Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Факультет соціології і права
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет права і адміністрації Варшавського університету

КІБЕРБЕЗПЕКА ТА ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ: ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
21 квітня 2017 року

Частина ІІ

Студентський погляд

Київ-2017

УДК 340.132:[342/951+004]+347.77/78
ISBN 978-966-622-834-8
К-38

Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: Матеріали міжнародної науково-практичної конференції. 21 квітня 2017 р., м. Київ, в 2-х частинах. Частина друга. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. – 124 с.

Матеріали конференції присвячені проблемним питанням правового забезпечення кібербезпеки та права інтелектуальної власності у сучасних умовах розвитку інформаційного простору. У даної частині матеріалів конференції подано студентській погляд на оцінку та шляхи вирішення означеної проблематики. Надані матеріали починаючих дослідників можуть бути корисними для науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться сучасними суспільно-правовими проблемами інформаційної безпеки людини забезпечення прав і свобод людини.

Участь у конференції взяли провідні експерти і вчені наукових установ і навчальних закладів України, Республіки Польща, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право», «Правова інформатика» та Вісник НТУУ «КПІ» «Політологія. Соціологія. Право»

Матеріали подано у авторській редакції.

Упорядники: Фурашев В. М., Петряєв С. Ю.

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП КПІ ім. Ігоря Сікорського
designlab.kpi.ua@gmail.com \
Балашов Д. В. (balashov.dim@gmail.com)

Рекомендовано до друку:
Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України. Протокол № 3 від 16.05.2017 р.
Вченою радою факультету соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Протокол № 9 від 29.05.2017 р.

ISBN 978-966-622-834-8
К-38

ЗМІСТ

Самчинська О. А., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М.*, к.т.н., доцет.*

ПРОБЛЕМАТИКА ЗАСТОСУВАННЯ ТЕРМІНІВ «ІНФОРМАЦІЙНА БЕЗПЕКА» ТА «КІБЕРБЕЗПЕКА»

Науково-технічна революція на початку XXI століття спричинила неабиякі системні перетворення у світі. Світова спільнота зрозуміла, що інформація та інформаційно-телекомунікаційні технології відіграють провідну роль в житті людства. Людство перейшло на новий щабель свого розвитку і інформаційне суспільство з'явилось не лише в концепції, а й наяву.

Стало зрозуміло, що в новому інформаційному суспільстві основну роль відіграє інформація. Саме за допомогою інформації та інформаційно-телекомунікаційним системам стало можливим розв'язати найважливіші глобальні проблеми, які постали перед людством у XXI столітті.

Але незважаючи на всі блага, які принесла нам науково-технічна революція, вона, як і будь-яке явище має дві сторони медалі. Тому з розвитком інформаційно-телекомунікаційних систем та зростанням ролі інформації в нашому житті гостро постала проблема безпеки інформації. Адже незважаючи на всю її користь, виявилось, що інформація може не лише допомогти, а й зашкодити значною мірою.

Сьогодні інформаційна сфера надзвичайно вразлива і піддається різноманітному впливу. Цей вплив може бути різним, особливо популярним та доступним на сьогодні, завдяки розвитку інформаційно-комунікаційних технологій став кібернетичний засіб впливу на інфосферу. Тому, перед кожною державою постало питання врегулювання цих відносин та створення відповідних систем, що забезпечують безпеку інформації.

Стан захищеності, який намагається досягти кожна держава, реалізуючи політику забезпечення інформації від шкідливого впливу, називають

«інформаційна безпека» та «кібербезпека». Так в країнах США та Європи вживають лише термін «кібербезпека», поняття «інформаційна безпека» там не існує. Якщо ж розглянути Україну та інші пострадянські країни, то там поширенішим поняттям є «інформаційна безпека». Для того, щоб визначити чи є ці поняття справді тотожними та чому в різних країнах їх застосовують по-різному, та чим керуються, застосовуючи один чи інший термін, потрібно розглянути питання «інформаційний простір», «кіберпростір», їх основні ознаки, і спираючись на ці поняття, визначити «інформаційну безпеку» та «кібербезпеку».

Сьогодні уся діяльність пов'язана з інформацією відіграє провідну роль у розвитку держави. Адже, від швидкості створення, обробки та поширення інформації, залежить ефективність управлінських рішень та інших значно зростає значення регулювання найбільш важливих сфер життєдіяльності людини, саме за допомогою інформаційно-телекомунікаційних заходів. Саме тому, інформаційна безпека є просто складовою національної безпеки. Вона є самостійною сферою забезпечення національної безпеки.

Що ж являє собою інформаційна безпека? Потрібно чітко розуміти, що означає поняття «безпека», адже безпека-це не відсутність загроз тому, що загрози існують завжди, безпека - це певний стан захищеності від цих загроз.

Що ж до інформаційної безпеки - це стан захищеності людини, суспільства та держави, їх життєво важливих інтересів від негативного впливу інформаційної діяльності та інформаційних технологій.

Об'єктом інформаційної безпеки, тобто те, на що спрямовано захист є насамперед: інформація, джерела інформації, методи та засоби її створення, збереження, розповсюдження, використання, а також нормативно-правові акти, які регулюють цю діяльність.

Суб'єктами інформаційної безпеки є людина, держава та суспільство, а конкретніше їх діяльність, пов'язана з інформацією.

Для того, щоб краще розуміти поняття інформаційної безпеки, проаналізуємо поняття «інформаційний простір».

Інформаційний простір – це певна форма співіснування матеріальних та нематеріальних об’єктів, а також процесів, спрямованих на задоволення інформаційних потреб всіх живих істот.

З даного визначення можна визначити об’єктів та суб’єктів інформаційного простору.

Об’єктами інформаційного простору є суб’єкти природного середовища, природні та штучні інформаційні відносини між ними, матеріальні та нематеріальні об’єкти на процеси, спрямовані на задоволення інформаційних потреб для забезпечення збереження життя живої істоти.

Суб’єктами інформаційного простору є живі істоти та їх угрупування, які здатні сприймати, запам’ятовувати, переробляти та передавати інформацію.

Тобто, можна зробити висновок, що інформаційний простір – це все з чого ми можемо сприйняти інформацію, тобто це фактично все, що нас оточує, включаючи живу та неживу природу.

Кіберпростір – це форма співіснування матеріальних та нематеріальних об’єктів та процесів, які спрямовані на створення, сприйняття, запам’ятовування, переробку та обмін інформацією.

Об’єктами кіберпростору є живі істоти та їх об’єднання, які здатні сприймати, запам’ятовувати переробляти та передавати інформацію. До них можна віднести: людину, суспільство, державу, природні та штучні інформаційні відносини між ними. Також, як об’єкти кіберпростору, можна визначити матеріальні та нематеріальні об’єкти, та процеси, які здатні створювати, сприймати, зберігати, перероблювати та передавати інформацію. Такими об’єктами є комп’ютери та інші розумні машини, та технології.

Що ж до суб'єктів кіберпростору, то ними є держава, суспільство, людина та інші істоти, які здатні сприймати, запам'ятовувати та передавати інформацію.

Проаналізувавши все вище сказане, можна зробити висновок, що кібербезпека – це стан захищеності, а точніше стан спроможності людини, суспільства та держави запобігати та уникати несвідомого негативного впливу інформації.

Дуже влучним є визначення Баранова О.А., за яким кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства та держави в умовах використання комп'ютерних та/або телекомунікаційних мереж, за якого мінімізується завдання ним шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

Проаналізувавши поняття «інформаційний простір», «інформаційна безпека та «кіберпростір», «кібербезпека» [1-4], можна зробити висновки, що хоча ці категорії, на перший погляд, дуже схожі, та деколи вживаються як синоніми, вони, все ж таки, мають певні відмінності та свої особливості.

По-перше, інформаційний простір – це природний простір, який виник без втручання людини та охоплює усе, що нас оточує, включаючи об'єкти неживої природи. Що ж до кіберпростору –це штучно створений простір, який людина створила в процесі інформаційної діяльності для задоволення своїх потреб.

По-друге, інформаційний простір, як зазначалося, включає в себе всі матеріальні та нематеріальні об'єкти, з яких можна отримувати чи сприймати інформацію. До кіберпростору входять лише живі істоти і матеріальні об'єкти, і процеси, які здатні сприймати, запам'ятовувати, обробляти та передавати інформацію.

Можна зробити висновок, що інформаційний простір є ширшим поняттям, а кіберпростір є невід'ємною складовою інформаційного простору.

Таким чином, можна зробити висновок, що нині, коли інформаційно-комунікаційні технології відіграють дуже важливу роль в житті людини, та є невід'ємною її складовою, поняття «інформаційна безпека» та «кібербезпека» є практично тотожними за своєю практичною сутністю. Тому, використання того чи іншого терміну не змінює сутності цього явища.

Список використаних джерел:

1. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 18. – Ст. 677.
2. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27 – 28. – Ст.181. \
3. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / Фурашев В.М. // Інформація і право – 2012.- №2(5)
4. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». / Фурашев В.М. // Правова інформатика. – 2012. - № 2 (34). – С. 51-59.

----------***----------

Паламарчук М. А., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М.*, к.т.н., доцент.*

ВЗАЄМОЗВ'ЯЗОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ІНОФРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Стрімкий перехід до інформаційного суспільства та його розвиток створили низку серйозних проблем та питань. Одним з таких питань є *інформаційна безпека.* Поняття національної безпеки не можна розглядати без урахування інформаційної безпеки. Питання інформаційної безпеки в Україні на даному етапі є особливо важливим.

Законодавство України розкриває значення поняття «інформаційна безпека». Під інформаційною безпекою розуміють - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому здійснюється запобігання нанесенню шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [2].

Отже, інформаційна безпека, як суспільства, так і держави визначається ступенем їх захисту, і як результат, захищеністю найважливіших сфер від небезпечних інформаційних впливів. Однією з ознак інформаційного суспільства є здатність до нейтралізації таких впливів.

Під «інформаційною діяльністю» варто розуміти дії громадян, юридичних осіб та держави, які спрямовані на задоволення їх інформаційних потреб. Така діяльність суб'єктів здійснюється в рамках існуючого законодавства. Стаття 9 Закону України « Про інформацію» містить перелік основних видів інформаційної діяльності. Основними видами інформаційної діяльності є: створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації [1].

