроз інформації, які можуть бути реалізовані з боку порушників. Так, за кодифікатором Генерального Секретаріату Інтерполу, несанкціонований доступ та перехват інформації містить в себе такі види комп'ютерних злочинів:

– «комп'ютерний абордаж» – доступ до комп'ютеру або до мережі без права на це. Цей вид злочину використовується для проникнення в чужі інформаційні мережі;

– «перехват» – перехват інформації за допомогою технічних засобів, без права на це. Він здійснюється або шляхом підключення до зовнішніх комунікаційних каналів, або шляхом підключення до периферійних пристроїв [4].

Ще одним видом комп'ютерних злочинів є внесення змін до комп'ютерних даних:

– логічна бомба – полягає в таємному вбудовуванні в програму набору команд, який повинен спрацювати лише одного дня, але за певних умов.

– троянський кінь – це таємне введення в чужу програму таких команд, які дозволяють здійснювати інші функції, що не планувалися власником програми, але одночасно зберігати і колишню працездатність [4].

Останнього часу популярність набув фішинг – різновид шахрайської діяльності, метою якої є отримання доступу до конфіденціальної інформації користувача (логінів, паролів) [5]. Фішингові повідомлення найчастіше надходять від імені відомих брендів і впливають на емоційне сприйняття інформації, зокрема вони можуть: викликати тривогу за стан своїх банківських рахунків; обіцяти грошові вигоди з докладанням мінімальних зусиль; закликати до пожертв тощо [5]. Не так давно з'явилося поєднане з фішингом поняття – фарминг. Зловмисники замінюють на серверах DNS цифрові адреси легітимних веб-сайтів на адреси підроблених, в результаті чого користувачі перенаправляються на шахрайські сайти [5].

Зараз існує кілька основних принципів, що дозволяють організувати відносно безпечне підключення до мережі Інтернет.

Наприклад, Firewall, який установлюється між мережею та Інтернетом і виконує роль мережного фільтра. Він налаштовується таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Інтернет і назад, і обмежити трафік з боку Інтернет до мережі, яка потребує захисту, тільки необхідними службами [7].

Ще один метод захисту – Network Address Translation, або NAT. Він полягає в заміні в IP-пакеті реальної адреси комп'ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні його в зовнішню мережу. Це дозволяє запобігти прямому обігу ззовні до внутрішніх комп'ютерів і приховує структуру мережі. Налічується кілька різновидів NAT [7]. Перша форма NAT найпростіша – це трансляція фіксованої внутрішньої адреси у фіксовану

зовнішню. Друга форма NAT – це трансляція групи внутрішніх адрес в одну зовнішню. При цьому всі внутрішні комп'ютери можуть працювати з Інтернетом одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується [7]. При використанні третьої форми NAT внутрішній комп'ютер, виходячи в Інтернет, одержує вільну в цей момент адресу з бази даних [7].

Застосування так званого «посередника» (proxy-сервера) також підвищує рівень захищеності мережі, тому що виключає необхідність прямого виходу в Інтернет комп'ютерів користувачів. Proxy-сервер складається ніби із двох частин – клієнтської та серверної. Коли клієнтський комп'ютер звертається до сайту через proxy-сервер, його клієнтський мережевий додаток взаємодіє зі серверною частиною proxy-сервера. При цьому proxy-сервер на рівні додатка передає клієнтський, і вже від імені proxy-сервера надсилає даний запит на сайт [7].

Список використаних джерел

1. Конституція України : закон України від 28 червня 1996 р. № 254к/96 // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 32.
2. Закон України «Про захист персональних даних» [Електронний ресурс] : Відомості Верховної Ради України (ВВР). – 2010. – № 34. – с. 481. –. Режим доступу : http://zakon5.rada.gov.ua/laws/show/2297-17.
3. Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [Електронний ресурс] : Відомості Верховної Ради України (ВВР). – 2014. – № 14. – с. 252. –. Режим доступу: http://zakon5.rada.gov.ua/laws/show/383-18.
4. Максимус Д.О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посіб. / Д.О. Максимус, О.О. Юхно. – Харків : НікаНова, 2013. – 102 с.
5. Злочинність у глобалізованому світі : матеріали XVI Всеукр. кримінол. конф. для студентів, аспірантів та молодих вчених (м. Харків, 12 груд. 2017 р.) / за заг. ред. А. П. Гетьмана і Б. М. Головкіна. – Харків : Право, 2017. – с. 195-197.
6. Мельник М. О. Організація захисту інтернет-ресурсу від несанкціонованого доступу та програмний захист авторських прав / М. О. Мельник, Н. С. Константинова, О. В. Бескупський // Системи обробки інформації. - 2017. - Вип. 2. – С. 122-125. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2017_2_25.
7. Fakher Atout. NAT/Firewall traversal:Issues and solutions [Електронний ресурс] : Fakher Atout. – Режим доступу : http://www.tml.tkk.fi/Publications/C/22/papers/Atout_final.pdf.

Дейнега Г.,
студентка ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

СТАТИЧНІ МЕТОДИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

Актуальність теми полягає в тому, що біометричні системи доступу є дуже зручними для користувачів. На відміну від паролів і носіїв інформації, які можуть бути втрачені, вкрадені, скопійовані, біометричні системи доступу засновані на людських параметрах, які завжди знаходяться разом з ними, і проблеми їх збереження не виникає. Втратити їх майже неможливо. Також неможлива передача ідентифікатора третім особам. Розрізняють такі статистичні методи біометричної аутентифікації:

- Ідентифікація за відбитками пальців – найпоширеніша біометрична технологія аутентифікації користувачів. Метод використовує унікальність малюнка папілярних візерунків на пальцях людей. Відбиток, отриманий за допомогою сканера, перетворюється в цифровий код, а потім порівнюється з раніше введеними наборами еталонів. Переваги використання аутентифікації за відбитками пальців: легкість у використанні, зручність і надійність. Універсальність цієї технології дозволяє застосовувати її в будь-яких сферах і для вирішення будь-яких завдань, де необхідна достовірна і досить точна ідентифікація користувачів. Зазвичай застосовуються три основні типи сканерів відбитків пальців: ємнісні, прокатні, оптичні. Найпоширеніші і широко використовувані це оптичні сканери, але вони мають один серйозний недолік. Оптичні сканери нестійкі до муляжів і мертвих пальців, а це значить, що вони не настільки ефективні, як інші типи сканерів. Так само в деяких джерелах сканери відбитків пальців ділять на 3 класу за їхніми фізичними принципам: оптичні, кремнієві, ультразвукові.
- Аутентифікація по райдужній оболонці ока використовує унікальність ознак і особливості райдужної оболонки ока. Райдужна оболонка утворюється ще до народження людини, і не змінюється протягом усього життя. Райдужна оболонка за текстурою нагадує мережу з великою кількістю оточуючих кіл і малюнків, які можуть бути виміряні комп’ютером, малюнок райдужної оболонки дуже складний, це дозволяє відібрати близько 200 точок, за допомогою яких забезпечується висока ступінь надійності аутентифікації. Для порівняння, кращі системи ідентифікації за відбитками пальців використовують 60-70 точок. Технологія розпізнавання райдужної оболонки ока була розроблена для того, щоб звести нанівець нав’язливість сканування сітківки ока, при якому використовуються інфрачервоні промені або яскраве світло. Вчені також провели ряд досліджень, які показали, що сітківка ока людини може змінюватися з часом, в той час як райдужна оболонка ока залишається незмінною. І найголовніше, що неможливо знайти два абсолютно ідентичних малюнка райдужної оболонки ока, навіть у близнюків. Для отримання

індивідуальної записи про райдужну оболонку ока чорно-біла камера робить 30 записів в секунду. Ледве помітний світло висвітлює райдужну оболонку, і це дозволяє відеокамері сфокусуватися на райдужці. Одна із записів потім оцифровується і зберігається в базі даних зареєстрованих користувачів. Вся процедура займає кілька секунд, і вона може бути повністю комп'ютеризована за допомогою голосових вказівок і автофокусування. Камера може бути встановлена на відстані від 10 см до 1 метра, в залежності від скануючого обладнання. Термін «сканування» може бути оманливим, оскільки в процесі отримання зображення проходить не сканування, а просте фотографування. Потім отримане зображення райдужної оболонки перетворюється в спрощену форму, записується і зберігається для подальшого порівняння. Окуляри та контактні лінзи, навіть кольорові, не діють на якість аутентифікації.

- Метод аутентифікації по сітківці ока отримав практичне застосування приблизно в середині 50-х років минулого століття. Саме тоді була встановлена унікальність малюнка кровоносних судин очного дна (навіть у близнюків дані малюнки не збігаються). Для сканування сітківки використовується інфрачервоне випромінювання низької інтенсивності, спрямоване через зіницю до кровоносних судинах на задній стінці ока. З отриманого сигналу виділяється кілька сотень особливих точок, інформація про яких зберігається в шаблоні. До недоліків подібних систем слід в першу чергу віднести психологічний фактор: людині неприємно дивитися в темний отвір, де щось світить в око. До того ж, подібні системи вимагають чіткого зображення і, як правило, чутливі до неправильної орієнтації сітківки. Сканери для сітківки ока набули великого поширення для доступу до надсекретних об'єктів, оскільки забезпечують одну з найнижчих ймовірностей помилки першого роду (відмова в доступі для зареєстрованого користувача) і майже нульовий відсоток помилок другого роду.

- Аутентифікація по геометрії руки використовує форму кисті руки. Через те, що окремі параметри форми руки не є чимось унікальним, доводиться використовувати кілька характеристик. Скануються такі параметри руки, як вигини пальців, їх довжина і товщина, ширина і товщина тильного боку руки, відстань між суглобами і структура кістки. Також геометрія руки включає в себе дрібні деталі (наприклад, зморшки на шкірі). Хоча структура суглобів і кісток є відносно сталими ознаками, але розпухання тканин або удари руки можуть спотворити вихідну структуру. Проблема технології: навіть без урахування можливості ампутації, захворювання під назвою «артрит» може сильно перешкодити застосуванню сканерів. Надійність аутентифікації по геометрії руки порівнянна з аутентифікацією за відбитком пальця. Системи аутентифікації по геометрії руки широко поширені, що є доказом їх зручності для користувачів та почали використовуватися в світі на початку 70-х років.

- Біометрична аутентифікація людини по геометрії особи досить поширений спосіб ідентифікації і аутентифікації. Технічна реалізація представляє собою складну математичну задачу. Широке застосування

мультимедійних технологій, за допомогою яких можна побачити достатню кількість відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах і інших місцях скупчення людей, стало вирішальним у розвитку цього напрямку. Для побудови тривимірної моделі людського обличчя, виділяють контури очей, брів, губ, носа, і інших різних елементів особи, потім обчислюють відстань між ними, і за допомогою нього будують тривимірну модель. Щоб знайти цю унікальну шаблону, відповідного певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту особи, нахилу, зміни освітленості, зміни виразу. Діапазон таких варіантів варіюється в залежності від цілей застосування даного способу (для ідентифікації, аутентифікації, віддаленого пошуку на великих територіях і т. д.).

- Аутентифікація за термограмою особи – спосіб, заснований на дослідженнях, які показали, що термограма особи унікальна для кожної людини. Термограма виходить за допомогою камер інфрачервоного діапазону. На відміну від аутентифікації за геометрією особи, даний метод розрізняє близнят. Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, температура тіла, охолодження шкіри обличчя в морозну погоду не впливають на точність термограми але цей метод на даний момент не має широкого поширення.

Отже, біометричні системи аутентифікації працюють в активному, а не пасивному режимі і майже завжди мають на увазі авторизацію. Хоча дані системи не ідентичні системам авторизації, вони часто використовуються спільно (наприклад, в дверних замках з перевіркою відбитка пальця).

Список використаних джерел

1. Болл М.Р. Руководство по биометрии. — М.: Техносфера, 2013. - С. 23. — 368 с.

2. Климакін С. П. Ера біометрики. [Навчальний посібник]/ Климакін С. П. – К.: «Слово», 2016. – 81 с.

3. Попов М.С. Біометричні системи безпеки. / Попов М.С., Петруненков А. А., Черномордик О. М. – К.: «Ідея», 2015.- 90с.

4. Рахта С.В. Райдужна оболонка ока. / Рахта С.В.– К.: Корінь, 2014. – 58 с.

5. Шаров В.Д. Біометричні методи комп’ютерної безпеки. [Навчальний посібник] / Шаров В.Д., Ломізова В.М., Бараковських Д.О. та ін. - М.: Рос. Екон. Акад., 2016. - 98 с.

Дем'яненко В.,
студентка ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

БІОМЕТРИЧНІ ХАРАКТЕРИСТИКИ: ВІДБИТКИ ПАЛЬЦІВ

Біометрія – це наука, що систематизує знання про методи та засоби ідентифікації людей, які здобуваються шляхом отримання та дослідження фізіологічних або поведінкових характеристик людини. Для використання цих даних на практиці створюються біометричні системи аутентифікації, які містять у собі біометричну інформацію та виконують процес доказу і перевірки особистості.

Біометричні системи аутентифікації працюють за двома регламентами: веріфікації та ідентифікації. Під час веріфікації отримані біометричні дані порівнюються з існуючими біометричними шаблонами, що відповідає на питання «Чи ви той, за кого себе видаєте?». У процесі ідентифікації відбувається порівняння інформації з багатьма екземплярами для встановлення особистості, тобто отримується відповідь на запитання: «Хто ви?».

Найпоширенішим на даний час методом біометричної ідентифікації є ідентифікація за відбитками пальців. Цей метод використовує унікальність малюнка папілярних ліній на дистальних фалангах пальців. Відбитки отримають за допомогою сканерів. Найчастіше використовують оптичні сканери, рідше – прокатні та ємнісні. Готові відбитки отримуються у кілька етапів:

1. Формується зображення відбитка пальця. Зчитування візерунка проводиться за допомогою вбудованої камери пристрою, чи за допомогою виявлення різниці потенціалів електричного поля між западинами та горбками папілярного візерунка. Сучасні технології дозволяють комбінувати ці методи. Результатом проведення цих операцій є готовий чорно-білий знімок відбитка.

2. Знімок інтерпретується в математичну модель, яка має вигляд цифрового коду.

3. Відбувається процедура порівняння цифрової моделі з шаблонами в базі даних для пошуку відповідників.

Безпосередньо процедура ідентифікації може виконуватись за допомогою встановлених на вході зчитувачів відбитків, що підключені до комп'ютера або, наприклад, вбудований сканер смартфона.