Неможливо розглядати інформаційну діяльність окремо від інформаційної безпеки, і навпаки. Оскільки, держава здійснює політику щодо забезпечення інформаційної безпеки України та визначає основні напрями діяльності органів державної влади, закріплюючи основні права та обов'язки щодо захисту інтересів України, при цьому дотримуючись балансу інтересів суспільства і держави в сфері інформації.

Отже, інформаційна діяльність не може виходити за межі створених державою у цій сфері норм, тому вона безпосередньо підпорядковується інформаційній безпеці.

Зауважимо, що захист інформації (конфіденційної, таємної) є одним з ключових моментів інформаційної безпеки. Повертаючись до видів інформаційної діяльності, проведемо паралель між захистом інформації та, безпосередньо, інформацією, яка відноситься до таємної та конфіденційної. Отже, захист такого особливого виду інформації неможливе без інформаційної діяльності.

Окрім того, створення законодавства, яке б регулювала основи інформаційної безпеки, визначало основні принципи такої діяльності, стратегії розвитку, плани дій зовсім неможливе без здійснення інформаційної діяльності, як такої. Проте варто враховувати і негативну сторону інформаційної діяльності, коли суб'єкти виходять за межі законодавства, або своїми діями скоюють порушення чинного законодавства, то вони автоматично можуть створювати загрозу інформаційній безпеці. Тобто, дані два поняття не можна розглядати один без одного. Помилка у одній з складових інформаційної діяльності, може спричинити серйозні наслідки для інформаційної безпеки, а отже, і для національної безпеки в цілому.

Підсумовуючи, можна сказати про те, що стан інформаційної безпеки надає суб'єктам можливість безперешкодно здійснювати свої права та реалізовувати свої можливості, що пов'язані з інформаційною діяльністю: одержання, використання, зберігання, захист. Окрім того, стан інформаційної безпеки створює належні умови для існування і розвитку інформаційних процесів.

Список використаних джерел:

1. Закон України « Про інформацію» від 02.10.1992 № 2657-XII
2. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V
3. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005. -432 с

----------***----------

Лозіцька М. В., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

ПОХОДЖЕННЯ ЗАГРОЗ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Виникає важливе питання: що ж розуміти під «загрозою», як і звідки вона породжується і найголовніше, хто вирішує, що якісь певні факти чи наміри можуть мати підривний характер для безпеки країни.

Відповідь знаходиться в межах осягання природи загроз, тобто їх етимології, створення та розвитку. Річ в тому, що розмірковувати про загрози можливо тільки в тому випадку, коли чітко окреслені національні інтереси. Так як загроза не може існувати сама по собі, вона не перебуває об`єктивно.

Загрози представляють собою деякі чинники, що виникають в середовищі, в якому діє об'єкт, до того ж, їх створення на пряму відноситься до виконання національних інтересів. Тому, загрози заважають як виникненню умов для виконання інтересів, так і самим національним інтересам. Отже, можемо зазначити, що загроза виникає тільки тоді, коли є чітко визначені національні інтереси та виконується реальна діяльність по їх реалізації [1, 4].

Сьогодні в умовах глобалізації, коли існування кордонів є майже не кричущим фактом, який може порушити право людини на вільне пересування, то присутність державного кордону для України є необхідністю для подальшого виживання. Ступеневе винищення української культури, мови, забуття звичаїв та традицій нашого народу, направлене на те, щоб поступово ми не мали змоги дати відповідь на єдине запитання: хто ти - громадянин України або українець, громадянин Європи чи громадянин відкритого суспільства?

Відбувається процес знищення етнічних ознак, ліквідації титульного етносу, його стилю життя, культури, традицій, який є таким, що створює

систему в державі, на основних засадах, котрого виникає і розбудовується держава. Проте, це можна буде реалізувати тільки за відсутності чітко окреслених національних інтересів [5].

Варто зазначити, що аналіз майбутнього країни, тільки через призму концепції безпеки є мізерним. Для здійснення національних інтересів у країні потрібно розробити документ концептуального характеру, в якому були б відображені національні інтереси та можливі шляхи їх виконання.

Нестача науково вмотивованих критеріїв виокремлення функціональних сфер - дає не в повній мірі можливість силам безпеки виконувати свої прямі повноваження в сфері безпеки, робить тяжчим процес прийняття і практичного виконання рішень.

Хочеться звернути увагу на ще один момент, такий як, характер загроз. XXI століття таке, в якому визначається контроль над джерелами планети, особливо природніми ресурсами.

В кого буде контроль над ресурсами (природніми, інформаційними і т. д.), в того буде контроль над всім світом.

Через це, енергетичну безпеку країни потрібно виділяти, як окрему сферу безпеки, через те, що втрачається контроль над природніми ресурсами, збільшується необхідність в ресурсах Росії. І це сьогодні істотно погіршує приховані можливості нашої держави, щодо стійкого та незалежного розвитку.

Нині характер загроз прямо передбачений інтересами, так як переважна більшість загроз в соціумі мають системний характер. Головним ланцюжком до успіху, є усунення вузькоутилітарного розуміння безпеки, як процесу утримання керування правлячою верхівкою. Безпека зароджується разом з інтересами, вона направлена, перш за все, на налагодження слушних умов для виконання інтересів.

Діяльність же, щодо розвіюванням причин, умов створення загроз є одним з напрямків безпеки. Безпека не локалізується заходами щодо

демонстрування загрози, вона не завершується очікуванням створення загроз, а виходить далеко за її межі, аж до запровадження нових алгоритмів створення факторів і тенденцій, які можуть за певних обставин перерости в загрозу. Через це безпека має значні відмінності від захисту.

Перелік загроз, є доволі масивним, тому потрібно виділяти не самі загрози, а параметри національних інтересів, пересилювання яких може вказувати на наявність загрози, а отже, може бути відправною точкою створення політики безпеки.

Характер загроз держави свідчить про його роль і місце в геополітичній конфігурації. Тому можна зробити висновок, що наявність загроз - свідчення того, де країна здійснює прориви або робить деякі помилки. Для політиків загрози є свідченням прояву помилок в послідовності управління.

Виходячи з цього, безумовно, можна сказати про позитивну роль, яку зіграла Концепція (основи державної політики) національної безпеки України (1997 - 2003 роки). Закон від 19 червня 2003 року "Про основи національної безпеки України", який скасував її дію, в методологічному плані практично нічим не різнився, за виключенням більш логічно побудованої і детермінованою системи загроз, і напрямів державної політики в сфері національної безпеки, а також виділенням декількох нових сфер життєдіяльності [2].

В даному розумінні хотілося б, щоб Концепція (стратегія) безпеки була б як своєрідна Конституція безпеки, без неї, держава подібно бедуїнам на верблюдах в пустелі, виючому проти безпілотної авіації, знаючи про загрозу, він не може побачити і ідентифікувати її, а загибель є неминучою, невідворотною і безальтернативною [3].

Список використаних джерел:

1. Конституція України
2. Закон України “Про основи національної безпеки України”

3. Постанова ВРУ «Про Концепцію (основи державної політики) національної безпеки України»
4. Ліпкан В. А. - Поняття та зміст націобезпекознавства\\Право України №9, 2003
5. Пилипчук В. Г. Еволюція наукових поглядів стосовно поняття «державна безпека» // Стратегічні пріоритети. - 2006. - № 2. - С. 48.

----------***----------

Аненков А. І., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковій керівник:
Фурашев В.М., *к.т.н., доцент.*

РОЛЬ ТА ЗНАЧЕННЯ КОРУПЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ БЕЗПЕКИ

Корупція – комплексне й багатогранне явище, більш складне, ніж ті спрощені шаблонні уявлення про корупцію, які циркулюють в пресі і які знайшли віддзеркалення в більшості існуючих визначень корупції. Наприклад, у тлумачному словнику дається таке визначення: «Корупція - моральне розкладання посадових осіб і політиків, що виражається у незаконному збагаченні, хабарництві, розкраданні і зрощування з мафіозними структурами» [1].

Таке визначення застосовується поряд із державами, з добре розвиненою правовою системою, де всім зрозуміло, що є законне збагачення, і що – незаконне. Але для держав з незадовільною правовою системою, яких сьогодні в світі більшість, це визначення не годиться, оскільки чиновники там крадуть цілком законно, ніякий закон їм цього не забороняє. Разом з тим, саме в таких державах ми бачимо найбільш кричущі приклади корупції.

Найчастіше, під корупцією (у вузькому сенсі слова) розуміють подію, коли посадова особа приймає протиправне рішення (іноді рішення морально не правомірне для громадської думки), з якого отримує певну вигоду інша сторона, а саме посадова особа, буде мати незаконну винагороду від цієї

сторони. Характерні ознаки даної ситуації приймається рішення, яке порушує закон або неписані суспільні норми, обидві сторони діють за згодою; обидві сторони отримують незаконні переваги; обидві намагаються приховати свої дії [3].

Зазвичай, бувають ситуації, коли чиновника змушують під тиском, або за допомогою шантажу прийняти незаконне рішення. Часто, це трапляється вже з затягнутими в злочинну діяльність чиновниками, які, піддаючись тиску, фактично отримують одну просту вигоду — їх не викривають.

Корисно розрізняти верхівкову і низову корупцію. Перша охоплює політиків, вище та середнє чиновництво і пов'язана з прийняттям рішень, що мають високу ціну (формули законів, держзамовлення, зміна форм власності тощо). Друга - поширена на середньому і нижчому рівнях, і пов'язана з постійним, рутинною взаємодією чиновників і громадян (штрафи, реєстрації тощо) [4].

Однією з основних проблем, з якими стикається міжнародне співтовариство, є корупція. Це питання, поряд з організованою злочинністю і торгівлею людьми, знаходиться у центрі уваги конвенцій, прийнятих у галузі попередження злочинності та кримінального правосуддя.

Загальновизнано, що корупція, є однією з найбільш серйозних проблем, яка загрожує соціально-економічному, політичному розвитку і підриває демократію, і моральні підвалини суспільства.