Ідентифікація за допомогою відбитків пальців широко застосовується по всьому світові тому що має безліч переваг: зручність та легкість використання, відсутність необхідності набирати паролі чи заносити ключі, мізерна можливість втрати свого «паролю», автоматизація процесу ідентифікації, швидкість роботи, стійкість до підробки, невеликий розмір сканерів, які вже сьогодні вбудовують у смартфони. Слід відзначити, що відбитки пальців, як біометрична характеристика, на даним момент є найдавнішими, а тому і

найбільш дослідженими, що дає їм велику перевагу над іншими характеристиками, такими як геометрія обличчя, голос, райдужна оболонка ока та ін.

Наукою, що вивчає методи встановлення особистості за допомогою відбитків пальців, називається дактилоскопія. Унікальність малюнків пальців вона пояснює тим, що доки не вдалося знайти двох людей з однаковими відбитками пальців, навіть у близнюків вони різняться. Перешкодою до визнання цього твердження стовідсотково вірним становить розмір вибірки - на сьогоднішній день досліджено відбитки не усіх людей. Причиною певної сумнівності щодо визнання методу ідентифікації відбитками пальців універсальним становить також рідкісна генетична мутація – адерматогліфія. У її носіїв цілком відсутній папілярний візерунок. Проте відсоток таких людей досить малий – за даними на 2016 рік виявлено всього чотири родини носіїв.

На відміну від аутентифікації користувачів паролем або ключем, біометричні технології завжди імовірнісні. Саме тому були введені спеціальні терміни, такі, як FAR FRR. Критерій FAR (False Acceptance Rate) визначає ймовірність сплутування однієї людини з іншою. Його також називають коефіцієнтом помилкового доступу чи помилкою другого роду. Критерій FRR (False Rejection Rate), який ще зветься помилкою першого роду або коефіцієнтом помилкової відмови в доступі, визначає ймовірність того, що людина може бути не розпізнана системою. Усі системи розпізнання відбитків пальців намагаються мінімізувати показники FAR та FRR, проте між ними існує залежність, тобто, при зменшенні FAR, FRR збільшується та навпаки. Щоб відчути вірогідності FAR та FRR, можна оцінити, як часто будуть виникати помилкові збіги, якщо встановити систему ідентифікації на прохідній організації з чисельністю персоналу N людей. Вірогідність помилкового збігу отриманого сканером відбитка пальцю для бази даних з N відбитків дорівнює $FAR * N$. Також, слід врахувати, що кожного дня через пункт доступу проходить також приблизно N людей. Тоді вірогідність помилки за робочий день $FAR * N * N.$ Звісно, в залежності від цілей системи ідентифікації, вірогідність помилки за одиницю часу може сильно змінюватися, проте якщо прийняти допустимим одну помилку протягом робочого дня, то

$$FAR * N^2 \approx 1 \rightarrow N \approx \sqrt{\frac{1}{FAR}}$$

Тоді отримаємо, що стабільна робота системи ідентифікації при FAR=0.1% =0.001 можлива при чисельності персоналу N≈30.

Для обчислення критеріїв FAR та FRR для відбитків пальців використовувались статистичні дані VeriFinger SDK, які вже кілька років одержували перемогу у міжнародному змаганні «International Fingerprint Verification Competition», де змагались алгоритми розпізнавання за пальцем. У результаті було отримане значення FAR = 0,001% та FRR = 0,6% при чисельності персоналу N ≈ 300, що свідчить про досить велику точність методу.

Жоден пристрій не може бути абсолютно досконалим, і біометричні системи – не виняток. Проте розвиток біометричних систем є однією з пріоритетних ланок розвитку сучасних технологій кібербезпеки. Для України цей розвиток – це ще один спосіб іти в ногу з часом, покращувати рівень безпеки та комфорту громадян. Саме тому актуальність біометричної ідентифікації, зокрема відбитками пальців, як найбільш популярного її відгалуження, росте з кожним днем.

Список використаних джерел

1. Белкин П.Ю., Михальский О.О., Першаков А.С.// Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов. // М.: Радио и связь, 1999 – 168 с.
2. Болл Р.М., Коннел Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У. // Руководство по биометрии. // — М.: Техносфера, 2007. – 368 с.
3. Горелик А.Л. Методы распознавания // А.Л. Горелик, В.А. Скрипкин – М.: Высшая школа, 1984 – 220 с.
4. Мартынова Л. Е., Умницын М. Ю., Назарова К. Е., Пересыпкин И. П. //Исследование и сравнительный анализ методов аутентификации // Молодой ученый, 2016 – 93 с.
5. Wikipedia [Электронный ресурс] : Биометрические системы аутентификации. – Режим доступа: https://ru.wikipedia.org/wiki/.

Дресвяннікова В.,
студентка ОС «Бакалавр» спеціальності «Право»
Науковий керівник: старший викладач кафедри права та публічного адміністрування Барегамян С.Х.
Маріупольський державний університет

ІНТЕРНЕТ-ПІРАТСТВО ЯК ПОРУШЕННЯ АВТОРСЬКИХ І СУМІЖНИХ ПРАВ

Сучасний розвиток інформаційних технологій глобальної інтернет-мережі відрізняється своєю швидкістю та невпинністю, а саме тому зумовлює збільшення кількості правопорушень, що пов’язані з використанням об’єктів авторського права.

Останнім часом підробки відомих брендів, безкоштовне завантаження музики чи відео, користування неліцензійними програмами настільки буденні та поширенні явища, що не викликають ніякої підозри серед користувачів.

На перший погляд, користування такими піратськими ресурсами – це злочин без жертв. Проте проблеми, пов’язані з інтелектуальним піратством, є одними з найнебезпечнішими формами порушення авторського права і суміжних прав. Недотримання прав інтелектуальної власності створює значні перепони для економічного та технологічного розвитку України, а також має негативний вплив на її інвестиційну привабливість.

Дослідженню зазначеної проблеми приділялось досить багато уваги, зокрема, слід відзначити праці наступних науковців: С. Войтко, А. Дідович, Ю. Логвінов, М. Мельников, Є. Ходаківський, О. Штефан та ін.

Метою дослідження є правовий аналіз поняття «інтернет-піратство», його законодавче закріплення, а також розгляд передбаченого покарання за це діяння.

Порушення авторських прав можна розподілити на два види: порушення немайнових прав, тобто плагіат і порушення майнових прав – піратство. Плагіат, коротко кажучи, – це привласнення авторства, а також використання чужого твору в своїх трудах без посилання на автора [1].

Термін «піратство» походить з англійської мови – «pirасу» – і означає порушення прав інтелектуальної власності [2], а також незаконне, навмисне використання об'єкта інтелектуальної власності з метою отримання матеріальної вигоди [1].

Вперше в Україні термін «піратство» був закріплений у Законі України «Про авторське право та суміжні права».

Стаття 50 Закону України «Про авторське право та суміжні права» визначає наступні дії, що можуть кваліфікуватися як порушення авторського права, а відтак як і підстави для звернення до суду за захистом:

- вчинення будь-яких дій, які порушують особисті немайнові права та майнові права авторського права;
- піратство у сфері авторського права, тобто опублікування, відтворення, ввезення на митну територію України, вивезення з митної території України і розповсюдження контрафактних примірників творів (у тому числі комп'ютерних програм і баз даних);
- плагіат – оприлюднення (опублікування), повністю або частково, чужого твору під іменем особи, яка не є автором цього твору;
- ввезення на митну територію України без дозволу осіб, які мають авторське право, примірників творів (у тому числі комп'ютерних програм і баз даних);
- вчинення дій, що створюють загрозу порушення авторського права;
- підроблення, зміна чи вилучення інформації, зокрема в електронній формі, про управління правами;
- розповсюдження, ввезення на митну територію України з метою розповсюдження, публічне сповіщення об'єктів авторського права, з яких без дозволу суб'єктів авторського права вилучена чи змінена інформація про управління правами, зокрема в електронній формі [3].

Треба зауважити, що зазначений перелік є загальним та невичерпним, оскільки сучасний розвиток технологій значно розширив діапазон можливих правопорушень у сфері реалізації результатів творчої, інтелектуальної діяльності, у тому числі й у сфері авторського права [4].

Отже, Закон дає визначення терміна «піратства» через категорію «контрафактна продукція». Проте ототожнювати ці поняття не можна, бо, за

своїм змістом піратська діяльність є більш широким поняттям, а контрафактна діяльність із виготовлення об'єктів авторського права є елементом піратства [5]. Отож, ці поняття можна вважати відображенням одного й того ж явища: контрафакція – це товар, який незаконно виготовляється, відтворюється і (або) розповсюджується, а піратство – це безпосередньо опублікування, відтворення, розповсюдження таких контрафактних примірників. Тобто незаконна дія – це піратство, а її предмет – контрафактна продукція [4].

Інтернет-піратство є окремим видом неправомірної діяльності, що завдає величезних збитків, проявляється у незаконному виготовлені та розповсюджені контрафактних примірників, тобто об'єктів авторського права. Суть Інтернет піратства полягає у відтворенні і розповсюдженні мережею фільмів, музичних творів, комп'ютерних програм, іграшок, інших об'єктів,що підпадають під охорону авторського права, без дозволу автора або іншої особи, яка має виключні та майнові права без дозволу на їх використання у встановленому законом порядку [4].

Найпопулярнішим способом, яким контент поширюється у глобальній мережі є протокол p2p. Так, при такому способі обміну файлами одна сторона надсилає файл іншій стороні у тому вигляді, у якому він був переданий. При використанні такого протоколу кожна із сторін є і відправником і отримувачем, тому що файл відправляється та отримується частинами.

В такому випадку проблемність правового регулювання полягає у тому, що торрент-сайти не містять самого об'єкта авторського права, а лише посилання на осіб, які ним володіють, при чому ці особи можуть перебувати в найрізноманітніших куточках землі одночасно [4].

У зв'язку з інтеграційними процесами в Україні доречно згадати про європейське визначення терміну «піратство» та законодавче закріплення цього явища.

Отож, регламент № 3295/94 Ради Європейського співтовариства від 22 грудня 1994 р. визначає «піратські товари» як товари, які є копіями або містять копії, виготовлені без згоди володільця авторських або суміжних прав, або володільця прав стосовно рисунка чи моделі, зареєстрованих у відповідному національному праві [6].

Щодо законодавчого закріплення попереднього визначення, то воно є в Рекомендації «Про заходи проти звукового та аудіовізуального піратства», прийнятій Кабінетом міністрів Ради Європи, де мова йде про те, що недозволені відтворення, розповсюдження або сповіщення для загального відома з комерційною метою творів, фонограм і виконань, захищених авторським правом і суміжними правами, в цілому розглядаються як «піратство», є незаконною діяльністю [7].

В Україні є два види відповідальності передбачені за порушення авторського права, тобто за піратство: адміністративна та кримінальна. Ознакою, що дозволяє визначити межу між адміністративною та кримінальною відповідальністю є комерційний масштаб.

Зокрема, за статтею 176 Кримінального кодексу України, піратство буде вважатися кримінально караним, якщо відповідними діями було завдано матеріальної шкоди у значному розмірі, а саме якщо її розмір у двадцять і більше разів перевищує неоподатковуваний мінімум доходів громадян [8].

Недоотримання ВВП та відповідне зменшення податкових надходжень,втрати на митних зборах, відтік високоінтелектуальних кадрів, зменшення інвестиційної привабливості країни, – все це втрати, що зазнає держава від інтернет-піратства. Але ж не треба забувати і про морально-політичні втрати такі як: втрата авторитету держави на міжнародній арені, формування в суспільстві правового нігілізму та почуття вседозволеності, втрата стимулів до інтелектуальної праці тощо [2].

Отже, виходячи з вище викладеного, можна зазначити, що порушення авторського права у вигляді інтернет-піратства – це актуальна проблема, яка потребує нагального вирішення, адже вона завдає неабиякої шкоди як окремим суб'єктам, так і державі. Важливо, аби в найближчий час українське законодавство зробило певний поступ у сфері інтелектуальної власності, зокрема авторського права та його практичного застосування, а саме розробило спеціальний нормативно-правовий акт, який регулював би питання авторського права в Інтернет мережі

Список використаних джерел

1. Бондаренко С. В. Авторське право та суміжні права: курс лекцій / С. В. Бондаренко. – К.: Ін-т інтел. власн. і права, 2008. – 288 с.
2. Кочина О. Поняття та види інтелектуального піратства в Україні / О. Кочина // Підприємництво, господарство і право. – 2016. – №6. –С. 19-22
3. Про авторське право та суміжні права [Електронний ресурс] : Закон України від 26.04.2017 р. № 3792-12. – Режим доступу: www.rada.gov.ua
4. Кирилюк А. В. Правопорушення авторських прав в інтернеті: поняття та види / А. В. Кирилюк // Часопис цивілістики. – № 22. –С. 117-121.
5. Штефан О. Дещо до питання про порушення у сфері авторського права / О. Штефан // Теорія і практика інтелектуальної власності. –2009. – № 6. – С. 3-13.
6. Регламент № 3295/94 Ради Європейського співтовариства від 22 грудня 1994 р. // [Електронний ресурс]. – Режим доступу : do.gendocs.ru/docs/index-62386.html?page=6
7. Липцик Д. Авторське право та суміжні права / Д. Липцик. – пер. с фр.; предисловие М. Федотова. – М. : Ладомир: изд-во ЮНЕСКО. – 2002. – 788 с.
8. Кримінальний кодекс України [Електронний ресурс] : Закон України від 05.04.2001 р. № 2341-III. – Режим доступу: www.rada.gov.ua

Жук Т.,
студентка ОС «Магістр» спеціальності «Журналістика (журналістика)»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ДЖЕРЕЛА ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА

У зв'язку зі стрімким розвитком інформаційних технологій і їх проникненням у всі сфери людської діяльності зросла кількість злочинів, спрямованих проти інформаційної безпеки. Велику зацікавленість з боку кібер-злочинців викликає діяльність і державних структур, і комерційних підприємств. Насправді ризик чатує не лише на крупні компанії, але й на окремих користувачів. За допомогою різних засобів злочинці отримують доступ до персональних даних – номерів банківських рахунків, кредитних карт, паролей, виводять обчислювальну систему з ладу або дістають повний доступ до комп'ютера. Надалі такий комп'ютер може використовуватися як частина зомбі-мережі – мережі заражених комп'ютерів, які використовують зловмисники для проведення атак на сервери, розсилки спаму, збору конфіденційної інформації, розповсюдження нових вірусів і троянських програм.

Актуальність роботи полягає у тому, що на сьогоднішній день зростає загроза несанкціонованого доступу до персонального комп'ютера будь-якого користувача. При цьому, особиста інформація має велику цінність для кожної окремої людини, а отже і методи її захисту мають бути своєчасними та відповідати швидкому розвитку загрози кібербезпеки.

Мета роботи – розглянути найпоширеніші джерела несанкціонованого доступу до персонального комп'ютера. Мета дослідження досягається такими завданнями:

- надати визначення поняття «несанкціонований доступ»;
- визначити основні чинники загроз несанкціонованого доступу;
- виокремити шляхи поширення загроз.

Несанкціонований доступ – це доступ до інформації з порушенням правових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, які не мають дозволу на доступ до цієї інформації [1].

Основними чинниками, що впливають на характер загрози, є такі чинники:

1. Антропогенний чинник, що обумовлений людськими діями, які можуть привести до порушення безпеки інформації. Такі дії можуть бути кваліфіковані, як навмисні або випадкові злочини. Джерела, дії яких можуть привести до порушення безпеки інформації можуть бути як зовнішніми, так і

внутрішніми. Такі джерела можливо спрогнозувати і прийняти необхідні міри [2].

2. Техногенний чинник, що обумовлений технічними засобами, є менш прогнозованим, і залежить від можливостей техніки, а тому вимагають особливої уваги [2].

3. Стихійний чинник, що обумовлений обставинами, які неможливо передбачити. Такі джерела загроз неможливо передбачити, а тому міри проти них мають прийматися завжди та своєчасно оновлюватись [2].

Важливо зазначити, що найпоширенішим чинником є саме людський. Виходячи з цього, існують декілька основних шляхів поширення загроз.

Перший і найголовніший – мережа Інтернет. Вона унікальна тим, що не може належати певним особам, а також не має територіальних меж. Саме це сприяє розвитку різноманітних та тематикою і типом веб-ресурсів. Ці особливості надають зловмисникам можливість скоєння злочинів в Інтернеті, уникаючи покарання та на умовах майже повної анонімності. Найчастіше зловмисники розміщують віруси і шкідливі програми на звичайних веб-ресурсах, маскуючи їх під корисне програмне забезпечення [3].

Локальна мережа, або інтранет – це внутрішня мережа, спеціально розроблена для управління інформацією усередині компанії або приватної домашньої мережі. Інтранет є єдиним простором для зберігання, обміну і доступу до інформації для всіх комп'ютерів мережі, тому, якщо один з комп'ютерів у мережі заражений, усі інші також знаходяться у потенційній небезпеці. Електронна пошта також може бути шляхом для передачі шкідливих програм. Наявність поштових застосунків практично на кожному комп'ютері і використання шкідливими програмами вмісту електронних адресних книг для виявлення нових жертв забезпечують сприятливі умови для розповсюдження шкідливих програм. Користувач зараженого комп'ютера, сам того не підозрюючи, розсилає заражені листи адресатам, які у свою чергу відправляють нові заражені листи або спам [3].

Знімні носії інформації — дискети, CD-диски, флеш-карти — на сьогоднішній день вже не так популярні, але все ж можуть становити загрозу для безпеки персональних даних. При активуванні файлу знімного носія, що містить шкідливий код, є загроза пошкодити дані на вашому комп'ютері і розповсюдити вірус на інші носії інформації або комп'ютери мережі [3].

Загрозу також може становити і Wi-Fi маршрутизатор, оскільки зловмисники можуть перехоплювати інформацію, що передається між комп'ютером та роутером [4].

Список використаних джерел

1. Охрименко С.А., Черней Г.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // НТИ. Сер.1, Орг. и методика информ. работы : журнал. — 1996. — № 5. — С. 5-13.

2. Основы информационной безопасности : учеб. пособие / Ю.Г. Крат, И.Г. Шрамкова. – Хабаровск : Изд-во ДВГУПС, 2008. –112 с.

3. Блинов А. М. Информационная безопасность : Учеб. пособие. Часть 1 / А. М. Блинов.–СПб.: СПБГУЭФ, 2010. – 96 с.

4. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — 98 с.

Захарова Г.,
студентка ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: старший викладач Дяченко О.Ф.
Маріупольський державний університет

БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ

Електронна пошта – це один з найбільш викростивуваних видів сервісу, як в корпоротивних, так і в Інтернет. Електронна пошта забезпечує внутрішній і зовнішній інформаційний обмін, формує транспортний протокол корпоротивних додатків, також являється засобом утворення інфаструктури електронної комерції. Завдяки цих функцій електронна пошта розв'язує одну з важливих на даний момент задач – формує єдиний інформаційний простір.

Електронна пошта має такі преваги: оперативність та легкість використовування, доступність, універсальність форматів листів і вкладень, надійність та швидкість інфаструктури доставки.

Але, не варто забувати про ризики. Доступність електронної пошти перетворюється в недолік, коли користувачі починають застосовувати пошту для розсилки спаму, легкість у використанні та безконтрольність приводить до витоку інформації.

Рівень захисту даних в системі електронної пошти впливає на загальний рівень інформаційної безпеки організації, а, отже, і ефективність її діяльності. Це обумовлює важливість створення надійного захисту для цього виду комунікацій. Більшість проблем, з якими зіштовхуються користувачі електронної пошти (спам, віруси, різноманітні атаки на конфіденційність листів і т.д.), пов'язані з недостатнім захистом сучасних поштових систем. Найбільш типові засоби для атак систем електронної пошти:

- Сніффери (Sniffer). Являють собою програми, що перехоплюють усі мережні пакети, що передаються через визначений вузол. За допомогою сніфферів можна дізнатися текст листа, імена користувачів і паролі.
- IP-спуфінг (spoofing). Ця хакерська атака можлива, коли зловмисник, що знаходиться усередині організації або поза її видає себе за санкціонованого користувача. Зловмисник, помінявши таблиці маршрутизації даних і направивши трафік на хибний IP-адресу, може сприйматися системою як санкціонований користувач і, отже, мати доступ до файлів, додатків, і в тому числі до електронної пошти.

•Man-in-the-Middle (<Людина в середині>) Тип атаки, що полягає в перехопленні всіх пакетів, переданих за маршрутом від провайдера в будь-яку іншу частину Мережі. Вони цілком можуть використовуватися для перехоплення повідомлень електронної пошти та їх змін, а також для перехоплення паролів та імен користувачів.

• Атаки на рівні додатків використовують добре відомі слабкості серверного програмного забезпечення (sendmail, HTTP, FTP). Можна, наприклад, отримати доступ до комп'ютера від імені користувача, працюючого з додатком тієї ж електронної пошти [1].

Отже, захист електронної пошти, повинен починатися ще на рівні IT-інфрастуктури організації.

Для захисту мережевої інфраструктури використовується чимало всіляких заслонів і фільтрів: SSL (Secure Socket Layer), TSL (Transport Security Layer), віртуальні приватні мережі. Це, насамперед, сильні засоби аутентифікації, наприклад, технологія двофакторної аутентифікації, при якій відбувається поєднання того, що у вас є, з тим, що ви знаєте. Ця технологія використовується, наприклад, в роботі звичайного банкомату, який ідентифікує по картці і за кодом. Для аутентифікації в поштовій системі теж буде потрібен токен, який генерує за принципом унікальний одноразовий пароль. Його перехоплення марне, оскільки він буде вже використаний і виведений з ужитку. Однак така міра ефективна тільки проти перехоплення паролів, але не проти перехоплення іншої інформації (наприклад, повідомлень електронної пошти).

Інші засоби захисту полягають в ефективному побудові та адмініструванні мережі. Мова йде про побудову комутованій інфраструктури, заходи контролю доступу та фільтрації вихідного трафіка, виправлення помилок в програмному забезпеченні за допомогою модулів і регулярному його оновленні, установка антивірусних програм та ін.

І, нарешті, самий ефективний метод – криптографія, що не запобігає перехопленню інформації і не розпізнає роботу програм для цієї мети, але робить цю роботу марною. Криптографія також допомагає від IP-спуфінга, якщо використовується при аутентифікації. Поштову систему із засобами криптозахисту є сенс використовувати в якості корпоративної поштової системи, яку можна розгорнути на власній IT-інфраструктурі, проблеми безпеки при цьому вирішуються найчастіше за рахунок установки шлюзу або заслонів на з'єднанні корпоративної мережі з Internet і на поштовому сервері. Цей варіант призначений, перш за все, для великих організацій з сильними IT-підрозділами і великими бюджетами. Для середніх і малих організацій переважно варіант оренди корпоративної поштової системи у ASP-провайдера. Від корпоративних поштових систем часто вимагають додаткових функцій підтримки спільної діяльності співробітників компанії. В якості корпоративних поштових систем часто згадуються Lotus Notes і Microsoft Exchange, які містять занадто багато цих додаткових функцій і менш підходять для Web-хостингу.

Таким чином, всі перераховані вище факти ще раз підтверджують

необхідність застосування в системах безпеки корпоративних мереж систем контролю вмісту електронної пошти, які здатні не тільки забезпечити захист системи електронної пошти і стати ефективним елементом управління поштовим потоком, але і значно підвищити ефективність діяльності підприємства чи організації.

Список використаних джерел

1. Резниченко О., Суржиков Є. Захист електронної пошти [Електронний ресурс]. – Режим доступу: http://easy-code.com.ua/2010/11/zaxist-elektronnoї-poshti/

Конєва О.,
ОС «Бакалавр»
спеціальності «Системний аналіз»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ ОСОБИ

Один з перших методів біометричної ідентифікацією людини - це аналіз геометричних характеристик. Спочатку він застосовувався в криміналістиці і був там детально розроблений. Потім з’явилися комп’ютерні реалізації цього методу. Суть його полягає у виділенні набору ключових точок (або областей) особи і наступному виділенні набору ознак. Кожна ознака є або відстанню між ключовими точками, або відношенням таких відстаней. На відміну від методу порівняння еластичних графів, тут відстані вибираються не як дуги графів. Набори найбільш інформативних ознак виділяються експериментально.

Ключовими точками можуть бути куточки очей, губ, кінчик носа, центр очі і т. п. рис.1. В якості ключових областей можуть служити прямокутні області, які включають в себе: очі, ніс, рот.

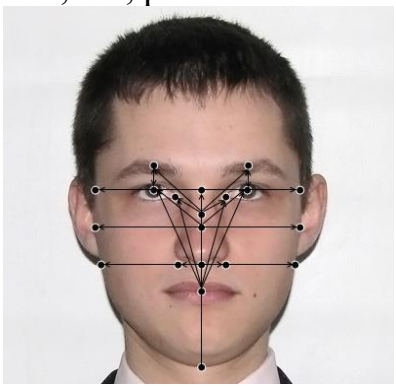


Рис.1 – Точки, що застосовуються в системах автоматичної ідентифікації

У процесі розпізнавання порівнюються ознаки невідомої особи з ознаками, що зберігаються в базі. Задача знаходження ключових точок наближається до трудомісткості безпосередньо розпізнавання, і правильне знаходження ключових точок на зображенні багато в чому визначає успіх розпізнавання.

Тому зображення обличчя людини має бути без перешкод, що заважають процесу пошуку ключових точок. До таких факторів відносять окуляри, бороди, прикраси, елементи зачіски і макіяжу. Освітлення бажано рівномірне і однакове для всіх зображень. Крім того, зображення особи повинно мати фронтальний ракурс, можливо, з невеликими відхиленнями. Вираз обличчя має бути нейтральним. Це пов'язано з тим, що в більшості методів немає моделі обліку таких змін.

Таким чином, даний метод пред'являє досить суворі вимоги до умов зйомки і потребує надійного механізмі знаходження ключових точок для загального випадку. Крім того, потрібне застосування більш досконалих методів класифікації чи побудови моделі змін. У загальному випадку цей метод не є найоптимальнішим, однак для деяких специфічних задач все ж перспективний. До таких завдань можна віднести документний контроль, коли потрібно порівняти зображення обличчя, отриманого в поточний момент, з фотографією в документі. При цьому інших зображень цього людини не є, і, отже, механізми класифікації, засновані на аналізі тренувального набору, недоступні.

Розподілена система виділення геометричних характеристик осіб для розпізнавання. Розглядається технологія автоматичного розпізнавання осіб в реальному часі шляхом виділення антропометричних точок обличчя з використанням геометричного підходу, реалізується в розподіленій інтернет-системі.

Сучасний рівень розвитку комп'ютерної техніки та інтернету обумовлює виникнення широкого кола завдань, пов'язаних з біометричною ідентифікацією людини, на основі зображення особи, райдужної оболонки ока, відбитків пальців, голосу, форми вух і носа. Ідентифікація людини по обличчю може використовуватися інформаційної безпеки для розмежування доступу, банківській сфері, соціальних мережах, криміналістиці, комп'ютерних іграх, практично в будь-якій системі, де необхідна автентифікація.

Докладна архітектура системи розпізнавання осіб представлена на рис.2.

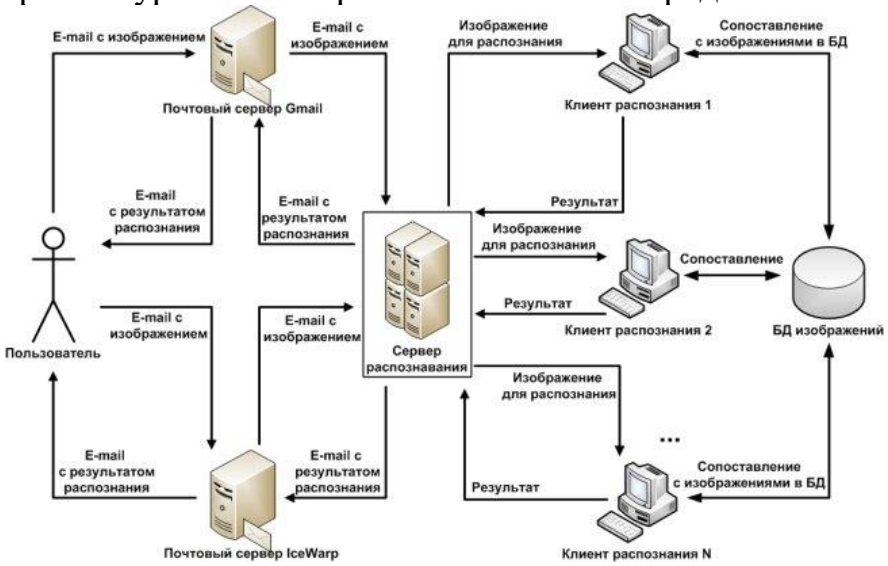


Рис. 2 – Архітектура системи розпізнавання осіб

Користувач ініціює початок роботи системи відправкою зображень на поштовий сервер, після чого це зображення потрапляє на сервер розпізнавання, який здійснює розподіл серед клієнтів розпізнавання. Клієнти розпізнавання виділяють геометричні характеристики осіб і за допомогою їх виконують зіставлення з базою зображень, після чого отриманий результат передається на сервер розпізнавання, який здійснює допомогою поштового сервера передачу результату користувачеві.