На Восьмому Конгресі по попередженню злочинності і поводженню з правопорушниками (Гавана, що проходила з 27 серпня по 7 вересня 1990 року) ООН була прийнята спеціальна резолюція «Корупція у сфері державного управління». У ній зазначалося, що проблеми корупції в державній адміністрації мають загальний характер і що, хоча вони надають особливо згубний вплив на країни з вразливою економікою, де спостерігається зв'язок корупції з іншими видами організованої злочинності, цей вплив відчувається в усьому світі. Вона рекомендує державам-членам

розробити стратегію боротьби з корупцією, а також розглянути питання про адекватність кримінально-правового реагування на всі види корупції, настійно закликає розробити правові положення для конфіскації коштів та майна, отриманих внаслідок корупції, забезпечити прийняття відповідних заходів проти підприємств, причетних до неї [2].

Рада Європи створює модель гармонізації правових норм, спрямованих як проти транснаціональної, так і проти внутрішньодержавної корупції, в першу чергу з метою створення сприятливих умов для надання більш ефективної правової взаємодопомоги у досяжних Раді Європи географічних межах.

Не менш важливу роль покликані зіграти неурядові міжнародні організації, зокрема, Транспаренсі Інтернешнл (Transparency International, далі ТИ), міжурядової організації моніторингу корупційності, створеної ООН в 1984 році. Найголовнішим завданням ТИ залишається формування антикорупційної середовища, яка виключала б можливість існування та поширення цього, здається, «непереможного» корупційного зла. Пріоритетним напрямком в реалізації цієї ідеї є формування антикорупційних коаліцій, які повинні не тільки приймати міжнародні акти, що протистоять хабарництву, але і втілювати в життя їх зміст, а також норм інших документів у цій сфері, встановлюючи критерії законної і моральної поведінки, цінність яких завжди надзвичайно висока [2].

Комплексність і багатогранність корупції, як явища, полягає ще й у тому, що насправді йдеться не про один, а по суті два різних явища – великої корупції і дрібної корупції, між якими немає суворої взаємозалежності. Саме до такого висновку приводить вивчення історії корупції. Наприклад, як вже було сказано, раніше була дуже поширена дрібна корупція. Без подарунка або хабаря не можна було дістати дефіцитний товар, а більшість товарів були дефіцитними [4].

Тому, всі підприємства тримали постачальників, які постійно давали дрібні хабарі чиновникам за право одержати для підприємства ті чи інші товари або ресурси. Можна сказати, що дача дрібних хабарів чи подарунків, була невід'ємною частиною роботи постачальників. І навіть прості громадяни були змушені постійно давати дрібні подарунки або хабаря: то продавцю, або директору магазину за дефіцитний товар, то головлікаря клініки за кваліфіковане лікування, то пляшку горілки сантехніку за якісний ремонт, і навіть швейцарові або метрдотелю за право потрапити в ресторан.

Список використаних джерел:

1. Марк Піт. Міжнародні заходи по боротьбі з корупцією. // Вісник ООН.

2. Овчинский Ст. С.. Кримінальна глобалізація і Конвенція ООН проти транснаціональної організованої злочинності. Монографія – М. : ІНФРА-М. - 2001.

3. Номоконов Ст. А. Росії потрібна стратегія боротьби з корупцією. // Журнал «Чисті руки». – 2007. - № 4.

4. Про проблеми міжнародної корупції // Журнал «Боротьба зі злочинністю за кордоном» (за матеріалами зарубіжної преси). - 2001. № 8.

----------***----------

Скиба Я. В., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

КОРУПЦІЯ ЯК БАГАТОГРАННЕ НЕГАТИВНЕ СУСПІЛЬНЕ ЯВИЩЕ. ПРОБЛЕМАТИКА ВИЗНАЧЕННЯ ПОНЯТТЯ «КОРУПЦІЯ»

Корупція – дуже складне негативне соціальне явище, яке вже протягом тривалого часу турбує не тільки Україну, а й весь світ.

За даними міжнародної організації Transparency International в 2016 році Україна зайняла 131 місце із 176 держав по стану корупції в країні, тоді як в 2007 році вона займала 118 місце. В 2012 році Міжнародна аудиторська компанія Ernst & Young опублікувала результати свого дослідження,

поставивши Україну в трійку найбільш корумпованих держав в світі на рівні з Колумбією і Бразилією.

Корупція - це настільки глобальна проблема, що має негативний вплив на всі державні сфери, а тому безпосередньо посягає на державну захищеність.

Більш за все, страждає економіка країни, адже це та сфера, де величезні прибутки є підґрунтям для розвитку корупційних зв'язків. Ось неповний перелік тих негативних наслідків в економіці, до яких може призвести корупція: розвиток тіньової економіки, порушення принципу добросовісної конкуренції на ринку, що призводить до зниження ефективності ринкової економіки, ускладнення бюджетних проблем України внаслідок неефективного використання бюджетних коштів, підвищення цін через «корупційні витрати», зниження ефективності роботи підприємств, установ та організацій внаслідок розвитку в них корупції, негативний вплив на імідж України в світі, внаслідок чого, відбувається блокування іноземних інвестицій. Щодо негативних наслідків в політичній сфері, то можна виділити: зниження рівня легітимності політичної влади, порушення основних принципів формування та функціонування влади в державі, відчуження влади від народу, внаслідок чого, втрачається авторитет державної влади, знижується рівень довіри населення, підпорядкування влади приватним та корпоративним інтересам, в окремих випадках інтересам корумпованих угруповань та кланів.

Корупція також призводить до порушення державою загальновизнаних принципів, що є прямою загрозою міжнародній безпеці. Як результат, у держави складається негативний імідж на світовій арені, ускладнюються відносини з іншими державами та міжнародними організаціями, втрата країною своїх позицій на економічній та політичній сценах, зокрема можливе виключення або неприйняття держави до міжнародних інституцій,

негативний вплив на економічні відносини між державами (припинення інвестування, відмова у наданні кредитів).

Для того, щоб боротись з чимось, необхідно знати його сутність. Тому, для боротьби з корупцією потрібно, перш за все, дати визначення цьому поняттю.

Явище використання особами, які займали важливе місце в суспільстві і володіли певною владою, свого становища задля задоволення власних потреб та інтересів, з'явилось ще в стародавні части. Проте, саме слово «корупція» (від лат.*corrumpere* — псувати) спочатку використовували в побуті, де воно означало процес псування їжі чи води, а згодом цим словом називали певні негативні діяння, за які передбачалось покарання, такі як розпусність молоді чи розлад порядку в полісі.

Як термін, що позначає саме зловживання посадовими особами наданою їм владою задля задоволення власних інтересів, він був вперше застосований в 80-х роках XX ст. До цього вживали такі терміни, як «хабарництво» або ж «зловживання службовим становищем».

Багато науковців, як вітчизняних, так іноземних, намагаються зрозуміти природу цього поняття та дати йому визначення, проте, до цього часу вони не можуть дійти єдиного висновку і кожен має власний погляд на дану проблему.

Перші спроби надати повне визначення терміну «корупція» були здійснені ще в середньовіччі. Так, наприклад, відомий політичний мислитель Нікколо Макіавеллі говорив, що корупція – це використання публічних можливостей у приватних інтересах [4].

Найбільш активна діяльність щодо дослідження поняття «корупція» була за радянських часів, і саме радянські вчені здійснили найбільш важливий внесок у вивчення явища корупції.

Проте, часто в Радянському союзі поняття «корупції» асоціювалось з поняттям «хабарництва», про що свідчить визначення, наведене в підручнику

для вузів і юридичних факультетів з Криміналістики за ред. Яблукова : «Корупція - злочин, що полягає в одержанні службовою особою особисто або через посередників матеріальних цінностей, або будь-якого іншого майна чи майнових вигод за виконання або невиконання в інтересах того, хто дає хабар, будь-якої дії, яку службова особа повинна була або могла вчинити, використовуючи своє службове становище» [5].

На мою думку, ототожнювати поняття «корупції» та «хабарництва» є неправильним, так як хабарництво, на відмінну від корупції, передбачає надання та отримання саме матеріальних цінностей, тоді як корупція передбачає також отримання послуг та інших нематеріальних цінностей.

Ця думка підтверджується визначенням «корупції» як зловживання державною владою задля отримання вигоди в особистих цілях», яке було наведено в документі ООН «Про міжнародну боротьбу з корупцією». На думку ООН, явище корупції ширше і включає в себе «хабарництво», яке означає одержання або надання службовій особі хабару для отримання певних вигід, «непотизм» або ж інша назва – «кумівство», коли посади надаються родичам або знайомим, незалежно від їх професійних здібностей, а також протиправне привласнення публічних коштів для особистого використання.

Більш широке та більш влучне, на мою думку, визначення наведено в Конвенції «Про Кримінальну відповідальність за корупцію», прийнятій в 1995 році міждисциплінарною групою з боротьби з корупцією, скликаної Радою Європи: «Корупція – це хабарництво та будь-яка інша винагорода особі, якій доручено виконання певних обов’язків у державному, або приватному секторі, що веде до порушень зобов’язань, покладених на неї за статусом державної посадової особи, приватного співробітника, незалежного агента, або іншого роду відносин з метою отримати будь-які незаконні вигоди для себе та інших» [2].

Неспроможність науковців дійти єдиної думки щодо визначення поняття «корупція» , пов’язана з тим, що явище «корупції» є багатогранним явищем і існує в трьох аспектах: політичному, соціально-економічному та правовому. А тому, кожне з наведених визначень є вірним, просто відображає сутність цього поняття лише з одного боку.

Так, прихильник політичного змісту корупції І.Корж стверджує, що «політична корупція дає змогу конвертувати владу в капітал, а капітал – знову у владу» [3].

З економічного боку розглядає корупцію І. Мазур зазначає: « Корупція– це комерціалізація посадовими особами своїх функціональних обов’язків» [4].

Прихильники правової природи корупції вважають, що вона полягає в уповільненні прийняття необхідних законів, а також прийнятті таких законів, які дають можливість їх неоднозначного тлумачення.

Однією з умов вступу України до ЄС є подолання корупції в державі. Намагаючись задовольнити цю вимогу, в Україні розпочали боротьбу з вказаною проблемою, зокрема було створено декілька спеціальних органів, а також розроблено законодавство щодо боротьби з корупцією. Так, відповідно до Закону України «Про запобігання корупції» від 14.10.2014 , « корупція - використання особою, зазначеною у частині першій статті 3 цього Закону, наданих їй службових повноважень чи пов’язаних з ними можливостей з метою одержання неправомірної вигоди, або прийняття такої вигоди, чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб, або відповідно обіцянка/пропозиція, чи надання неправомірної вигоди особі, зазначеній у частині першій статті 3 цього Закону, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов’язаних з ними можливостей» [1].