Як показує практика криміналістики, необхідно виділити близько 30 особливих точок на зображенні обличчя людини, які будуть максимально стійкими до невеликих змін (ракурсу, освітленості, міміки, косметики, віковим змінам). Групи точок мають такий пріоритет: очі, брови, ніс, рот, на їх основі можливе виділення безлічі різних параметрів для ідентифікації. В якості параметрів для розпізнавання використовуються відстані, що вимірюються вздовж горизонталей і вертикалей, так як вони вимагають менше обчислювальних витрат на їх отримання і обробку, мають високу точність вимірювання.

Для оптимального вирішення задачі розпізнавання осіб проведено аналіз існуючих алгоритмів. Після чого була обрана схема розпізнавання осіб, яку розробив Самаль Д. І. :

• пошук області обличчя на зображенні;

• виявлення центрів зіниць на портреті;

• поворот зображення (якщо потрібно) – центри зіниць повинні знаходитися на горизонтальній прямій;

• масштабування (нормалізація всіх портретів по певному відстані між зіницями);

• кадрування (вирізання прямокутної області з заданими розмірами отриманого в результаті попередніх кроків зображення);

• вирівнювання характеристик яскравості зображення, тобто застосування різних фільтрів, що змінюють контраст, інтенсивність і т. д., в залежності від вихідних значень параметрів;

• вирівнювання характеристик яскравості зображення, тобто застосування різних фільтрів, що змінюють контраст, інтенсивність і т. д., в залежності від вихідних значень параметрів;

• виділення інформації, необхідної для подальшого процесу розпізнавання, наприклад, використання детектора краю (оператор Собеля, Дериша – Deriche) або підкреслення окремих рис обличчя («High Boosting»).

У ході пошуку області обличчя на зображенні спочатку використовується алгоритм Viola-Jones, який реалізований в бібліотеці комп’ютерного зору OpenCV.

Детектор на основі алгоритму Viola-Jones є одним з кращих за співвідношенням показників ефективність розпізнавання/швидкість роботи. Також цей детектор володіє вкрай низькою ймовірністю помилкового виявлення особи. Алгоритм Viola-Jones досить стійкий (близько 20 градусів) до

повороту зображення. При куті нахилу більше 20 градусів відсоток виявлень різко падає. Проте при невеликих кутах нахилу до 10 градусів, алгоритм продовжує надійно визначати обличчя людини. На відміну від справжніх осіб, випадкові помилкові виявлення інших об'єктів не володіють такою стійкістю. Даний метод заснований на посиленні простих класифікаторів. Посилення простих класифікаторів – підхід до вирішення задачі класифікації (розпізнавання), шляхом комбінування примітивних «слабких» класифікаторів в один «сильний». Під «силою» класифікатора у даному випадку мається на увазі ефективність (якість) рішення задачі класифікації.

Для виявлення центрів зіниць на знайденій області особи використовується оператор Собеля, інверсія і метод Отсу. Оператор Собеля являє собою згортку вихідного зображення з двома масками розміром 3×3 окремо і підсумовування результатів. Виділені контури і знайдені центри зіниць, позначені хрестиками, показані на рис. 2.

Поворот, масштабування, кадрування і вирівнювання характеристик яскравості зображення забезпечують функції бібліотеки OpenCV.

В якості детектора країв, крім перерахованих раніше, можливо використовувати популярний і ефективний детектор країв Кенні, який добре зарекомендував себе. Оператор Кенні спочатку виконує згладжування на півтонового зображення, а потім формує протяжні контурні сегменти, простежуючи сусідні пікселі з великими значеннями модуля градієнта.

Висновки. Розпізнавання осіб на основі геометричних характеристик потребує надійного механізмі знаходження ключових точок для загального випадку, який забезпечується запропонованим алгоритмом. Представлена система реалізує важливі для практики функції: розпізнавання виконується в реальному часі за рахунок використання розподіленої технології розпізнавання осіб, система здатна працювати автоматично, отримуючи на вхід зображення з поштового сервера і відправляючи результат своєї роботи через поштовий сервер.

Список використаних джерел:

1. Фаулер М. Архітектура корпоративних програмних додатків.: Пер. з англ. – М: Видавничий будинок «Вільямс», 2008. – 544 с. : іл. – Хрон. тит. англ.

2. Колісник А. В., Ладиженський Ю. В. Розподілена інтернет-система автоматичного розпізнавання зображень у реальному часі / А. В. Колесник, Ю. В. Ладиженський // Інформатика та комп'ютерні технології / Матеріали V міжнародної науково-технічної конференції студентів, аспірантів та молодих науковців – 24-26 листопада 2009 р., Донецьк, ДонНТУ. – 2009, с. 206-208.

3. Зінін А. М., Кірсанова Л. З. Криміналістична фотопортретна експертиза. – М.: МВС СРСР ВНКЦ, 1991. – 88с.

4. Самаль Д. І. Алгоритми ідентифікації людини за фотопортретом на основі геометричних перетворень. Автореферат на здобуття наукового ступеня кандидата технічних наук. – Мінськ, – 2002.

5. Форсайт Д., Поинс Ж. Комп'ютерне зір. Сучасний підхід. : Пров. з англ. – М: Видавничий будинок «Вільямс», 2004. – 928 с. : іл. – Хрон. тит. англ.

Мєдвєдєва А.,
студентка ОС «Магістр»
спеціальності «Журналістика»
Науковий керівник: доцент,
кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасному суспільстві неможливо обійтися без соціальних мереж і в сучасному світі переважають інтернет технології. В даний час кожна людина, пов'язана з комп'ютером, зареєстрована хоча б в одній соціальній мережі [1].

Метою роботи є визначити та проаналізувати засоби забезпечення захисту персональних даних та конфіденційності серед користувачів у соціальних мережах.

Мета визначила наступні завдання дослідження:

- опрацювати наукову літературу за темою дослідження захисту персональних даних;
- визначити заходи безпеки під час користування соціальними мережами;
- виявити користь та шкоду соціальних мереж в Інтернеті;
- проаналізувати можливі способи захисту персональних даних в соціальних мережах.

Предметом дослідження є соціальні мережі як потенційна загроза конфіденційності та персональних даних.

Інформаційна безпека стає ключовим фактором в процесі надання електронних послуг. Сучасні інфокомунікаційні послуги відрізняються використанням великого обсягу чутливої інформації, яка потребує захисту (персональні дані, платіжна інформація, ключі і секрети).

Захист персональних даних в соціальних мережах є актуальною. Адже при реєстрації на будь-яких сайтах, вимагають персональні дані кожної людини (ПІБ, дата народження і т.д.).

Зростання популярності соціальних мереж привертає увагу викрадачів особистих даних, хакерів, спамерів, розробників вірусів [2].

Оператор соціальної мережі зобов'язаний провести обробку персональних даних, однак при цьому рівень конфіденційності і захист особистих даних покладено практично повністю на самого користувача

Cookies - невеликий фрагмент службової інформації, що поміщається веб-сервером на комп'ютер користувача. Найпростіше cookies вкрасти в місцях, найменш захищених і найбільш масових (наприклад, кафе з доступом до wi-fi).

Фішинг - вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логінів і паролів [3].

Ще один тип загроз, який мігрував в соціальні мережі з систем інтернет-банкінгу - це програми для крадіжки паролів. Вони впроваджують частини свого коду в ваш браузер для того, щоб викрасти ваші реєстраційні дані до того, як вони будуть відправлені на сервер.

У профілях Facebook ми багато про себе повідомляємо, але деякі люди йдуть ще далі і зламують пароль, отримують можливість робити зміни на сторінці і використовувати її в своїх цілях, і це вже — крадіжка особистості, одна з найсерйозніших мережевих небезпек [4].

Для захисту персональних даних у різних соціальних мережах введено декілька простих правил, які допоможуть краще захиститися в глобальній мережі.

В першу чергу слід вигадати складний пароль мінімум з 8 символів, з урахуванням регістру. Також слід увімкнути двофазну авторизацію через телефон. Не слід залишати номер свого мобільного на жодному з сайтів, блогів. Його легко відслідкувати просто використавши пошук по фото [5].

В соціальних мережах не слід використовувати геолокацію. Також слід активувати функцію заборони індексації сторінок гулом. Інформацію про себе потрібно розміщувати обдумано, аби не потрапити в зону ризику.

Список використаних джерел

1. Безопасность персональних данных в социальных сетях [Електронний ресурс] . – Режим доступу: http://human.snauka.ru/2015/11/13018

2.Виды защиты информации в социальных сетях [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/socialnyeseti94/zasita-informacii-v-socialnyh-setah/vidy-zasity-informacii-v-socialnyh-setah

3. Захист персональних даних в соціальних мережах [Електронний ресурс] . – Режим доступу: http://www.vaas.gov.ua/news/zaxist-personalnix-danix-v-socialnix-merezhax/

4. Злом фейсбук — способи і захист [Електронний ресурс] . – Режим доступу: https://insite.cc/blog/smm/vzlom-fejsbuk-sposobi-i-zahist.html

5. Як захистити персональні дані у мережі — поради спеціалістів [Електронний ресурс] . – Режим доступу: http://universe.zp.ua/?p=4505

Михайленко І.,
студентка ОС «Бакалавр»
спеціальності «Право»
Науковий керівник: старший викладач
кафедри права та публічного адміністрування Барегамян С.Х.
Маріупольський державний університет

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНИ

У кінці XX ст. інформаційно-комунікаційні технології, перш за все глобальна інформаційна мережа Інтернет, стали одним із факторів, які суттєво впливають на розвиток суспільства. Зі стрімким розвитком технологій дуже складно визначити час, коли саме поняття «прав людини» вперше застосувалось до Інтернет-середовища. Згідно з міжнародним правом, держави зобов'язані захищати, поважати і виконувати права людини та громадянина. Дане дослідження покликане проінтерпретувати універсальні стандарти та механізми захисту прав людини у новому контексті – в Інтернеті, згідно чинного законодавства.

Аналіз наукової літератури показує, що одним із перших українських науковців, хто розкриває зв'язок прав людини та Інтернету став юрист А. Пазюк, права дитини в цифрову епоху досліджує С. Лівінгстон, захист прав дитини в Інтернеті як соціально-педагогічну проблему розглядають Н. Агаркова, І. Ковчина.

Для розуміння механізму захисту прав, слід вказати основні види правовідносин, пов'язаних з Інтернетом, на основі яких виникають дані права:

– правовідносини, що реалізуються в зв'язку з використанням Інтернету (між споживачами-користувачами і постачальниками послуг доступу, телекомунікаційних та інформаційних сервісів, інформаційних продуктів і ін.);

– приватні правовідносини майнового (електронні платежі) і нематеріального характеру (міжперсональні комунікація), що здійснюються через Інтернет, в тому числі в соціальних мережах;

– публічні правовідносини, пов'язані з наданням адміністративних (управлінських) послуг між державою і приватними особами (електронне управління і ін.) і виконанням державами своїх правоохоронних функцій (відповідальність за правопорушення в Інтернеті);

– публічні правовідносини, пов'язані з управлінням Інтернетом в широкому розумінні.

Види таких правовідносин реалізуються в кіберпросторі і регулюються національним правом і міжнародним приватним правом, то останній із зазначених видів правовідносин носить змішаний (гібридний) характер і здійснюється як у віртуальному середовищі, так і поза кіберпростору. Це пов'язано з тим фактом, що в правовідносинах з управління Інтернетом беруть участь, як суб'єкти міжнародного приватного права (фізичні та юридичні особи

національного права, а також транснаціональні корпорації), так і міжнародного публічного права (держави, міжнародні організації).

Система національної безпеки будь-якої країни та її громадян 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). Діяльність із формування системи забезпечення національної безпеки України та гарантії захисту прав її громадян 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.

Кібербезпека стала пріоритетним питанням нормативно-правової бази органів інформаційно-комп'ютерного захисту, але на сьогодні не існує уніфікованої моделі побудови національної системи кібербезпеки та загальної системи захисту прав громадян у цій сфері. Але це питання є одним із пріоритетних на теперішній час, про це свідчать проекти змін до чинного законодавства та нові законопроекти, що знаходяться у початковій стадії.

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» [1]. 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. Існує й Проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю від 19.06.2015 р. Відповідні зміни передбачається внести зміни до низки законодавчих актів, зокрема, до Кодексу України про адміністративні правопорушення, законів України «Про

оперативно-розшукову діяльність», «Про Службу безпеки України», «Про контррозвідувальну діяльність», «Про основи національної безпеки України», «Про розвідувальні органи», «Про телекомунікації» [2].

Основні права людини, в тому числі свобода думки, слова і свобода інформації, зафіксовані в міжнародних актах, зокрема, в Загальній декларації прав людини, Міжнародному пакті про громадянські та політичні права, Міжнародному пакті про економічні, соціальні та культурні права, Європейській конвенція про захист прав людини та ін [3]. Ці документи створюють міжнародне розуміння суті прав людини, які набувають особливої значимості саме в своїй сукупності в умовах транскордонного Інтернету і необхідності забезпечення захисту таких прав і свобод в інтернет-просторі. Інтерпретація прав людини стосовно інформаційного суспільства та Інтернету дозволяє наділити віртуальну особистість людини цілком реальними правами, кожне з яких підтверджено і захищено тим чи іншим міжнародним документом і розкривається в національному законодавстві.

Безперечно, виконання завдання щодо захисту прав людини і дотримання домовленостей залежить, перш за все, від рівня досягнень країни і механізмів, що існують на національному рівні. Діючі національні закони, політичні рішення, процесуальні норми і механізми є ключовими факторами для реалізації прав людини не лише в реальному світі, а й у віртуальному.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України: [Електронний ресурс] : Указ Президента України від 27.01.2016 року № 96 за станом 15.03.2016 року//Урядовий кур'єр від 18.03.2016 – № 52.– Режим доступу: http://rada.gov.ua
2. Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю: [Електронний ресурс] : Законопроект від 19.06.2015 р. № 2133а. – Режим доступу: http://rada.gov.ua
3. Загальна декларація прав людини від 10.12.1948 року: [Електронний ресурс] : Генеральна Асамблея ООН; резолюція № 217А (III) від 10.12.1948 року. – Режим доступу: http://rada.gov.ua

Русаневич А.,
студентка ОС «Магістр»
спеціальності «Журналістика (зв'язки з громадськістю)»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ЗАКОНОПРОЕКТ ПРО КІБЕРБЕЗПЕКУ УКРАЇНИ: НЕДОЛІКИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

Сьогодні у міжнародному праві забороняється використання збройної агресії однією суверенною державною проти іншої. Це, насамперед, виражається через існування таких принципів як суверенної рівності держав, незастосування сили або погрози силою, мирного вирішення міжнародних спорів, територіальної цілісності держав та непорушності державних кордонів. Однак, не дивлячись на ці основоположні ідеї сучасного міжнародного права, збройна агресія продовжує існувати у сучасному світі. На початку XXI століття такі конфлікти представляють дуже велику небезпеку для всього людства. Як зазначає В. Ю. Кравченко «В останні роки стрімкий технологічний розвиток, доступність зброї і посилення процесів глобалізації спричинили трансформацію політичної боротьби» [1, с. 139].

Окрім цього, класичне розуміння поняття зброї, як виключно збройно-технічного компоненту будь-якої агресії, давно відійшло в минуле. Під зброєю розуміємо не тільки сукупність технічних пристроїв, що використовуються для ураження живої сили противника, його техніки та споруджень, а й інформаційний, економічний, політичний вплив, засоби якого справедливо вважають відповідною зброєю. З цього приводу Л. Є. Смола зазначає, що особливістю сучасних збройних конфліктів є зростання ролі невійськових способів у досягненні політичних та стратегічних цілей, які за своєю ефективністю переважають силу зброї. Автор уточнює це твердження через наявність масштабного використання методів та засобів інформаційної війни, в т. ч. з використанням світових ЗМІ [2, с. 76].

Принциповою для розуміння специфіки сучасної війни є ідея функціонального перетворення на зброю традиційно невійськових засобів силового впливу та об'єднання їх на цій підставі з власне військовими методами [3, с. 28].

В сьогоднішньому глобальному світі інформаційні технології використовуються для забезпечення національної та військової безпеки, що стало поштовхом для виокремлення самостійної середи кіберпростору. Він не має якихось встановлених кордонів або меж, але, не зважаючи на це, може вважатися міжнародним простором. Дана тема є актуальною для нашої держави у зв'язку з розгортанням на Сході України фактично військових дій та агресивними діями країни-супротивника, які поширюються на всі сфери суспільного життя, в тому числі й на інформаційну складову в контексті кіберпростору.

Підвалини для подальшого співробітництва держав було закладено Резолюцією Генеральної Асамблеї (ГА) ООН 53/70 ще у 1998 р. Своєю Резолюцією ГА ООН закликала держави-члени до співробітництва у розгляді існуючих загроз у сфері інформаційної безпеки; визначення основних понять, що стосуються інформаційної безпеки; а також до інформування Генерального Секретаря щодо доцільності розробки міжнародних принципів, які підвищать безпеку глобальних інформаційних телекомунікаційних систем та сприятимуть боротьбі з інформаційним тероризмом [4]. Уже у 2000 р. та 2001 р. Генеральною Асамблеєю ООН було підготовлено Резолюції 55/63 та 56/121 відповідно. Цими Резолюціями державам, серед іншого, рекомендується обмінюватися інформацією, експертами задля більш ефективної боротьби зі злочинним використанням інформаційних технологій, забезпечувати співпрацю на рівні слідчих органів держав [5]. Своєю Резолюцією 57/239 2003 р. «Створення глобальної культури кібербезпеки» ГА ООН вкотре підкреслює важливість сучасних інформаційних телекомунікаційних систем для розвитку суспільства і водночас наголошує, що уряди, бізнес, громадські організації та індивідуальні особи-користувачі Інтернет мають бути обізнані щодо відповідних ризиків і також вживати заходів для підвищення безпеки [6].

Основним документом у цій сфері у рамках Ради Європи є ратифікована 49-ма державами Конвенція про кіберзлочинність 2001 р. (Будапештська конвенція про кіберзлочинність). Вона набула чинності для України 1 липня 2006 р. Це – перший міжнародний акт, направлений на захист населення та міжнародне співробітництво держав у сфері кіберзлочинності [7].

У 2012 р. у Женеві відбулася Всесвітня конференція електрозв'язку МСЕ1. Під час конференції ухвалено нову редакцію Регламенту Міжнародного союзу електрозв'язку, зміни до якого не вносилися 24 роки. В Резолюції підкреслювалося, що всім зацікавленим сторонам необхідно разом працювати над розробкою стандартів та принципів в цілях захисту від кібератак та полегшення виявлення джерел кібератак.

У рамках ЄС першим документом, що регулює кіберсферу, є Директива 95/46 Європейського парламенту та Ради від 24 жовтня 1995 р. про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних. Відповідно до цієї Директиви держави-члени мають захищати основні права та свободи фізичних осіб, і, зокрема, їх право на недоторканність приватного життя щодо обробки персональних даних [8].

З метою забезпечення більш високого рівня кібербезпеки у Європейському Союзі Європейський парламент і Рада Європейського Союзу у 2004 р. створили Європейське агентство з мережевої та інформаційної безпеки. Статтею 2 Регламенту № 460/2004 передбачено такі цілі створення даного агентства: розширити можливості Співтовариства щодо реагування на проблеми інформаційної безпеки; надавати допомогу і рекомендації Комісії та державам-членам з питань, пов'язаних із мережевою та інформаційною безпекою; надавати допомогу Комісії у технічній підготовчій роботі з оновлення і

розробки законодавства Співтовариства у сфері мережевої та інформаційної безпеки [9].

У 2016 р. підписано документ, що продемонстрував собою прагнення європейських держав до співробітництва у кіберсфері. Ним стала Директива ЄС з мережевої та інформаційної безпеки (EU Network and Information Security (NIS) Directive). Її метою є досягнення високого загального рівня безпеки мережевих та інформаційних систем у рамках Союзу [10].

Після атак у 2007 р. на кіберпростір Естонії НАТО остаточно ухвалили рішення про створення Центру з підвищення кваліфікації зі спільної кібероборони – CCD COE (Cooperative Cyber Defence Centre of Excellence). Центр сфокусувався на координації кіберзахисту та створенні політики для надання допомоги союзникам під час нападів. Рішенням Північноатлантичної Ради CCD COE була створена як Міжнародна військова організація.

Відповідно до зростаючої ролі кіберпростору багато держав створюють власні національні законодавчі норми та стратегії кібербезпеки. Так, нині 27 країн-членів НАТО, Європейський Союз, 12 країн Європи, що не є членами НАТО, а також 38 країн із інших частин світу мають власні національні стратегії кібербезпеки. Серед них і Україна, де у 2016 р. Указом Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України» було затверджено національну стратегію кібербезпеки [11]. Раніше, у 2009 р., штаб-квартира НАТО ухвалила стратегічний документ «Рамки співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами». Цим актом було закладено підґрунтя для налагодження співробітництва у сфері кібербезпеки між країнами-учасниками, зокрема й Україною [12].

Кіберпростір стає ареною конфліктів між державами, організаціями та приватними особами. За сучасних умов активізації міжнародних терористичних, екстремістських організацій та злочинних структур, які використовують інформаційні технології для реалізації своїх злочинних намірів, забезпечення інформаційної безпеки є однією з найважливіших складових системи забезпечення національної і міжнародної безпеки [13, с. 120].

Не можна сказати, що кібербезпека в Україні перебуває поза увагою законодавця та інституцій безпекового сектору. На сьогодні Верховна Рада України підтримала законопроект «Про основні засади забезпечення кібербезпеки України» у другому читанні. Зазначимо, законопроект про кібербезпеку уже розглядали у другому читанні навесні 2017 року, однак депутати визнали, що він містить багато мінусів, тому відправили його на доопрацювання. Прийнятий цей законопроект був 5 жовтня 2017 року, набрання чинності якого відбудеться 9 травня 2018 року. За проект закону №2126а проголосували 257, проти – 0, утримались 18 народних обранців. Не голосував 81 депутат.

Не зважаючи на такий прогресивний крок нашої держави у сфері безпеки кіберпростору, неможна стверджувати, що даний законопроект немає недоліків. Тож, які основні проблеми законопроекту «Про основні засади кібербезпеки»?

По-перше, законопроект не визначає єдиний орган, який би здійснював оперативне управління всіма суб'єктами забезпечення кібербезпеки. РНБО здійснює лише координацію, Генштаб – оперативне управління в «особливий період». На практиці, кібервійну країна-агресор ніколи не оголошує. І, відповідно, не можна з упевненістю стверджувати, коли така війна закінчиться. Отже, без єдиного відповідального органу, що буде мати повноваження командувати всіма силами та засобами кібербезпеки, наша країна не зможе ефективно реагувати на відповідні кібератаки.

По-друге, в законопроекті щодо кібербезпеки України не визначена організація, що буде управляти впровадженням кібербезпеки на загальнодержавному рівні (та охопить не тільки силові відомства, але й академічний, громадський та приватний сектори, пересічних громадян).

Третім проблемним аспектом є те, що такий центральний орган виконавчої влади як Державну служба спеціального зв'язку має надмірні повноваження із аудиту об'єктів критичної інфраструктури, що знаходяться в приватній власності (по суті це буде весь великий та середній бізнес). Водночас, ця служба має право визначати вимоги для осіб на посади аудиторів та порядок їх атестації. Це створює можливості для зловживань, тиску на бізнес з боку держави в особі Держспецзв'язку, передумови для корупції (коли ліцензії для аудиту будуть видаватися тільки «своїм» фірмам, які, в свою чергу, будуть робити перевірки «на папері»), та суперечить політиці держави з дерегуляції.

Ще одним суперечливим фактом є продовження існування Комплексної система захисту інформації. В законопроекті зазначається, що методика аудиту кібербезпеки буде визначена на основі міжнародних стандартів. Але в той же час ніхто не відміняє поточний Закон України «Про захист інформації в інформаційно-телекомуніукаційних системах», що вимагає створення КСЗІ. Це, на думку більшості експертів та науковців, є неефективним. Окрім цього такі норми йдуть всупереч одна одній.

П'ятою проблемою, яку ми можемо виділити з огляду на положення законопроекту про кібербезпеку, є наділення СБУ надмірними правами з проведення таємних (негласних) перевірок кібербезпеки критичних об'єктів. Це по суті надає СБУ права проводити хакерські атаки на приватний бізнес. Постає питання чи це тотальне шпигунство, чи право держави атакувати приватний бізнес?

Тож, з огляду на певні недоліки, які існують у законопроекті щодо кібербезпеки, пропонуємо шляхи його вдосконалення.

1. Визначити єдиний орган, який буде здійснювати оперативне командування всіма суб'єктами забезпечення кібербезпеки (кіберпідрозділами силових відомств) у мирний час. Пропонується визначити таким органом Генштаб ЗСУ, у відповідності до моделі прибалтійських країн.

2. Визначити Офіс трансформації кібербезпеки, що здійснюватиме управління, відслідковування та координацію впровадження кібербезпеки на національному рівні (на кшталт Офісу реформ).

3. Обмежити повноваження Держспецзв'язку та СБУ об'єктами критичної інфраструктури, що є власністю держави. Щодо приватних об'єктів – віддати повноваження з регулювання та контролю кібербезпеки галузевим регуляторам, міністерствам, або саморегулюючим організаціям, створеним учасниками відповідних галузей, у відповідності до моделі, яка працює в США. Аудит кібербезпеки приватного бізнесу має проводитись незалежними аудиторами (або самими власниками критичних об'єктів), а звіти – надаватися галузевим регуляторам. Саморегулююча організація в США є прикладом, що розробила галузеві стандарити з кібербезпеки для енергетичного сектора, які можна було б запровадити в Україні.

4. Вимоги щодо атестації аудиторів необхідно замінити на вимоги наявності в штаті аудиторів, сертифікованих згідно міжнародним стандартам, що забезпечить неупередженість процесу їх атестації.

5. Негласні перевірки критичних об'єктів приватної форми власності необхідно скасувати.

Список використаних джерел

1. Кравченко В. Ю. Теорія «гібридної війни»: український вимір / В. Ю. Кравченко // Вісник Дніпропетровського університету. – 2015. – № 2. – С. 139-148

2. Смола Л.Є. Аспекти нелінійної війни в контексті україно-російського конфлікту на Донбасі / Л. Є. Смола // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін. – К. : Вид-во НПУ ім. М. П. Драгоманова, 2015. - Вип. 16. - С. 74-78

3. Горбулін В. П. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.

4. Resolution Adopted by the General Assembly 53/70. (1999). Developments in the Field of Information and Telecommunications in the Context of International Security. ccdcoe.org

5. Resolution adopted by the General Assembly 55/63. (2001). Combating the criminal misuse of information technologies. ccdcoe.org. Retrieved from URL : https://ccdcoe.org/sites/default/files/ documents/UN-001204-CriminalMisuseIT.pdf.

6. Resolution Adopted by the General Assembly 57/239. (2003). Creation of a global culture of cybersecurity . ccdcoe.org. Retrieved from URL : https://ccdcoe.org/sites/default/files/documents/ UN-021220-CultureOfCS.pdf

7. Конвенція про кіберзлочинність: Конвенція Ради Європи, Міжнародний документ від 23.11.2001 р., ратифіковано Законом N 2824-IV від 07.09.2005 р. // Офіційний вісник України. – 2007. – № 65

8. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the

Free Movement of Such Data. (1995). Official Journal of the European Communities, No. L 281/31, 24 October.

9. Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. (2004). Official Journal L 077, 13/03/2004, 0001–0011.

10. European Commission. Network and Information Security (NIS) Directive. (2016). Digital Single Market, Digital Economy & Society, Directive (EU) 2016/1148. URL : https:// ec.europa.eu/digital-single-market/news/network-and-information-security-nis-directive.

11. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. // Офіційний вісник Президента України. – 2015. – № 13

12. Framework for Cooperation on Cyber Defence Between NATO and Partner Nations. (2009). NATO/EAPC Unclassified, Document EAPC(C)D(2009)0010. uan.ua. URL : http://uan. ua/sites/default/files/41210385dod2.pdf.