На мою думку, визначення є не досить вдалим, так як повністю не відповідає нормам міжнародного законодавства. Так, відповідно до Закону

суб'єктами корупційних діянь можуть бути тільки службові особи, якщо це стосується використання службових повноважень та будь-яка особа, яка пропонує або надає неправомірну вигоду, тоді як в жодному міжнародному акті немає вказівки на те, що суб'єктом є саме службова особа, це може бути особа, яка наділена певними обов'язками та можливостями. Не відповідає також і об'єкт корупційних діянь. Відповідно до міжнародних норм - це є будь-який обов'язок особи та її поведінка, тоді як в українському законодавстві об'єктом є службові повноваження та пов'язані з цим можливості. Також не враховано ситуацію, коли особа отримує відповідні матеріальні блага або пільги платно, за встановленою ціною, проте не маючи на те відповідних підстав або порушуючи права інших осіб, наприклад позачергово. Позитивним нововведенням в антикорупційному законодавстві є відповідальність осіб за пропозицію та надання неправомірної вигоди. Проте, особа, яка надає неправомірну вигоду, може бути тільки посередником, тоді в Законі варто також зазначити, що суб'єктом в такому разі є особа, від імені якої надається неправомірна вигода, і в інтересах якої здійснюється використання службових повноважень.

Отже, корупція – основна загроза соціально-економічного розвитку населення, тому, основним завданням сьогодення є пошук ефективних шляхів подолання цієї загрози. Першим і найбільш важливим кроком має бути удосконалення українського антикорупційного законодавства, зокрема, щодо визначення поняття «корупції», яке на даний момент є не досить вдалим і не відображає повністю сутності цього явища. Законотворцям варто було б враховувати думки науковців, а також варто було б взяти до уваги визначення поняття «корупції», наведені в документах міжнародних організацій, таких як: Конвенція ООН «Про міжнародну боротьбу з корупцією», Конвенції Ради Європи «Про Кримінальну відповідальність за корупцію» та ін.

Список використаних джерел:

1. «Про запобігання корупції» :Верховна Рада України; Закон від 14.10.2014 № 1700-VII
2. Кримінальна конвенція про боротьбу з корупцією (ETS 173) Рада Європи; Конвенція, Міжнародний документ від 27.01.1999 № ETS173
3. Корж І. Політична корупція та правова безпека України / І. Корж // Право України. – 2009. – № 6. – С. 55–60.
4. Мазур І. Корупція як інститут тіньової економіки / І. Мазур // Економіка і право. – 2005. – № 8. – С. 34–38.
5. Яблоков Н.П. Криминалистика: учебник для вузов и юрид. факультетов / Н.П. Яблоков. – М.: ЛексЭст, 2003. – 376 с.

----------***----------

Єсипенко Ю. О., *студентка ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В.М., *к.т.н., доцент.*

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЇЇ ОБ'ЄКТИ

Історія людства свідчить, що важливим чинником його розвитку була і є інформація. Інформація і стрімкий розвиток інформаційних технологій нині потребують формування системи інформаційної безпеки.

Перш за все, необхідність розвитку інституту інформаційної безпеки, як на теоретичному, так і на практичному рівнях, зумовлене загрозами людині, пов'язаними з обігом інформації. Кожен з нас, хоче бути захищеним від будь-яких спроб посягання на власні честь та гідність, власний спосіб життя. Однак, досить часто ми навіть не замислюємося над тим, що викладені у соціальні мережі фотографії чи написані повідомлення, які здаються сьогодні безпечними, через кілька років можуть стати основою компромату проти нас.

Ми вважаємо, що інформаційна безпека – це стан захищеності життєво-важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:

1) негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої за визначеною метою неповної, невчасної, невірогідної та упередженої інформації;

2) негативні наслідки застосування інформаційних технологій;

3) несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням [3].

Важливим для визначення інформаційної безпеки є з'ясування об'єктів інформаційної небезпеки, тобто тих сфер суспільного життя, які захищаються.

До об'єктів інформаційної небезпеки належать:

А) людина, соціальні групи, суспільство, держава;

Б) інформація як об'єкт суспільних відносин;

В) інформаційно-комунікаційна інфрастуктура, у т.ч. об'єкти критичної інфраструктури [3].

Аналіз чинного законодавства дає підстави вважати, що більшість норм спрямовані на захист інформації. Так, Кримінальний кодекс України містить в Особливій частині склади злочину, які передбачають відповідальність за порушення нормального обігу інформації, тобто її спотворення, знищення, несанкціонований доступ до неї та її поширення [2].

Проте, ми вважаємо підхід, спрямований на захист інформації, як особливого об'єкту суспільних відносин, недоречним в умовах, коли існує реальна загроза людині. Стаття 3 Конституції України визначає людину, її життя й здоров'я, честь і гідність найвищою соціальною цінністю. А тому, на мій погляд, серед пріоритетів у системі об'єктів захисту в рамках інформаційної безпеки має бути саме людина [1].

Це особливо актуально нині, коли кожна людина може стати жертвою інформаційного насильства, маніпуляцій свідомістю, що забезпечується за

рахунок втягнення людини до віртуального простору та тиск на її базові потреби.

Ще однією загрозою для людини - є зосередження великої кількості персональної інформації у різних суб'єктів. Витік такої інформації може призвести до тяжких наслідків. На жаль, нині, не кожен розуміє таку загрозу, коли надає у віртуальному просторі згоду на обробку персональних даних.

Окремо, слід зазначити про важливість захисту суспільства й держави, які також є об'єктами інформаційної безпеки та потребують захисту.

Так, джерелом небезпеки є ускладнення інформаційних систем і мереж зв'язку критичної інфраструктури, що забезпечує життя суспільства.

Такі загрози можуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов техніки і програмного забезпечення, шкідливого впливу зі сторони злочинних структур і кримінальних елементів[4, с.101-103].

Не менш небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації (ЗМІ) в руках невеликої групи власників. У такому випадку, створюється загроза маніпуляції свідомістю суспільства, поширення екстремістських ідей та антисоціальних установок.

Особливо актуальним є зростання комп'ютерної злочинності та тероризму. Такі загрози існують, як щодо суспільства, так і щодо держави.

Отже, як бачимо, нині існує низка загроз людині, суспільству й державі. Проте, на жаль, законодавець, поки що, ставить в пріоритет політики у сфері інформаційної безпеки захист інформації. Ми вважаємо, що держава має захищати передусім життєво-важливі інтереси суспільства й держави, людину як найвищу соціальну цінність.

Список використаної літератури:

1. Конституція України. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
2. Кримінальний кодекс України. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2001-05

3. Про поняття «інформаційна безпека» / Фурашев В.М. // Правова інформатика. – 2011. – № 1(29). – С. 47-53.

4. Правове забезпечення інформаційної діяльності в Україні/ Володимир Горобцов, Андрій Колодюк, Борис Кормич та ін.; Ред. І. С. Чиж; Ін-т держави і права ім. В.М.Корецького, Нац. Академія Наук України, Держ. комітет телебачення і радіомовлення України. -К.: Юридична думка,2006. - 384 с.

----------***----------

Кушнір К. О., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

БЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ

Що ми розуміємо під безпекою інформаційних систем? Її можна визначити як спосіб захищеності системи від втручання в процес її функціонування (випадкового або навмисного), в тому числі від можливості розкрадання інформації, яка отримана несанкціоновано [1].

Захист інформації - це важлива складова частина підтримання національної безпеки України. Організувати захист інформації можливо завдяки системі, таких заходів, як правові, організаційні та інженерно-технічні. Інформацією є зафіксоване на інформаційних носіях уявлення про предмети, процеси, явища чи події [2, с. 7].

Що ж являє собою загроза інформаційної безпеки? Це умови та фактори, які є небезпечними для життєво-важливих інтересів людини, усього суспільства та держави в інформаційному напрямку. Існують три групи основних загроз інформаційної безпеки:

1) Загроза впливу недостовірної, чи неякісної інформації, яка негативно впливає на особу, державу чи суспільство;

2) Загроза щодо інформаційних прав та свобод громадянина (право на одержання, передачу, або виробництво, а також використання інформації;

3) Загроза стосовно права на інтелектуальну власність особи, право на особисту таємницю, на захист честі та гідності людини.

Всі фактори загроз можна розподілити за видовою ознакою на: політичні, економічні та організаційно-технічні [3, с. 14].

У Законі України «Про інформацію» вказано, щоб захистити інформації, потрібно вживати наступні заходи:

а) перетворити інформацію завдяки спеціальним даним, щоб приховати зміст цієї інформації, підтвердити її справжність та цілісність;

б) засоби та методи, які мають можливість забезпечити конфіденційність та доступність конкретної інформації за умови впливу на цю інформацію загрози (природного або штучного характеру);

в) правові, адміністративні, організаційні, технічні та інші заходи, які можуть забезпечити збереження цілісності інформації та доступу до неї;

г) діяльність, яка спрямована на забезпечення конфіденційності та доступності інформації.

Суб'єктами інформаційних відносин являються фізичні та юридичні особи, інформація про них.

Предмет суспільного інтересу не можна вважати інформацією, яка може свідчити про загрозу державному суверенітету, також про можливість порушення прав людини, забезпечення реалізації конституційних прав, свідчити про фізичну особу, яка є ідентифікованою [4, с. 10].

Враховуючи вищезазначене, можемо зробити висновок, що є характерною для електронних даних особливістю. Це непомітно та легко спотворити, зробити копію чи знищити інформацію. У зв'язку з цим, потрібно організувати безпечність у функціонуванні інформаційних даних, тобто захистити інформацію. Захищена інформація це та, яка не змінила свою достовірність в процесі передачі та збереження даних.

Що стосується несанкціонованих дій стосовно інформації, то вони можуть бути викликані різноманітними причинами та здійснюватися за

допомогою різних методів впливу. Наприклад, такі дії можуть обумовити стихійні лиха (урагани, пожежі, вибухи або інше), техногенні катастрофи, терористичні акти. Боротися з ними дуже важко, враховуючи їх непередбачуваність.

Найбільшим збитком для інформаційних систем є неправомірні дії співробітників та комп'ютерні віруси. З метою захисту інформацій, в комп'ютерних та інформаційних мережах часто використовують різні програмні та технічні засоби. Це, наприклад, системи обмеження доступу до даного конкретного об'єкту, сигналізація чи відеоспостереження. Існує, в тому числі, ефективний захист в комп'ютерних мережах - це маршрутизатор, який фільтрує пакети переданих даних, і, завдяки цьому, з'являється можливість заборони здійснення детального контролю адреси відправника чи одержувача.

Отже, всі заходи стосовно збереження та захисту інформації, повинні бути комплексними. Це надає більше шансів для забезпечення безпеки та захисту інформаційних систем.

Список використаних джерел:

1. Інформаційні системи і технології в управлінні організацією. - [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/74227/informatika/bezpeka_informatsiynih_sistem
2. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ — 352 с.
3. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах/ Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. – К., 2013. – 435 с., іл.160.
4. Захист інформації в комп’ютерних системах. Навчально-методичний посібник для студентів напряму 6.040302 Інформатика/ Вакалюк Т.А. – Житомир: Вид-во ЖДУ, 2013. – 136 с.
5. Закон України "Про інформацію" // Відомості Верховної Ради України (ВВР). – 1992.

----------***----------

Бондаренко І. І*., студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

ПРОБЛЕМА ПИТАННЯ ЦИФРОВОГО СЛІДУ ТА ЦИФРОВОЇ ТІНІ

Постановка проблеми: у статті викладена сучасна проблема цифрового сліду, або так званого всезагального стеження.

По-перше поняття:

Цифровий слід (або цифровий відбиток; англ. Digital footprint) - сукупність інформації про відвідування та внесок користувача під час перебування в цифровому просторі. Може включати в себе інформацію, отриману з Інтернету, мобільного Інтернету, веб-простору і телебачення.

Тобто, цифровий слід це всі наші дії пов’язані з глобальною мережею. До таких дій можна віднести всі дії в інтернеті: фотографії та відео, що ви викладаєте, перегляд сторінок, переписки, коментарі, вподобання, покупки тощо.

Головне в цьому питанні - це сфера застосування вашого цифрового сліду, адже саме це постає його як проблему.

Найбезневиннішими для нас є маркетологи. Вони використовують так званий «таргетинг», або «таргет реклама». Реклама, яка створюється на даних відвідування сайтів і запитів пошукових системах.

Це реклама не лише продукції. В сучасному світі правоохоронні органи активно використовують цифровий слід для впізнання злочинців, або тих людей, які потенційно можуть ними стати. Окрім вище перелічених способів, їм також доступні нейротичні мережі, які розпізнають обличчя і вже по його зображенню можуть відшукати пов’язане з ним все, що є в мережі.

Роботодавці почали активно використовувати цифровий слід для вибору кадрів для свої підприємств. Вони «гуглять» вас, аналізують ваші

сторінки в соціальних мережах для того, щоб зрозуміти, що ви з себе уявляєте, наскільки ви серйозна людина і наскільки ви їм підходите. Не дивно, що в сучасних резюме пропонують зробити посилання на соціальні мережі, або прямо кажуть про те, що це необхідно. Не треба більше витрачати час і влаштовувати співбесіди, коли можна відсіяти більшість кандидатів, завдяки цифровому сліду.

І звісно же, як без шахраїв; вони можуть зібрати дані про вас, приватні фото, тощо і почати шантажувати вас. Чи зламати вашу електронну пошту, знайшовши відповідь на «таємне питання» по вашому цифровому сліду.

Цифровий слід, здебільшого, несе негативний характер, щось накшталт «Великого брата», який слідкує за усіма. Так, по факту так воно і є, але хто надає дані цьому брату? – Ми самі.

Так, саме від нас все залежить, як ми будемо себе вести в мережі, не дивлячись на те, що зараз деякі вважають інтернет чи не єдиним засобом демократії. Він все одно потребує від нас певної дисципліни і рамок.

Скільки буде відомо про вас залежить від ваших дій. Всі ваші фото, відео, коментарі, «лайки» стають надбанням суспільства, а з ними уже роблять, що хочуть.

Рекомендації:

Для початку, варто переконатись, що ваш інтернет-портрет відповідає вашому справжньому. Це все здебільшого потрібно для роботодавців. Якщо, ви цікава людина, це може навіть підвищити ваші шанси, адже зараз вирішальною якістю є креативність. Демонструйте свою кращі сторони, ваш стиль, ваші захоплення. Але не варто нападати на когось, ображати чи звертати на себе увагу якимись необдуманими діями.

Спробуйте «прогуглити» себе, яку інформацію про вас знаходить пошукова система?

Якщо взагалі все погано, ви можете видали свої сторінки в соціальних мережах. Через деякий час (в середньому місяць), ваші дані звідти повністю будуть знищенні.

Можна зробити висновок, що необхідно просто кожен раз обдумувати, що ви викладаєте і пишете, бо це формує ваш образ в очах людей, які це бачать.

Список використаних джерел:

1. «Цифровой след цифрового следа. Что раскроют спецслужбам метаданные». – [Електронний ресурс]. – Режим доступу: http://crime.in.ua/statti/20130912/metadannye
2. ЦИФРОВОЙ СЛЕД ИЛИ О ТОМ, ЧТО РАБОТОДАТЕЛИ ИЩУТ В GOOGLE. – [Електронний ресурс]. – Режим доступу: http://www.gadgetstyle.com.ua/employers-and-google-search/
3. Валерий Сидоров, Что такое Digital Footprint, или Как узнать, сколько «цифрового хлама» мы производим ежедневно? – [Електронний ресурс]. – Режим доступу: http://netler.ru/pc/digital-footprint.htm

----------***----------

Григор'єва (Рубель) М. Р., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *доцент, к.т.н..*

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ КОМП`ЮТЕРНОГО ТЕРОРИЗМУ В УКРАЇНІ

Аналіз останніх наукових робіт та публікацій у ЗМІ щодо діяльності терористичних організацій в інформаційному просторі проведений академіком Гавришем показав, що найбільший інтерес для терористів становлять: енергетична сфера; військова та ядерна структура держави; сфера транспортних перевезень (особливо повітряний транспорт) та фінансова сфера держави [2]. Дослідження, проведені Інформаційною групою Комісії з консультацій в області безпеки національних телекомунікацій США щодо уразливості систем електропостачання кібератакам, показали, що "фізичне

руйнування все ще являє найбільшу загрозу, з якою може зіштовхнутися енергетична інфраструктура. Поряд із цим вже з'явилася проблема електронного вторгнення, але вона все ще становить відносно незначну небезпеку" [6]. На думку експертів, з усіх перелічених сфер життєдіяльності людини найбільш відкритою для глобального інформаційного простору є саме фінансова сфера, яка є привабливою для потенційних кіберзагроз – втручання у роботу банків, фондових бірж, зрив міжнародних фінансових угод. Це пов'язано з тим, що сьогодні вся фінансова система зорієнтована на спрощення системи доступу клієнтів до банківських, торгівельних і біржових послуг із використанням нових інформаційних технологій (в тому числі і здійснення багатьох операцій у мережі Інтернет) [3]. Таким чином, в контексті макроекономіки збої в системах електропостачання, збої у функціонуванні транспортного руху та інші "сценарії" кібертерору – стандартні події, які не стосуються національної безпеки. Для національної економіки, де десятки або навіть сотні систем забезпечують найважливіші інфраструктури, збій у системах унаслідок кібератаки може залишитись непоміченим у повсякденному житті або бути віднесеним до стандартних затримок та виходу з ладу обладнання (крім випадків, коли атака буде поєднана з фізичним нападом – застосуванням вогнепальної зброї, вибухами, захопленням стратегічно значущих об'єктів). В контексті інформаційної безпеки все більшу небезпеку становить всесвітня глобальна мережа Інтернет, що через свою відкритість і анонімність стає головним "інформаційним полем", яке використовують терористичні організації у своїх цілях:

— збір коштів для підтримки терористичної діяльності (у тому числі шляхом шахрайства, вимагання та шантажу);

— поширення агітаційно-пропагандистської інформації про діяльність терористичних організацій, їх цілі та завдання, наміри, форми

протесту, звернення до масової аудиторії з повідомленнями про визнання своєї відповідальності за вчинені теракти тощо;

— здійснення організаційної діяльності, наприклад, розміщення у відкритому доступі й розсилання відкритих та зашифрованих інструкцій (наприклад, інструкцій з самостійного виготовлення вибухових пристроїв), повідомлень про час зустрічей зацікавлених осіб тощо;

— анонімне залучення до терористичної діяльності співучасників, наприклад, хакерів і представників бізнесу, які надають різні інформаційні послуги на комерційній основі;

— планування та координація дій, яка надає можливість децентралізувати управління терористичними організаціями та розширити потенціал малих терористичних груп;

— здійснення інформаційно-психологічного впливу на населення з метою шантажу, створення паніки та поширення дезінформації тощо.

Крім того, на даному етапі терористи зосереджують свої зусилля на зборі інформації та формуванні баз даних. У цьому контексті терористи переслідують дві основні мети. Одна – формування компромату (на підставі отриманих персональних даних про приватне життя керівників країн, банків і корпорацій), завдяки якому можна спробувати вплинути на керівників різних рівнів і отримати доступ до необхідних інформаційних ресурсів країни або корпорації. Інша – створення баз розвідувальних даних, які використовуються при підготовці атак. Наприклад, японське терористичне угруповання “Аум Сінрікьо”, яке здійснило газову атаку в токійському метро в 1995 році, перед цим створило комп’ютерну систему, що була здатна перехоплювати повідомлення поліцейських радіостанцій і відслідковувати маршрути руху поліцейських автомобілів [7]. Інформаційну боротьбу можна визначити як боротьбу сторін за завоювання переваги щодо кількості, якості та швидкості здобування інформації, її своєчасного аналізу й використання [5]. Напади на комп’ютерні мережі за допомогою несанкціонованого доступу здійснюються

з метою порушення роботи відповідних установ. Так, Відділ захисту Пентагона свідчить, що кожного тижня інформаційні вузли Міністерства піддаються більш ніж 60 нападам. Більшість із них здійснюють хуліганські хакери, але під час бомбардування Югославії у 1999 році групи хакерів з Росії, Сербії та інших країн цілеспрямовано атакували належні американським державним структурам сервери, що завдало значної економічної, військової та політичної шкоди країнам НАТО. До сьогодні кібертероризм не завдав будь-якої суттєвої шкоди урядовим чи комерційним мережам й поки не становить великої загрози (крім таких країн, як США, Швеція, Шрі-Ланка та деяких інших). Разом із тим багато спеціалістів наголошують на недостатньому рівні захисту життєво важливих інформаційних вузлів. На думку сучасних фахівців з комп'ютерного тероризму, сьогодні основною метою терористів, перш за все, є здійснення масового деструкційного впливу на психіку та свідомість людей у потрібному для них напрямі, з використанням інформаційних систем і систем зв'язку. Можна припустити, що головним напрямом кібертерористів у майбутньому буде створення систем дистанційного маніпулювання свідомістю як конкретної людини, так і суспільства в цілому [4]. Тому таке використання терористичними організаціями інформаційних технологій і глобальної мережі Інтернет у недалекому майбутньому може стати однією з нових і небезпечних загроз людству.