13. Марков В. В. Напрями діяльності НАТО у справі протидії кіберзлочинності / В. В. Марков, О. В. Караченцев // Право і безпека. – 2014. – № 4 (55). – С. 119–123.

Федірко В.,
студент ОС «Бакалавр»
спеціальності «Системний аналіз»
Науковий керівник: доцент,
кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ЛЮДСЬКИЙ ФАКТОР У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Соціальна інженерія – це наука, що вивчає людську поведінку та фактори, які на неї впливають. Часто її використовують для маніпуляції з метою спонукати людину виконати певні дії чи розголосити конфіденційну інформацію.[1] Вона стає усе більш популярною у зв’язку з підвищенням ролі соціальних мереж, електронної пошти або інших видів онлайн-комунікації в нашому житті. У сфері інформаційної безпеки даний термін широко використовується для позначення ряду технік, використовуваних киберзлочинцями. Останні мають своїй на меті виманювання конфіденційної інформації у жертв або спонукають жертви до здійснення дій, направлених на проникнення в систему в обхід системи безпеки.

Навіть сьогодні, коли на ринку доступна величезна кількість продуктів для забезпечення інформаційної безпеки, людина все ще володіє ключами від всіх дверей. Будь то комбінація облікових даних (логін і пароль), номер кредитної карти або дані для доступу до онлайн-банку, найслабкіша ланка в системі забезпечення безпеки — це не технології, а живі люди. Таким чином, якщо

зловмисники застосовують до користувачів маніпулятивну психологічну техніку, дуже поважно знати, які прийоми найбільш характерні в даній ситуації, а також розуміти принцип їх роботи, щоб уникнути неприємностей [2].

Фішинг. Цей вид шахрайства побудований на надсиланні листа, ніби від банку чи іншою установи, в якому міститься посилання у якому необхідно ввести пароль чи іншу конфіденційну інформацію, яка необхідна шахраю. При цьому приводи для надсилання такої інформації можуть бути різними, наприклад, відновлення бази даних після її випадкової втрати.

Вішинг. Назва цього виду інтернет-шахрайства пішла від попереднього та полягає у імітування дзвінків на мобільний телефон, ніби як від банківської установи (із попередньо записаним голосом) та отриманні запиту про комунікацію із банком для підтвердження тієї чи іншої інформації. При цьому жертва отримує вимогу сказати свій пароль або іншу конфіденційну інформацію, яка необхідна для доступу до банківських рахунків.

Фармінг. Процедура полягає у перенаправленні жертви на неправдиву IP-адресу. Шахрай встановлює на комп'ютерах шкідливу програму, яка після запуску на комп'ютері забезпечує перенаправлення жертви замість шуканих нею сайтів на підроблені сайти.

Попередження про вірус на комп'ютері. В даному випадку розробник шкідливого програмного забезпечення попереджає жертву про зараження її комп'ютера вірусом і повідомляє, що для очищення операційної системи необхідно перейти за посиланням та встановити необхідну програму. Саме ця програма є шкідливою та забезпечує доступ до необхідної інформації.

Quid pro quo. Вказаний вид інтернет-шахрайства базується на вмінні особи у телефонній розмові або електронною поштою увійти в довіру до жертви (зазвичай офісного працівника) та, представившись співпробітником служби технічної підтримки, запропонувати йому вирішення проблеми, в ході чого він і отримає всю необхідну конфіденційну інформацію.

«Віртуальне викрадання». У якості засобу зв'язку виступає телефон. Зловмисники зазвичай дзвонять жертві і говорять, що член сім'ї був викрадений і для його звільнення потрібно негайно заплатити викуп. Злочинець створює відчуття терміновості і страху, жертва виконує вимоги шахрая, навіть не переконавшись, чи дійсно викрадений хтось з родичів.

«Віртуальна хвороба». Схожа на «віртуальне викрадення» схема, яка частіше за все направлена на людей похилого віку. Жертві дзвонять нібито з поліклініки, говорять, що в недавніх аналізах є ознаки небезпечного захворювання і потрібно негайно лягти на операцію для врятування життя, зрозуміло, платну. Після оплати, звичайно, нікого не оперують, тому що хвороби жодної і не було.

«Дорожне яблуко». Цей спосіб здійснення шахрайства базується на використанні фізичних носіїв інформації. Так, шахрай може залишити у будь-яких публічних місцях флеш-носій, CD-диск із таким зображенням, яке може зацікавити жертву та примусити її переглянути на своєму комп'ютері.

Зворотна соціальна інженерія. Реалізація цього способу може бути здійснена лише у випадку, коли шахрай попередньо знайомий із жертвою та заслуговує на її довіру. У такому випадку жертва сама звертається до шахрая (наприклад, системного адміністратора), із проханням допомогти відновити втрачений файл (який заховав сам шахрай). При цьому їй повідомляється, що таку дію можна зробити якнайшвидше лише зайшовши у її обліковий запис. Таким чином, жертва за власним бажанням повідомляє всю інформацію шахраю.

Претекстинг. Атака, для здійснення якої шахрай представляється іншою особою та вивідує у жертви всю необхідну інформацію. Однак такий вид інтернет-шахрайства вимагає дуже якісної підготовки та збору всієї необхідної попередньої інформації про особу [3].

У наш час треба бути дуже обачними зі своїми персональними даними, або даними які не підлягають розголошуванню. У будь-якому разі ви ніколи не будете захищені на усі сто відсотків, але правила нижче допоможуть вам не втрапити в халепу через особисту необачність.

- Завжди перевіряйте посилання, якщо збираєтесь вводити дані у них
- Не бійтесь здатися недовірливим. Якщо ви розмовляєте з людиною уперше майте на увазі те, що він або вона можуть бути зовсім не тими, ким представилися, навіть якщо вони володіють якоюсь специфічною інформацією.
- Дізнайтеся якомога більше про шляхи маніпулювання, які використовують шахраї, для того щоб у разі зустрічі із ними ви могли їх відрізнити.
- Надавайте перевагу особистим зустрічам для передачі важливої інформації

Технологічні заходи захисту залишають великі прогалини в нашій безпеці і тому всім нам слід розуміти процеси, за допомогою яких нас можуть змусити розповісти чи зробити те, що ми не хочемо [4].

Список використаних джерел

1. Вікіпедія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Соціальна_інженерія
2. Касперский [Електронний ресурс]. – Режим доступу: https://www.kaspersky.ru/blog/socialnaya-inzheneriya-ili-kak-vzlomat-cheloveka/2559/
3. Соціальна інженерія: виклики та перспективи боротьби в українському контексті[Електронний ресурс]. – Режим доступу: http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/

Хлюстов С.,
студент ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: доцент,
кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ОРГАНІЗАЦІЙНІ ЧИННИКИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Рік за роком експерти і аналітичні компанії, що спеціалізуються в області інформаційної безпеки (ІБ), відзначають одну і ту ж глобальну тенденцію: кількість кібератак збільшується, вони стають все витонченішими і призводять до все більш тяжких наслідків. В цьому сенсі не став винятком і минулий рік. Так, згідно з даними дослідження The Global State of Information Security Survey 2016, проведеного компанією PwC спільно з журналами CIO і CSO, «... в 2015 році кількість виявлених інцидентів в сфері інформаційної безпеки виросло на 38%». При цьому, як зазначає Тім Клау, партнер, керівник відділу аналізу і контролю ризиків PwC в Росії, в 2015-му в нашій країні істотно зросла не тільки фактичну кількість атак, але і наноситься ними шкоду - за його словами, середній фінансовий збиток від ІБ -інцідентов збільшився на 47%.

Разом з тим в ході проведеного в рамках дослідження опитування компаній (з охопленням 127 країн світу) головними джерелами ІБ-інцидентів були названі співробітники компаній і організацій: справжні (на це вказали 34% опитаних; роком раніше - 35%) і колишні (29% ; роком раніше - 30%).

Людські та організаційні чинники можуть бути пов’язані з технічною інформаційною безпекою.

Факторів, що впливають на безпеку комп’ютера діляться на дві категорії, а саме людський фактор і організаційний фактор. Людські чинники є важливішою за інші чинників. Вони діляться на наступні групи:

- фактори, які відносяться до управління, а саме робоче навантаження і неякісна робота персоналу;
- фактори, пов’язані з кінцевим користувачем.

Далі ми зосередимося на чотирьох людських факторах, які мають серйозні наслідки для впливу на поведінку користувачів:

1. Нестача мотивації

Багато організацій вважають, що співробітників необхідно мотивувати на безпечну поведінку з інформаційними активами, і керівництво повинно бути в змозі визначити, що мотивує їх персонал.

2. Недолік обізнаності

Недолік обізнаності пов’язаний з відсутністю загальних знань про атаки. Загальні приклади відсутності обізнаності можуть бути наступними: користувачі не знають, як визначити шпигунські програми і шпигунське ПЗ і як важливо вказувати надійний пароль. Вони не можуть захистити себе від крадіжки особистих даних, а також як контролювати доступ інших користувачів до їх комп’ютера.

3. Переконання

Спільними прикладами ризикованого переконання є наступні: вони вважають, що установка антивірусного програмного забезпечення вирішує їхні проблеми щодо захисту інформації.

4. Неписьменне користування технологіями

Навіть найкраща технологія не може досягти успіху у вирішенні проблем інформаційної безпеки без безперервного людського співробітництва та ефективного використання цієї технології. Загальні приклади неналежного використання технологія полягає в наступному: створення несанкціонованої реконфігурації систем, доступ до паролів інших, отримання неприпустимою інформації. Ризики в області комп'ютерної безпеки можна класифікувати декількома способами: перевищення привілеїв, помилки та упущення, відмова в обслуговуванні, соціальна інженерія, несанкціонований доступ, розкрадання особистих даних, фішинг, шкідливі програми і несанкціоновані копії.

П'ять ознак того, що ваша компанія знаходиться в групі ризику

Оцінки різних аналітичних компаній і експертів в області ІБ свідчать: близько половини інцидентів в сфері захисту даних пов'язано з діяльністю інсайдерів. Аналітичний центр Falcongaze підготував список ознак того, що компанії варто турбуватися питанням захисту від витоків інформації. Наведемо його.

- Відсутність корпоративної політики безпеки.
- Висока ротація кадрів і часті скорочення.
- Неконтрольоване використання співробітниками месенджерів, електронної пошти, соціальних мереж.
- Наявність співробітників, які багато часу проводять в ділових поїздках і відрядженнях.
- Неконтрольований документообіг, внаслідок чого доступ до конфіденційної інформації може отримати будь-хто.

Є й інші ознаки, що показують, що захист від витоків інформації приділено недостатньо уваги, але, як стверджують в Falcongaze, якщо хоча б один з перерахованих пунктів справедливий для вашої компанії, вона однозначно потрапляє в групу ризику.

Підведемо підсумки

У чому полягає стратегія компанії щодо захисту даних з урахуванням людського фактору?

- Вироблення спільної стратегії і концепції ІБ.
- Професійна організація програмно-апаратної інфраструктури ІБ.
- Навчання співробітників відділу ІБ, оптимальний розподіл їх функцій щоб уникнути дефіциту людських ресурсів.
- Регулярне навчання та тренінги рядових співробітників і керівників для підвищення загальної грамотності в сфері захисту інформації з моделюванням часто зустрічаються загроз.

•Регулярне проведення аудиту з подальшим виявленням вразливих місць структури інформаційної безпеки.

Список використаних джерел

1. Хабрахабр – самое крупное в Рунете сообщество людей, занятых в индустрии высоких технологий : [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/344542/
2. Security : [Електронний ресурс]. – Режим доступу: https://www.itweek.ru/security/article/detail.php?ID=183714
3. Softline.rbc: [Електронний ресурс]. – Режим доступу: http://softline.rbc.ru/page/rol-chelovecheskogo-faktora/1

Хоцький А.,
студент ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: старший викладач Дяченко О. Ф.
Маріупольський державний університет

МЕТОДИ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В ІНТЕРНЕТІ

Забезпечення досить високої анонімності суб'єкта при його взаємодії з адресатом в інформаційно-обчислювальних мережах відноситься до числа складних проблем сучасних інформаційних технологій. Нами розглянуто властивість анонімності з технічної точки зору, коли втрата конфіденційності пов'язана з програмно-апаратними засобами, а не з соціальним аспектом.

Мета нашого дослідження виявити переваги і недоліки найбільш поширених методів забезпечення анонімності користувача. Розглянимо ці методи з різною архітектурою.

Узагальнена назва технологій VPN (Virtual Private Network), це тип технологій що дозволяє забезпечує одне або кілька мережевих з'єднань [1].

1) Найбільш широко використовується тип технологій PPTP. Він швидкий, легко налаштовується, проте вважається найменш захищеним в порівнянні з іншими;
2) Протоколи L2TP, L2TP забезпечують транспорт пакетів, IPSec відповідає за шифрування. Дана зв'язка має більш сильне шифрування, ніж PPTP, забезпечує цілісність повідомлень і аутентифікацію сторін;
3) OpenVPN – найбільш безпечний, відкритий протокол, а отже, найбільш поширений, дозволяє обходити багато блокування, але вимагає окремого програмного клієнта;
4) SSTP безпечний, як і OpenVPN, але сильно обмежений в платформах: Vista SP1, Win7, Win8, Win10.

К перевагам VPN / SSH відносяться швидку і зручну передачу пакетів інформації, не треба окремо налаштовувати додатки. К недоліком VPN / SSH відносять потребу довіряти VPN / SSH-сервера провайдеру.

Tor –відкрите програмне забезпечення і система проксі-серверів, яка дає змогу встановити анонімне мережеве з'єднання, захищене від прослуховування.

В ній клієнт з'єднується з Інтернетом через ланцюжок вузлів. Як правило, ланцюжок складається з трьох вузлів, кожному з них невідомі адреси клієнта і ресурсу одночасно. Він має досить високий рівень анонімності клієнта при передачі тільки http-трафіку [2].

Перевагою Tor є висока ступінь анонімності клієнта при дотриманні всіх правил, просто завантажується і не викликає труднощів при використанні. Однак вихідний трафік Tor прослуховується та має низьку швидкість.

Анонімна мережа I2P, яка працює поверх Інтернету. В ній є свої сайти, форуми та інші сервіси. За своєю архітектурою вона повністю децентралізована, також в I2P ніде не використовуються IP-адреси.