Щодо проявів "комп'ютерного тероризму" на території України, слід зазначити, що одержуючи безсумнівні переваги від використання новітніх інформаційних систем, побудованих на основі глобальних комп'ютерних мереж, Україна також поступово входить у певну залежність від їх ефективного функціонування. У звітах правоохоронних органів та роботах дослідників відмічається, що світові тенденції розвитку комп'ютерних технологій дозволяють прогнозувати, що його загроза з кожним роком у світі, в тому числі і для України, буде зростати. Разом з тим, окремі українські

експерти з проблем тероризму вважають, що передумови для проявів тероризму в Україні є [1].

Отже, на основі міжнародного досвіду можемо виділити внутрішні та зовнішні фактори, що можуть вплинути на розвиток кібертероризму в Україні. До внутрішніх можна віднести економічні та соціальні проблеми, що виникли сьогодні у державі, такі, наприклад, як різке розмежування населення за рівнем доходів, напруженість у політичному житті, криміналізація всіх сфер життя суспільства тощо. До зовнішніх – те, що процеси глобалізації та подальша ескалація тероризму у світі, навряд чи залишать Україну осторонь, бо сьогодні наша держава залишається одним з найбільших європейських коридорів. До того ж Україна є активним учасником міжнародної безпеки, наші контингенти беруть участь у миротворчих операціях у різних країнах світу, що неминуче притягує до нас увагу світового тероризму.

Список використаних джерел:

1. Василь Крутов: “За міжнародну безпеку у відповіді всі країни”. [Електронний ресурс]. – Режим доступу: <http://www. antiterunity. org/ru/massmedia/krutov080627. php>.
2. Гавриш, С. Б. Комп’ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії [Електронний ресурс] / С. Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика).— Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm
3. Гриняев С.Н. Информационный терроризм: предпосылки и возможные последствия. [Электронный ресурс]. – Евразийский вестник. – № 19, Режим доступа к журналу: <www. e-journal. ru/besop-st3-19. html>. 12
4. Клепов А. Кибертерроризм и свобода личности. [Электронный ресурс]. – Режим доступа: <http://www. proza. ru/2009/04/10/500>.
5. Попов М.О., Лук’янець А.Г. До забезпечення воєнної безпеки в умовах загрози інформаційної війни // Наука і оборона. – 1999. – № 2. – 37–43.
6. Strategic Goal One: Keep America Safe by Enforcing Federal Criminal Laws (Fiscal Year 2000 Performance Report and Fiscal Year 2002

Performance Plan). – P. [Електронний ресурс]. – Режим доступу: <http://www. usdoj. gov/ag/ annualreports/pr2000/NewSG1. pdf>. 10

7. Verton D. Black Ice: The Invisible Threat of Cyberterrorism. – N. Y, 2004. – 304p.

----------***----------

Ліненко Ю. О., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

КІБЕРЗЛОЧИННІСТЬ

Інформаційні технології з кожним днем все сильніше і сильніше стають частиною нашого життя. Межа між реальним і віртуальним просторами поступово зникає. Це відбувається, в тому числі, тому, що у віртуальному просторі з'являються явища, які, як здавалось раніше, можуть бути притаманні лише простору реальному. Наприклад, злочинність.

Про таке явище як, кіберзлочинність, доводиться чути, напевно, кожному. Дуже багато людей, навіть, стикаються з ним напряму. Загроза присутня одночасно і на національному рівні, і на міжнародному. Об'єктом кіберзлочинів може бути що завгодно, але все так, чи інакше зводиться до важливої особистої інформації (паролі, персональні дані тощо)[1]. Одним із найрозповсюдженіших проявів кіберзлочинності є піратство (порушення авторських прав). Рівень піратства в Україні нині перевищує 80 %. Швидкий розвиток інформаційних технологій, по суті, лише загострює проблему, адже законодавці банально поспішають за ним. І це – не уривок із сценарію голлівудського науково-фантастичного трилера, чи роману Стівена Кінга. Це – констатація факту.

Кіберзлочинність може мати дуже різні прояви. Але, конкретно, в Україні до кіберзлочинів відносять[3]:

— вже зазначене порушення авторського права;

— порушення прав суміжних з авторським;

— шахрайство;

— незаконні дії з документами на переказ;

— незаконні дії з платіжними картками;

— незаконні дії з іншими засобами доступу до банківських рахунків;

— виготовлення обладнання для вчинення зазначених дій;

— ввезення порнографічних предметів;

— виготовлення порнографічних матеріалів;

— збут порнографічних матеріалів;

— незаконне використання відомостей, що становлять комерційну таємницю;

— незаконне збирання таких відомостей;

— незаконне використання відомостей, що становлять банківську таємницю;

— незаконне збирання таких відомостей.

На щастя, засоби захиститися від кіберзлочинів, або, принаймні, мінімізувати їх вірогідність існують:

- використання надійних паролів, які регулярно замінюються;

- використання антивірусних програм;

- періодична перевірка облікових записів;

- використання спеціальних інструментів конфіденційності та безпеки.

З приводу кіберзлочинності, було проведено дослідження Міжвідомчим науково-дослідним центром з проблем боротьби з організованою злочинністю, Національною академією внутрішніх справ й Науково-дослідним центром правової інформатики АПрН України. Результатом їхніх спільних зусиль, стала Концепція стратегії реалізації державної політики, щодо боротьби з кіберзлочинністю. У грудні 2001 року дана концепція була розглянута й схвалена вченою радою Національною академією внутрішніх справ України[2].

Інше важливе дослідження, було проведене Департаментом інформаційних технологій МВС України у 2002 році, згідно з яким вдалося встановити наступне: у 2002 році було виявлено близько 25 кіберзлочинів, з них: розслідувано було 15, зупинено на підставі п. 3 ст. 206 КПК України – 5.

Далі більше. 2003 рік: виявлено – 66 злочинів, розкрито – 45, зупинено справ – 19. 2004 рік: виявлено – 52, розслідувано – 38, зупинено – 16. 2005 рік: виявлено – 60, розслідувано – 31, зупинено – 33.

Негативна тенденція збільшення кількості нерозкритих кіберзлочинів продовжує зростати.

Серед причин можна назвати наступні:

— вчинення більшість кіберзлочинів є швидкоплинним й прихованим;

— кіберзлочинці часто є дуже оснащеними й висококваліфікованими;

— обмін інформацією між правоохоронними органами різних держав є погано узгодженим;

— високий рівень недовіри потерпілих до правоохоронних органів;

— профільних вузів для підготовки спеціалістів в даній галузі практично нема;

— обдарована молодь знаходить соціальної неприваблив працю в даній сфері через неналежний рівень фінансування;

— між спецпідрозділами різних відомств наявна нездорова конкуренція.

Кіберзлочинність (як і будь-який інший різновид злочинності) об’єктивно є явищем, яке неможливо викорінити цілком і повністю, так, щоб воно взагалі зникло. Можна лише суттєво знизити його рівень.

Цього можна досягти наступними засобами:

— розвивати дослідження у сфері заходів зниження рівня хуліганської і кримінальної активності в Інтернет;

— сайти торгівельних компаній й компаній, що займаються наданням послуг мають пройти сертифікацію й інвентаризацію на предмет попередження шахрайства;

— створення у українському сегменті Інтернет - сайтів присвячених протидії кіберзлочинності.

Роблячи висновки, хотілось би сказати, що знизити рівень кіберзлочинності, можна лише активними діями. Крім того, позитивні результати проявлять себе лише через деякий час. Миттєвого ефекту не буде.

Життя не стоїть на місці. Будь-які засоби протидії будуть породжувати зустрічну протидію. Це замкнуте коло, яке неможливо розірвати. Можна лише постійно вдосконалювати засоби боротьби й бути в курсі з часом.

Список використаних джерел:

1. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине // Закон и жизнь. – 2004. – № 7. – с. 15
2. Біленчук Д.П. Кібрешахраї – хто вони? //Міліція України, 1999. №7-8. С.34
3. Біленчук П.Д.,Романюк Б.В.,Цимбалюк В.С. Комп'ютерна злочинність - К.: Атіка, 2002,С.25

----------***----------

Вінтоник Т. М., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцет.*

КІБЕРЗЛОЧИН, ЯК ЗАГРОЗА ДЛЯ КОЖНОГО

В світі кримінально-правових феноменів, тероризм посідає одне з перших місць, в контексті міжнародних злочинів. Одним з проявів тероризму є комп'ютерний тероризм, або як ще часто його називають електронний

тероризм, тероризм в мережі. Технічний прогрес почав настільки швидко розвиватися, що людство не встигло призупинити зростання небезпеки, яке почало зростати, разом з появою нових інформаційних технологій.

Сутність злочинів в мережі, в першу чергу, почало проявлятися в тому, що комп'ютерна інформація почала використовуватися неправомірно, або й сама стала об'єктом для посягання.

Без вагань можна сказати, що розширення сфери застосування комп'ютерних технологій має позитивне значення для розвитку суспільних відносин у сфері інформатизації. Однак, воно ставить перед державою та суспільством нове завдання боротьби із злочинами в цій сфері та створення нормативно правових актів для вирішення цих проблем.

Кіберзлочини, як один із видів злочинної діяльності охоплює великий різновид правопорушень, які здійснюються за допомогою ПК і мережі. Щодо об'єкту кіберзлочинів ними можуть бути, як персональні дані фізичних осіб, так і інформація державного призначення. Науковці стверджують, що даний вид злочинів є небезпечною не тільки на національному, а в деякій мірі на глобальному рівні [2].