Перевагою I2P є висока ступінь анонімності клієнта, повна децентралізація, що веде до стійкості мережі, конфіденційність даних (наскрізне шифрування між клієнтом і адресатом). Недоліком I2P є низька швидкість [3].

Були розглянуті поширені методи забезпечення анонімності в мережі, їх технічні особливості, а також їх переваги та недоліки. Найбільш надійне рішення для анонімного серфінгу в Інтернеті на сучасному етапі – це спільне використання VPN мереж і анонімного браузера, наприклад, Tor. Для забезпечення анонімності відправника електронних повідомлень, найбільш підходить використання засобу анонімізації I2P. При цьому, завжди необхідно враховувати можливі атаки через плагіни і XSS, помилки в програмному забезпеченні, запити до DNS серверів, хибно налаштовані вузли в мережах Tor і I2P, і т.д. Крім розглянутих методів існують окремі проекти, присвячені забезпеченню анонімності в мережі, в тому числі доповнення для браузерів і різні «анонімізатори».

Список використаних джерел

1. Козак Р. О. Аналіз засобів забезпечення анонімності *в* мережі Інтернет / Р. О. Козак // Вимірювальна та обчислювальна техніка в технологічних процесах. - 2014. - № 1. - С. 100-105.
2. Tor: Overview : URL: https://www.torproject.org /about/ overview.html.en.
3. Introducing I2P : [Електронний ресурс]. – Режим доступу: http://geti2p.net/en/docs/ how/ tech-intro

Хрипкова А.,
студентка ОС «Бакалавр» спеціальності «Кібербезпека»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ДВОФАКТОРНА АУТЕНТИФІКАЦІЯ

Майже вся важлива інформація абонентів зберігається в електронному вигляді. 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 автентифікація або 2FA.

Двофакторна автентифікація - це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи автентифікаційних даних. Введення додаткового рівня безпеки забезпечує більш ефективний захист аккаунта від стороннього доступу. Двофакторна автентифікація 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, який автоматично генерується та надсилається вам будь-яким способом, окрім трансляції в Інтернеті. Він може бути надісланий на ваш мобільний телефон як SMS-повідомлення, може бути навіть роздрукованим і відправленим вам на папері за добрим старомодним способом, або згенерований додатком, запущеним на вашому телефоні або токеном. 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.

Як правило, одноразовий пароль - це серія безглуздих чисел або символів, або це може бути півдюжини коротких випадкових слів, що генерується за допомогою певних алгоритмів. Давайте розглянемо це детальніше.

Отже, якщо одноразовий пароль дасть вам доступ до комп'ютерної системи, то цей одноразовий пароль, яким ви володієте, очевидно має відповідати паролю у пам'яті комп'ютера так само, як звичайний пароль. Єдина проблема полягає в тому, що пароль повинен мінятися кожного разу, коли ви використовуєте його. Це означає, що має бути певна форма синхронізації, яка дозволяє як вам, так і комп'ютерній системі використовувати той самий, постійно мінливий пароль, і комп'ютер не повинен кожного разу передавати його вам яким-небудь безпечним способом, наприклад, електронною поштою. Ви можете подивитись, як це буде працювати з системою на базі мобільного телефону: комп'ютерна система генерує одноразовий пароль, надсилає його вам в текстовому повідомленні SMS, а потім дозволяє певний період часу вводити його перш ніж період дії пароля закінчиться. Система поштової розсилки працює таким же чином, але паролю доведеться діяти довше, щоб забезпечити затримку транзиту (наприклад деякі банки почнуть надсилати вам весь роздрукований список одноразових паролів, які називаються номерами автентифікації транзакцій, що ви використовуєте, а потім викреслюєте послідовно, підбираючи список паролів, що зберігаються на комп'ютерній системі).

Але ж яким чином працює синхронізація, якщо у вас є щось подібне до токену безпеки, який створює для вас одноразові паролі? Один із способів, що називається TOTP (Time-based One-Time Password Algorithm) або синхронізацією часу, включає в себе токен і комп'ютерну систему, які генерують нові одноразові паролі на основі числової версії поточного часу. Вони можуть зайняти час, скажімо, 5:08 вечора, перетворити його на числовий код 1708, а потім запустити його за допомогою генератора коду та алгоритму, який називається хеш-функцією (або хеш-кодом) для створення унікального 10-цифрового коду, що стає вашим одноразовим паролем. Поки токен та комп'ютерна система синхронізують свої годинники, токен завжди буде генерувати одноразовий пароль, який відповідає тому, що шукає комп'ютер. Але якщо годинники вийдуть з ладу, токен більше не створюватиме правильні паролі, і їх потрібно буде перезапустити.

Інший алгоритм має назву HOTP та передбачає комп'ютерну систему та токен. Як параметр, що відповідає за динаміку генерації паролів, використовується подія, тобто сам факт створення: кожен раз при створенні нового пароля, лічильник подій збільшує своє значення на одиницю, і саме це монотонне зростаюче значення використовується як основний параметр алгоритму. Перший раз, коли потрібен пароль, комп'ютер та токен використовують номер лічильника 0001 з номером для генерації пароля; деякий час у майбутньому після того, як було створено багато паролів, лічильник може стояти на рівні 0299 усередині комп'ютера та токену, так що ця цифра буде використовуватися для створення пароля наступного разу. Ця техніка називається лічильною синхронізацією і не страждає від невигідності тримання годин на етапі. Другим параметром для розрахунку одноразових паролів є симетричний ключ, який повинен бути унікальним для кожного генератора (клієнта) і закритим від усіх, крім сервера і самого генератора (клієнта).

Роботу алгоритму HOTP можна описати наступною формулою:

HOTP(K, C) = Truncate(HMAC-SHA-1(K, C)), де:

- K - Секретний ключ, унікальний для кожного клієнта і відомий тільки йому та серверу.
- C - Поточний стан 8-байтового лічильника за подією.
- D - Кількість цифр у генерованому паролі.

Процес роботи алгоритму можна розбити на наступні етапи:

1) Створюється рядок HS розміром у 20 байт, застосовуючи хеш-функцію HMAC-SHA-1, ініціалізовану параметрам K і C: HS = HMAC-SHA-1 (K, C).
2) Вибираються певним чином 4 байти із HS: S{bits} = Truncate (HS).
   a) Чотири останніх біта останнього байту результату S{bits} перетворюються в число offset Є (0,15).
   b) Послідовність байтів HS [offset] .. HS [offset + 3] перетвориться на змінну P.

c) Truncate (HS) повертає останні 31 біта P. Причина, через яку ігнорується старший біт P, полягає в різних варіантах реалізації цілочисельних обчислень у різних процесорів.

3) Результат роботи Truncate() перетворюється до послідовності з D цифр: HTOP = toNumber (Truncate (HS)) mod10^D.

Основною відмінністю між двома алгоритмами є генерація пароля на основі мітки часу, яку використовує в якості параметра TOTP алгоритм. При цьому використовується не точне значення часу, а поточний інтервал, межі якого були встановлені заздалегідь (наприклад, 30 секунд). HOTP генерує ключ на основі секрету, що розділяється і не залежить від часу лічильника. Модель цього алгоритму заснована на подіях - наприклад, кожен раз, коли генерується черговий одноразовий пароль, лічильник буде збільшуватися. Отже, згенеровані згодом паролі повинні бути різними кожен раз.

Роблячи підсумки, можна сказати, що за умови використання тієї ж самої хеш-функції, як і в HOTP, дана відмінність в роботі алгоритму робить TOTP безпечнішим і кращим рішенням для одноразових паролів.

Список використаних джерел

1. Two-factor authentication. – URL : http://www.explainthatstuff.com/how-security-tokens-work.html

Хрипченко Ю.,
студентка ОС «Магістр» спеціальності «Журналістика (спеціалізація Зв'язки з громадськістю)»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ЗАХИСТ ІНФОРМАЦІЇ У ЗАСОБАХ МАСОВОЇ КОМУНІКАЦІЇ

Захист інформації є одним з важливих аспектів збереження інформаційних даних у комунікативному просторі. У сучасному інформаційному суспільстві технології відіграють роль активатора проблеми захисту інформації, адже комп'ютерні злочини стали характерною ознакою викрадення, пошкодження та зміни даних. Правова система не здатна забезпечити повноцінний захист інформації, тому її збереження залежить тільки від правильного зберігання та поширення даних. Знання того, які існують комп'ютерні загрози та, які способи і методи існують для їх уникнення є актуальними як для кожної людини, так і для засобів масової інформації, які здійснюють свою діяльність за допомогою інформації.

Мета дослідження – виявити особливості захисту інформації у засобах масової комунікації. Мета дослідження досягається за допомогою наступних завдань:

- визначити основні загрози для інформації у галузі соціальних комунікацій;

- проаналізувати способи і методи захисту інформації у ЗМК.

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» захист інформації – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1]. У науковій літературі також можна зустріти відповідні терміни «безпека інформації» та «безпека інформаційних технологій».

Основними принципами інформаційної безпеки у ЗМК є забезпечення цілісності, конфіденційності і доступності інформації для всіх авторизованих користувачів.

Основними випадками порушення інформації є: несанкціонований доступ, витік інформації, втрата інформації, підробка інформації, блокування інформації, порушення роботи інформаційних систем. Загалом найбільшу загрозу безпеці інформації становлять люди, які є нинішніми чи колишніми працівниками організації, просто ознайомленими з роботою організації чи «учнями» у несанкціонованому проникненні до будь-яких мереж.

До найбільш поширених видів комп'ютерних злочинів відносяться: несанкціонований доступ до інформації, що зберігається у комп'ютері, та її розкрадання; підробка комп'ютерної інформації; уведення у програмне забезпечення «логічних бомб»; комп'ютерні віруси; злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення – створення і залишення без контролю «люків» («чорних ходів»); комп'ютерні злочини в мережі Інтернет.

Комп'ютерний вірус – спеціально написана невелика за розмірами програма, яка може створювати свої копії, впроваджуючи їх у файли, оперативну пам'ять, завантажувальні області і т. ін. з метою зараження їх, та здатна виконувати різноманітні небажані дії [2]. Комп'ютерні віруси за середовищем існування бувають файловими, завантажувальними, комбінованими (файлово-завантажувальними), пакетними та мережними. За ступенем деструктивності віруси поділяються на нешкідливі, небезпечні і дуже небезпечні.

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні.

До програмних методів захисту інформації відносяться: стеганографічний метод захисту інформації, метод захисту від комп'ютерних вірусів, методи криптографічного захисту інформації, метод біометричного захисту інформації.

Розглядаючи програмні засоби захисту інформації у ЗМК, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі дізнатися про його існування. Найчастіше стеганографія використовується для створення цифрових водяних знаків, які записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки

можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений [2].

Захист від комп'ютерних вірусів теж є значимим засобом захисту інформації, особливо, якщо інформація створюється і зберігається в електронному вигляді. Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Але найбільш поширеним методом залишається використання антивірусних програм – спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів. Антивірусні програми, у свою чергу, поділяють на: програми-детектори, програми-доктори, програми-ревізори, програми-фільтри, програми-вакцини. Проте варто пам'ятати, що жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержувати загальних правил і користуватись останніми розробками антивірусних лабораторій [1].

Криптографічний захист (шифрування) інформації – це вид захисту, який здійснюється за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності тощо. На відміну від тайнопису, яке приховує сам факт передачі повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст [2].

Методи криптографії поділяють на дві групи – підставлення (заміни) і переставлення. Підстановчний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза – ключ. У разі використання перестановного алгоритму змінюються не символи, а порядок їх розміщення в повідомленні. Залежно від доступності ключів розрізняють: симетричне шифрування – для шифрування і розшифрування використовується один ключ, та асиметричне – для шифрування використовується один, відкритий (загальнодоступний) ключ, а для дешифрування – інший, закритий (секретний) [3; 226-228].

Системи біометричного захисту використовують унікальні для кожної людини фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною аутентифікацією. Його суть – визначити, чи справді індивід є тією особою, за яку себе видає. Біометричний метод захисту втілено в сучасних технологіях: розпізнавання відбитків пальців; розпізнавання голосу; аналіз геометрії руки, що передбачає вимірювання фізичних характеристик руки і пальців користувача; сканування сітківки ока; сканування райдужної оболонки; розпізнавання обличчя; розпізнавання динаміки підпису; розпізнавання стилю набирання символів на клавіатурі [2].

Отже, засоби масової комунікації, як суб'єкт створення, зберігання та

поширення інформації потребує надійного захисту від різнорідних загроз для забезпечення цілісності, конфіденційності і доступності інформації для всіх авторизованих користувачів. Основними випадками порушення інформації є: несанкціонований доступ, витік інформації, втрата інформації, підробка інформації, блокування інформації, порушення роботи інформаційних систем. Всього цього можна уникнути, якщо вміти застосовувати основні методи захисту інформації: стеганографічний метод, метод захисту від комп'ютерних вірусів, методи криптографічного та біометричного захисту інформації.

Список використаних джерел

1. Технології захисту інформації : [Електронний ресурс]. – Режим доступу : http://www.uzhnu.edu.ua/uk/infocentre/get/4186
2. Дурняк Б. В. Способи захисту інформації у засобах масової інформації / Б.В. Дурняк, І.М. Лях // Поліграфія і видавнича справа. – 2012. – № 2. – С. 60-63. – Режим доступу : http://nbuv.gov.ua/UJRN/Pivs_2012_2_10
3. Остапов С.Е. Технології захисту інформації : навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

Шульга Л.,
студентка ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Шпигунське програмне забезпечення (програма шпигун, Spyware) - програма, яка таємним чином встановлюється на комп'ютер з метою збору інформації про конфігурацію комп'ютера, користувача, призначеної для користувача активності без згоди останнього. Також можуть виконувати інші дії: зміна налаштувань, установка програм без відома користувача, перенаправлення дій користувача.

Шпигунські програми не відносяться до звичайних вірусів, це окремий тип протиправного втручання в комп'ютерну систему користувача. На відміну від вірусів, шпигунських програм для комп'ютера не завдають шкоди - ні системі, ні програмами, ні призначеним для користувача файлів. Однак користувач, якщо на його комп'ютер впроваджена шпигунська програма, навряд чи зможе розраховувати на всю продуктивність своєї машини - Spyware задіє якусь кількість оперативної пам'яті, і від цього комп'ютер може працювати повільно.

Шпигунські програми можуть здійснювати широке коло завдань, наприклад:

- збирати інформацію про звички користування Інтернетом і найбільш часто відвідувані сайти (програма відстеження);
- запам'ятовувати натискання клавіш на клавіатурі (кейлоггери) і записувати скріншоти екрану (screen scraper) і в подальшому відправляти інформацію творцеві spyware;

- несанкціоновано і дистанційно керувати комп'ютером (remote control software) - бекдори, ботнети, droneware;
- інсталювати на комп'ютер користувача додаткові програми;
- використовуватися для несанкціонованого аналізу стану систем безпеки (security analysis software) - сканери портів і вразливостей і зломщики паролів;
- змінювати параметри операційної системи (system modifying software) - руткіти, перехоплювачі управління (hijackers) та ін. - результатом чого є зниження швидкості з'єднання з Інтернетом або втрата з'єднання як такого, відкривання інших домашніх сторінок або видалення тих чи інших програм;
- перенаправляти активність браузерів, що тягне за собою відвідування веб-сайтів наосліп з ризиком зараження вірусами.

Програми віддаленого контролю і управління можуть застосовуватися для віддаленої технічної підтримки або доступу до власних ресурсів, які розташовані на віддаленому комп'ютері.

Технології пасивного відстеження можуть бути корисні для персоналізації веб-сторінок, котриепосещает користувач.

Уся зібрана шпигунськими програмами інформація відправляється тим, хто їх створює розробникам Spyware. Це може бути їх електронну адресу, інтернет-сервер або будь-яке інше простір в інтернеті. більшості випадків користувачі не підозрюють, що вони знаходяться під наглядом - шпигунські програми, як правило, працюють непомітно, оскільки їх розробники зацікавлені в тривалому отриманні потрібної їм інформації.

Історія і розвиток:

Згідно з даними AOL і NationalCyber-Security Alliance від 2005 року 61% Респондентное комп'ютерів містили Туїлі іншу форму шпигунських програм, з них 92% користувачів не знали про присутність "шпигунів" на їх машинах і 91% повідомили, що вони не давали дозволу на інсталяцію.

До 2006 року spyware стали одніміз превалюють загроз безпеки комп'ютерних систем, що використовують Windows. Комп'ютери, в яких Internet Explorer служить основним браузером, є частічноуязвімимі не тому, що Internet Explorer найбільш широко використовується, ноіз-за того, що його тісна інтеграція з Windows дозволяє spyware получатьдоступ до ключових вузлів ОС.

Методи, які використовують шпигунські програми для зараження комп'ютерів:

1. Помилковий маркетинг. Є багато розробників шпигунського софта, які прагнуть обдурити користувачів, надаючи їх шпигунські програми, як корисні інструменти, наприклад, потужний пошуковий сервіс, швидкий менеджер завантажень або надійний прискорювач інтернету. Користувачі завантажують і встановлюють такі програми, але, тим не менше, практично всі вони є марними або неефективними. Хоча більшість таких програм можна видалити вручну, їх

шкідливі компоненти залишаються в системі і функціонують в колишньому режимі.

2. Зв'язка програмного забезпечення. Є багато безкоштовних програм, які складаються в зв'язці з небезпечними доповненнями, розширеннями і плагінами. Вони представлені як компоненти, які необхідні для чіткої роботи програми. На жаль, але більшість таких доповнень є шпигунськими паразитами. Видаливши хост додатки, ви не видалите шпигунське програмне забезпечення.

3. Уразливості безпеки. Це і вразливість веб-браузерів використовуються для поширення різних загроз, включаючи шпигунських. Їх виробники запускають небезпечні веб-сайти наповнені шкідливим кодом і небезпечними спливаючими банерами з рекламою. Коли користувач відвідує такий сайт або натискає на банер або оголошення, в їх систему проникає небезпечний, шкідливий скрипт. Користувач не може знайти нічого підозрілого, так як вірус не відображає ніякого майстра установки, діалогу або попередження.

4. Інші загрози. Також відомо, що деякі типи шпигунів активно поширюються іншими вірусами. Трояни, черв'яки і бекдоров найнебезпечніші віруси, які можуть поширювати шпигунське програмне забезпечення.

Як захистити себе від програм-шпигунів:

- Встановити сучасну антивірусну програму і активувати в ній функції пошуку небажаних програм (шпигунські програми, кейлогерів, трекерів, адваре і тп).
- Встановити фаєрвол і контролювати мережеву активність встановлених програм.
- Уважно перевіряти налаштування приватності операційних систем і браузерів, відключати зайві функції і відправку особистих даних будь-кому.
- Уважно ставитися до установки програм і вибору компонентів при інсталяції. Разом з корисною програмою вам може бути встановлений цілий набір небажаного ПЗ "в навантаження".
- Періодично проводити аудит встановлених програм і видаляти непізнані або рідко використовувані, так ви звузите потенційну зону ризику.

Список використаних джерел

1. Безопасность персональних данных в социальных сетях [Електронний ресурс]. – Режим доступу: http://human.snauka.ru/2015/11/13018
2. Кримінальний кодекс України [Електронний ресурс] : Закон України від 05.04.2001 р. № 2341-III. – Режим доступу: www.rada.gov.ua

Янчинська В.,
ОС «Бакалавр» спеціальності «Системний аналіз»
Науковий керівник: доцент, кандидат технічних наук Меркулова К.В.
Маріупольський державний університет

КРІПТОВАЛЮТА В УКРАЇНІ

Кріптовалюта – це різновид цифрових грошей, в основі якої лежить технологія криптографії, тобто, шифрування даних. Вона не має фізичного вигляду, а існує тільки в електронному вигляді. Її основні особливості - це анонімність, децентралізація і захищеність. Циркуляція криптовалюта всередині системи відбувається безпосередньо - без участі третьої сторони. Кожен з учасників - абсолютно дорівнює. Ні у кого немає привілеїв, незалежно від його соціального і фінансового статусу. В основі цих віртуальних грошей лежить децентралізована відкрита база даних - блокчейн.

Кріпта VS Фіат.

При згадці слова «валюта», в розумі спливають образи банкнот, банків. Ми звикли до фіатному влаштую в фінансових системах. Фіат - це стандартна, регульована валюта. Начебто долара або євро. Основні відмінності криптовалюта від фіатних валют полягають в наступному:

• криптовалюта не має фізичного вигляду. Так, фіат також існує в електронному вигляді, проте банкнот або кріптовалютних монет не буває. Не плутайте фізичні монети, гаманці-накопичувачі, які використовують для роботи з крипт.

• криптовалюта не випускається центральним банком і не прив’язана до економіки будь-якої країни. Випуск і емісія криптовалюта не контролюється кимось одним. Обмежити ці процеси не може ніхто. Тільки особливості самої системи. Курс сформований ринковим шляхом і безпосередньо ніяк не пов’язаний з економікою будь-якої країни.

• Вона анонімна. Для роботи з банком, платіжними системами, Вебмані необхідно вказувати хоча б частину особистих даних. У криптовалюта в цьому немає необхідності. Кожен учасник анонімний. Вся інформація про нього - це набір знаків в адресі гаманця.

• Прямі транзакції. Ніяких процесингових центрів, посередників, емітентів і третіх сторін в цій віртуальній валютній системі немає. Є проста передача коштів між учасниками мережі безпосередньо.

Як працює криптовалюта

Більшість криптовалюта функціонують і циркулюють в блокчейн. Це децентралізована база даних, куди записується і зберігається інформація про всі транзакції. Вона не розміщується на якомусь окремому сервері або жорсткому диску, а розбита по вузлах. Підтримують її активні учасники мережі - звичайні користувачі повновагих гаманців.Окремі осередки з записаними даними - це блоки. При цьому всі блоки між собою пов’язані. Виходить ланцюжок (chain) - від цього і походить назва Блокчейн (Blockchain). Зв'язок встановлюється через запис хеш-суми попереднього блоку в нові блоки. Через це окремий блок

змінити практично неможливо - для цього доведеться «ламати» все блоки в ланцюжку.

Приставка «крипто» обумовлена тим, що Bitcoin і інші валюти використовують шифрування і криптографічні хеш-функції. Так у кожного учасника мережі є приватний або закритий ключ і відкритий ключ. Приватний використовується для підпису «листи передачі прав власності». Це лежить в основі всіх транзакцій і забезпечує передачу криптовалюта від одного учасника до іншого. А публічний відкритий ключ вже використовується для верифікації чужих транзакцій в блокчейн.

Як користуватися криптовалютою.

Щоб користуватися криптовалюта, наприклад, Bitcoin, необхідно відкрити гаманець. Робиться це шляхом скачування клієнта на жорсткий диск, або в мережі. Популярний варіант онлайн-гаманця для біткоіни доступний на сайті blockchain.info.

Навіщо потрібна криптовалюта?

Криптовалюта може бути корисна для різних цілей, починаючи від покупок і закінчуючи заощадженням грошей. Перелічимо основні варіанти використання криптовалюта:

Платежі. Причому не просто транзакції, а анонімні, швидкі і прямі транзакції. Здійснюються як між приватними особами, так і для покупки товарів або послуг в інтернеті.

Зберігання грошей. «Викрасти» криптовалюта з гаманця практично неможливо. Так як всі операції незворотні і використовують приватні ключі, перехопити їх або зламати неможливо. За умови, що ви нікому не дали свій приватний ключ, ваша криптовалюта буде завжди в цілості.

Інвестиції. Bitcoin і іншу крипту розглядають в якості інвестиційного активу за рахунок коливань курсу і загального зростання популярності. Причому криптовалюта підходить як для короткострокового заробітку шляхом торгівлі на біржі, так і для довгострокового, так як курс демонструє тенденцію до зростання.

Бізнес. Все більше компаній і сервісів підключають платежі в криптовалюта. Буденністю стали суто криптовалютние стартапи, що збирають кошти через ICO (краундфандінг). Якщо у вас особисто є бізнес-ідея, пов'язана з блокчейн або віртуальною валютою, то ви можете ініціювати збір коштів через ICO.

Звідки береться криптовалюта?

Найпоширенішим способом видобутку криптовалюта вважається Майнінг (від mining - добувати). Майнінг - це рішення криптографічних завдань різної складності з використанням потужностей обладнання.

Навіщо це взагалі потрібно і чому Майнер отримують винагороду? Цей процес чимось нагадує роботу торрент-трекера. Учасники трекера займаються роздачею файлів і за це отримують рейтинг, який в подальшому

використовується для скачування нових даних. Майнер ж, використовуючи обчислювальні потужності, підтримують працездатність мережі.

Кінцева мета Майнінг - підбір цифрового підпису, що закриває блок. Як тільки це відбувається, блок закривається, майнер отримує винагороду і починає формуватися новий блок. Для видобутку різних криптовалюта задіюється потужності процесора (CPU), відеокарт (GPU) або спеціалізоване обладнання (ASIC, FPGA). Майнінг - це один із способів заробітку криптовалюта.

Чим забезпечена криптовалюта

Наскільки курс криптовалюта обгрунтований і чим він підкріплений? Є різні думки з цього приводу. Американський IT-магнат і мільярдер Марк Кьюбан влітку 2017 року обрушився з критикою на Bitcoin і крипту в цілому в своєму Twitter: «Це більше схоже на культ і релігію, ніж на справжній актив. Тільки при цьому з золота можна зробити непогані прикраси, а з віртуальних монет нічого. Це бульбашка».

Після цього курс знизився, і Марк додав: «Ти розумієш, що це міхур, коли випадковий пост в Твіттері може змусити валюту знизити ціну».

Однак потім сам Кьюбана почав інвестувати в ICO і навіть радить людям тримати 1/10 власних коштів в криптовалюта.

Так а чим же підкріплений курс?

По-перше, для видобутку криптовалюта потрібно потужне обладнання, яке споживає чимало електрики і поступово втрачає свою продуктивність. Виходить, що частково і амортизація переноситься на вартість монет.

По-друге, блокчейн. Це те, чого немає ні в однієї іншої платіжної системи. Блокчейн універсальний, надійний, децентралізований. При цьому гарантує анонімність і високу швидкість транзакцій. І застосовується він в різних сферах. Починаючи від фінансового сектора, завершуючи альтернативною енергетикою. Це очевидні переваги, які визначають цінність криптовалюта.

Вартість цих віртуальних монет встановлюється ринковим шляхом. Чим більше попит на певну криптовалюта, тим вище її курс. Попит же в свою чергу залежить від тих переваг, які пропонує монета. Якщо завтра біткойн зроблять офіційною валютою в Китаї, то її вартість «злетить до небес». Попит формується на тлі новин, нових розробок, анонсів компаній.

Статус криптовалюти в Україні.

Національний банк України (НБУ) до сих пір чітко не визначився, що ж робити з криптовалюта. Таку позицію фінансовий регулятор висловив недавно.

Однак днями з’ясувалося, що в Україні криптовалюта не отримали визнання. Про це заявив заступник голови НБУ. За його словами, оскільки немає центрального емітента, то "це точно не валюта". Тобто, Нацбанк не може визнати це платіжним засобом. Головна причина, це те, що "люди можуть втратити гроші", зокрема, в результаті шахрайства з криптовалюта.

Прямої законодавчої заборони на операції з використання криптовалюта в Україні не існує. Саме тому ні роз’яснення НБУ, ні інші підзаконні

нормативно-правові акти не можуть замінити закон, який би прямо врегулював або заборонив оборот кріптовалюта.

Очевидно, що законодавство України та влади відстають від викликів часу. Хоча НБУ і Державна фіскальна служба заявляли про незаконність кріптовалюта, це не відлякує наших співвітчизників від їх використання.

Висновок. Чи є майбутнє у кріптовалюти? Однозначно відповісти питання на цей складно. Хоча б тому, що кожен закладає свої терміни в слово "майбутнє".

Однак, даний точно тісно пов’язане з цифровими валютами. З моменту своєї появи в 2009-му році, можливості і популярність кріптовалюта тільки ростуть. Тому в першу чверть 21-го століття варто очікувати періоду інтенсивної кріпторевolюції. Чим швидше ви до неї приєднаєтеся - тим краще.

Список використанних джерел

1. Криптовалюты : [Електронний ресурс] . – Режим доступу: http://www.inliberty.ru/library/571-kriptovalyuty // Mercatus Center, George Mason University.

2. Криптовалюта в Украине. Все, что нужно знать : [Електронний ресурс] . – Режим доступу: https://nv.ua/techno/it-industry/kriptovaljuta-bitcoin-v-ukraine-vse-chto-nuzhno-znat-1918518.html.

ЗМІСТ