Будь-хто, не залежно від статусу, може потрапити під приціл зловмисника, яким зламують систему і отримують доступ до персональних даних. Одними з найбільш поширених видів таких злочинів є: кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг.

Злочинці, у вигідний для них спосіб, застосовують один із видів онлайн атак, для того, щоб досягти поставленої перед собою цілі і створити загрозу для однієї особи чи кругу людей.

Доцільно буде привести приклад ситуації, яка відображає всю загрозу кіберзлочинності та наслідки, до яких призводить злочин

Хочу нагадати чи можливо ознайомити з справою Меган Майєр [1]. У 2006 році в невеликому містечку США посварилися дві подруги, 13-річні школярки - Меган Майєр і Сара Дрю. Мати однієї з дівчат, сприйняла цю

сварку близько до серця і встановила нагляд за колишньою подругою дочки. Вона не найняла для цього приватних детективів, а просто створила в соціальній мережі MySpace аккаунт від імені симпатичного 16-річного хлопця на ім'я Джош Івенс, який втерся в довіру до простодушної Меган Майєр і незабаром завів з нею роман. Лорі писала від імені Джоша втрьох: з 13-річною Сарою, і зі своєю молодою підпорядкованою на роботі Ешлі Гріллс. Одного дня, міфічний Джош, який зумів до того моменту підкорити серце провінційної школярки, раптом почав її всіляко ображати, принижувати і прямо порадив дівчинці позбавити світ від своєї присутності. У той же день, Меган Майєр наклала на себе руки, повісившись у шафі. ФБР, розслідуючи обставини її самогубства, відразу вийшло на слід віртуального Джоша Івенса, чия порада призвела до загибелі дівчинки.

В світі, в такий спосіб, кіберзлочинці призводять до трагічних ситуацій, які в більшості залишаються без покарання, тому, варто дослуховуватися до порад для самозахисту.

Зокрема, дослідники кіберзлочинності та розробники протидії онлайн-тероризму, виділяють декілька правил (порад), як захистити себе від кіберзлочинців.

Перший з підходів, щодо захисту - це створення паролів високого рівня захисту та систематична заміна цих даних. Наступне, на що варто звернути увагу, задля свого захисту - це встановлення противірусних програм на пристрої.

На рівні державної онлайн-системи, потрібно проводити онлайн-уроки, які б навчали людей розпізнавати вірусні програми та прийоми злочинців, використовувати захисні мережі, використовувати можливість конфіденційності та безпеки браузерів.

Загалом, кіберзлочини – це не тільки проблема, це катастрофа, яка зростає з кожним днем і можна передбачити, що завдасть ще більшої шкоди не тільки окремій державі, а і людству в цілому. Тому, на сьогоднішній день

важливим є етап мережевого самозахисту, який хоч і в незначній кількості, але зменшить обсяг кібератак, як на державному так і на міжнародному рівні.

Список використаних джерел:

1. Verdict in MySpace Suicide Case//http://www.nytimes.com/2008/11/27/us/27myspace.html
2. Золотар О. О. Права і свободи людини: інформаційний вимір.

----------***----------

Фарадж Д. Ю., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н, доцент.*

НЕГАТИВНИЙ ВПЛИВ КІБЕРЗЛОЧИННОСТІ НА ОСОБИСТУ ІНФОРМАЦІЙНУ БЕЗПЕКУ

На сьогоднішній день неможливо уявити життя без інформаційних технологій, тобто використання засобів комунікації та комп'ютерної техніки. У діяльності людства майже в усі галузі впроваджуються комп'ютери. З кожним днем зростає кількість інтернет-користувачів, так як, підключення до глобальної мережі є доступним і зручним. Персональний комп'ютер та мобільний телефон, які підключені до Інтернету, можуть сприйматися як необхідне та належне. Інтернет забезпечує доступ до великої кількості інформації, можливості переведення банківських, біржових та торгових операцій, швидку передачу даних, переказ коштів та багато іншого. Для більшості людства Інтернет став цілим віртуальним світом. Але, як і в реальному світі, так і у віртуальному, ніхто не застрахований від злочинів, а саме кіберзлочинів. До кіберзлочинів можна віднести: викрадення комп'ютерної інформації, крадіжку коштів з банківських рахунків, розповсюдження комп'ютерних вірусів, шахрайства з платіжними картками, порушення правил експлуатації автоматизованих електронно-обчислювальних систем тощо.

Поняття «кіберзлочин» утворене з двох слів: «кібер» та «злочин», де «кібер» мається на увазі поняття «кібернетичний простір». Тобто, кіберзлочин означає злочин у кіберпросторі. Даний вид злочинності полягає у тому, що готування до злочину та його скоєння здійснюються, не відходячи від робочого місця. Ці злочини, з кожним днем, стають доступними кожному, так як, дешевшає комп'ютерна техніка і можна скоювати злочини у будь-якому місці, на будь-якій відстані. Наприклад, злочинець знаходиться у Києві, об'єкт посягання – в Алжирі. Можна навести дві причини розвитку і росту кіберзлочинності. Першою причиною є те, що злочинець майже нічим не ризикує на успішне скоєння злочину. Другою причиною є прибутковість, так як, кіберзлочинність дуже прибуткова на сьогоднішній день. Відмінність кіберзлочинця від звичайного злочинця полягає у тому, що для здійснення певної атаки, кіберзлочинцю не потрібна вогнепальна або холодна зброя, його основна зброя це – комп'ютерні віруси, логічні бомби та «троянські коні», які він використовує за наявності комп'ютера та певних хакерських навичок для проникнення до мережі, а також злому та модифікації програмного забезпечення.

Кіберзлочинцем може стати, будь-яка особа, яка захоче зайнятися злочином у мережі Інтернет. Але ж успішність проведення кібератаки може залежати від рівня підготовки особи, яка намагається вчинити злочин: це може бути особа, яка отримала певну освіту в ІТ-технологіях та вирішила зайнятися злочинною діяльністю в мережі Інтернет, або ж це певна особа, яка не має спеціальної освіти, але впевнена в собі та вирішує вчиняти несанкціоновані втручання до чужих комп'ютерів, задля заволодіння певною інформацією. Особи, які починають займатись кіберзлочинністю, мають бути дуже обережними, адже, один невірний крок і особа сама себе видасть, і її буде легко притягнути до кримінальної відповідальності.

На сьогоднішній день, в процесі розвитку найновіших технологій, не треба далеко ходити, щоб стати кіберзлочинцем. Все, що потрібно, – це

наявність комп’ютера та доступ до мережі Інтернет; злочинець починає підшукувати собі потенційну жертву. Візьмемо для прикладу, будь-яку соціальну мережу: для кіберзлочинців - це є однією із золотих жил, адже, люди самі викладають особисту інформацію у себе на сторінці, зокрема, це інформація про ПІБ, адреса проживання, фото- та відеоматеріали, на яких, можливо, видно матеріальне становище особи. Злочинець, за допомогою соціальних мереж, може зібрати певну компрометуючу інформацію про особу для подальшого її шантажу, в процесі чого може збагатитися. Тому, не потрібно у соціальних мережах викладати повну біографію, якщо соціальна мережа є способом зв’язку, шляхом переписок, то можна зробити, так звані, «фейкові» сторінки з неправдивими даними і спокійно переписуватись – це значно захистить від заволодіння особистою інформацією злочинцями. Великій кількості людей притаманна така риса характеру, як бажання отримати щось "на халяву", але це хотіння призводить до їх обману. В мережі Інтернет дуже поширений такий вид злочинності, як інтернет-шахрайство. Яскравими прикладами такого шахрайства, можна назвати лотереї, які не є державними, та спрямовані на те, щоб обдурити певну особу. Організатори таких лотерей записують поштові скриньки тих, хто захопився повідомленою інформацією про, так званий, виграш в лотереї, в якій насправді вони ніколи не брали участь. Після того, як жертви проінформовані про те, що вони ніби то щось виграли, їм пропонують зайти на певний сайт, та у спеціально відведеному рядку, ввести номер та ПІН-код картки свого рахунку, ніби то для оплати послуг доставки, але в кінцевому результаті злочинці, отримавши дані картки, відразу зникають, а особі, яка потерпіла таку атаку, ніхто не поверне втрачені кошти, так як вона сама винна у тому, що трапилось. Одним із найпоширеніших видів інтернет-шахрайства можна виділити «фішінг», від англійського слова «fishing», означає «риболовля», тобто, злочинці займаються виманюванням персональних даних довірливих користувачів Інтернету, а саме, через розсилання дуже великої кількості

листів, замаскованих під офіційні бланки фінансових установ, з посиланням на сайти-пастки, які візуально копіюють сайти банків, казино та крамниць. Прикладом цього виду шахрайства є розсилання на поштові скриньки користувачам Інтернету певних листів з рекламним повідомленням, щось накшталт: «Зареєструвавшись за посиланням у казино X, ви отримаєте 10$ у подарунок». Звичайно, дуже велика кількість, так званих, любителів «халяви» поведуться на це, ризикуючи втратити певну суму коштів, так як, при реєстрації вони вводять кредитні дані та паролі банківських рахунків. До найпоширеніших кіберзлочинів, також, можна віднести: вішинг, кард-шарінг, мальваре та протиправний контент. Вішинг – цей вид кіберзлочинності, який полягає у тому, що злочинці розсилають повідомлення на електронні скриньки з проханнями зателефонувати на певний міський номер, а коли особи дзвонять, то при телефонній розмові у них намагаються випитати конфіденційну інформацію, щодо даних їх банківської картки. Кард-шарінг – це метод, завдяки якому, кілька незалежних ресиверів можуть отримати доступ до перегляду платних каналів кабельного, або супутникового телебачення, при використанні однієї карти доступу. Цей вид злочину полягає у тому, що особа використовує кард-шарінг для перегляду каналів на декількох телевізорах у одному будинку, щоб не платити двічі за одне й те саме. Кард-шарінг завдає багато проблем компаніям та розробникам систем умовного доступу. Мальваре – це вид кіберзлочину, за допомогою якого, злочинці створюють і розповсюджують віруси та шкідливе програмне забезпечення. Протиправний контент – це контент, за допомогою якого, злочинець пропагує тероризм, екстремізм, порнографію, наркоманію та культ жорстокості і насильства. Існує ще багато видів кіберзлочинів, до яких можна віднести: скімінг, кеш-тренінг, кардінг, піратство, рефайлінг, соціальна інженерія тощо.

Незважаючи на наявність органів, на яких покладено забезпечення кібербезпеки, боротьба з кіберзлочинністю та протидія кіберзлочинам

залишається неорганізованою. Тому, на нашу думку, щоб вберегти себе від інтернет-шахраїв, необхідно знати перелік можливих дій, які допоможуть захиститися від атак злочинців. До дій які, можуть вберегти особу від кібератаки можна віднести: створення надійних паролів на захист персональної інформації та періодична заміна їх, встановлення програм антивірусів та використання захищених мереж. Також, щоб вберегти себе від кібератаки, потрібно менше викладати особистої інформації у соціальних мережах, не залишати адресу проживання, контактні телефони та адреси електронних скриньок там, де це не потрібно; завжди пам'ятати, що безкоштовний сир – лише у мишоловці. І потрібно пам'ятати те, що злочинцям легше обдурити ту особу, яка хоче бути обдуреною, тому кожен має бути обережним.

Мироненко Ю. С., *студент ФСП*
КПІ ім. Ігоря Сікорського.
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

КІБЕРСОЦІАЛІЗАЦІЯ: ВИТОКИ ТА НАСЛІДКИ

Розвиток інформаційно-комунікативних технологій призвів до формування нової реальності суспільного буття – віртуального простору, в який поринає все більша частка суспільства. З кожним роком в Україні й світі збільшується частка користувачів мережі Інтернет та соціальних мереж. А це, в свою чергу, призводить до такого явища як кіберсоціалізація.

Під кіберсоціалізацією варто розуміти становлення особистості в соціальному середовищі за допомогою інформаційних технологій, інформаційної комунікації та інформаційної культури. Кіберсоціалізація включає в себе як аспект становлення особи у кіберпросторі, так і особливості її становлення – соціалізації - у соціальному (реальному) середовищі [1, 2].

Питання кіберсоціалізації особливо актуально тим, що її активними суб'єктами є майбутнє нашої країни – діти та молодь. Дослідження впливу віртуального простору на процес становлення особистості та специфічні риси становлення системи знань і цінностей у підростаючого покоління є досить важливими складовими вивчення процесу кіберсоціалізації.

Ми вважаємо, що кіберсоціалізація зумовлена наступними чинниками:

По-перше, комп'ютеризація та інформатизація, а також введення в програму початкової школи курсу інформатики. Останніми роками спостерігається збільшення частки користувачів мережею Інтернет, що зумовлено забезпеченням доступу до комп'ютерної мережі. Також за рахунок комерціалізації інформаційної мережі спостерігається зростання кількості користувачів гаджетами та смартфонами. Нині майже кожен має доступ до комп'ютерної мережі, а тому може бути потенційним користувачем Інтернету. Крім того, особлива увага приділяється вивченню курсу інформатики у школі: з 2013 року вивчення курсу інформатики почалось у молодшій школі та з 5 класу, тим самим забезпечено знаннями про сутність роботи з комп'ютерними мережами та можливості мережі Інтернет дітей [3].

По-друге, наявністю бар'єрів у реальному житті. На жаль, але реальне життя сповнене бар'єрів, які підліток іноді не бажає долати. Це можуть бути бар'єри, викликані природними ознаками (колір шкіри, зовнішність тощо), майновими ознаками (соціальний статус особи, батьків, приналежність до певної соціальної категорії, наявність коштів), географічними (кордони), мовними (незнання певної мови). Віртуальний простір дозволяє уникнути цих бар'єрів та спілкуватися на великій відстані з різними людьми, незалежно від віку, статі, зовнішності, майнового забезпечення [1].

По-третє, недостатній виховний вплив з боку батьків. Важливим чинником на соціалізацію особи є вплив її батьків. На жаль, на сьогодні актуальним є питання усунення батьків від виховання. Ігнорування батьками проблем своїх дітей, намагання шляхом нераціональних обмежень вирішити

їх проблеми або, навпаки, ігнорування таких проблем призводить до загострення конфлікту між поколіннями, що, в свою чергу, лише сприяє входженню особи у віртуальний світ. Особа не знаходить підтримки серед батьків, вчителів чи колективу, а тому починає шукати себе у віртуальному просторі, якій відкритий для неї.

Аналізуючи явище кіберсоціалізації, ми можемо зробити висновок, що це явище має ряд позитивних наслідків. Зокрема, особа може реалізувати себе у віртуальному просторі, знайти цікаві знайомства, обмінюватись інформацією та розвивати мовні навички, спілкуватися з людьми на великій відстані та подорожувати по світу й мати доступ до знань, не виходячи з будинку. Однак при цьому є й певні негативні тенденції, які з кожним роком ми все більше відчуваємо на собі:

По-перше, виникає реальна загроза Інтернет-залежності людини. Дійсно, віртуальне середовище дає можливість особі створити якісно-новий образ самої себе, вдосконалити свої якості та риси (сформувати власну «історію», змінити вік, стать, взагалі уявлення про себе), однак при цьому особа має навички спілкування відповідно до такого, віртуального, образу. У реальному житті така людина досить часто не може знайти себе. Вона не може побудувати комунікацію у реальному середовищі, самореалізуватися та подолати перешкоди. Навпаки, зіштохнувшись з проблемами реального життя, вона поглиблюється у віртуальний простір й стає залежною від нього, що знаходить вияв у поведінці людини (експресивно-емоційна реакція на спроби позбавити таку людини (чи обмежити) доступ до Інтернету, тривале проведення часу в соціальних мережах, постійний моніторинг повідомлень та лайків в соціальних мережах).

По-друге, інтелектуальна, моральна та фізична деградація особистості. Як влучно зазначає А. М. Бежевець, людина є біосоціальною істотою, яка не може існувати поза соціумом. Вихід людини з природного соціального середовища у кібернетичне середовище сприяє її соціальній деградації: такій

людині важче побудувати комунікацію з реальним життям, а споживання низькоякісного контенту (порнографічні, суїцидні матеріали) негативно впливає на інтелектуальний та моральний рівень населення. В людини формується помилкове уявлення, що будь-яку інформацію можна знайти в Інтернеті, що негативно позначається на її самовдосконаленні. Людина обмежена своїм, власно-створеним, образом у віртуальному просторі, але не готова до подолання реальних бар'єрів. Вже сьогодні в суспільства є велика частка людей, які не володіють необхідними комунікативними навичками спілкування, не здатні до творчості та креативності та обмежені при пошуку рішення тією інформацією, яка вже подана в Інтернеті [1].

По-третє, залишається й велика загроза маніпуляцій та інформаційного насильства. Нині вагому частку Інтернет-користувачів складають діти та підлітки, психіка яких лише формується. Під впливом різного контенту зловмисники намагаються маніпулювати свідомістю дітей, схиляючи їх до суїциду, вживання алкогольних, тютюнових чи наркотичних виробів, поширюючи ідеї екстремізму.

На жаль, сьогодні цим проблемам на державному рівні приділено недостатньо уваги. Ми не помічаємо, як у наш час закладаються т.зв. «міни», які через кілька років вибухнути та позначитись на нашому житті. Нездатність людей до їх саморозвитку та самовдосконалення, інтелектуальна та моральна деградація, поширення хвороб, пов'язаних з нерозвиненим ритмом життя, призводять до деградації всього суспільства та стають загрозою для всього людства.

На нашу думку, вирішення проблем кіберсоціалізації полягати в тому, що слід залучати батьків до виховання дитини, прищеплювати підростаючому поколінню творчість та креативність, розвивати інтелектуальний рівень шляхом відмови від стандартизованих програм навчання та подолання існуючих бар'єрів і стереотипів.

Список використаних джерел:

1. А.М. Бежевець. ДЕЯКІ АСПЕКТИ КІБЕРСОЦІАЛІЗАЦІЇ ОСОБИСТОСТІ. - [Електронний ресурс]. – Режим доступу: http://ippi.org.ua/sites/default/files/bamakm_13_1_2015_0.pdf
2. К.В. Музиченко ФЕНОМЕН КІБЕРСОЦІАЛІЗАЦІЇ ПІДРОСТАЮЧОГО ПОКОЛІННЯ. - [Електронний ресурс]. – Режим доступу: http://enpuir.npu.edu.ua/bitstream/123456789/4788/1/Muzychenko.pdf
3. Харченко Н. Динаміка використання Інтернет в Україні: лютий-березень 2016 р. - [Електронний ресурс]. – Режим доступу: http://www.kiis.com.ua/?lang=ukr&cat=reports&id=621

----------***----------

Уліцька В. І., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В.М., *к.т.н., доцент.*

КІБЕРТЕРОРИЗМ: ВИГАДКА ЧИ РЕАЛЬНА ЗАГРОЗА?

XXI сторіччя – ера можливостей. Насамперед, це стосується науки і техніки, що перейшли на новий щабель розвитку – комп'ютеризований. Наразі, ми навіть не до кінця усвідомлюємо, наскільки технології проникли у наше повсякденне життя і який вплив вони мають на наші дії та на нас самих. Що ж робити, якщо еволюція людства досягла такого рівня, яке потребує контролю та навіть захисту? Відповідь на це питання має тільки час, який ми повинні раціонально використовувати для досягнення позитивного результату в цій сфері. Мова йде, про комп'ютерні технології, а особливо про мережу Інтернет, поява якої перевернула з ніг на голову усталене розуміння обороту інформації. У медалі дві сторони – і з цим важко не погодитись. Приносячи неоціненну користь своїм користувачам, Інтернет виступає своєрідним «полем бою» для тих, хто використовує його у зловмисних цілях.

Науковою мовою таке явище має назву «комп'ютерний тероризм» або «кібертероризм». З першого погляду, нічого складного: є хакер – суб'єкт, є об'єкт посягання – певний комп'ютер, вчинення протиправних дій цим

хакером та наслідки, що ці дії тягнуть за собою, а також певна мета. Готовий склад злочину, чи не так? Однак, на законодавчому рівні визначення «кібертероризму» просто не існує, а тому і відповідальності за такі дії бути не може.

Вперше, необхідність назвати таке явище виникла у 1980-х роках і зробив це американський вчений Беррі Коллін. Це поняття мало спрощену форму і означало ведення терористичних дій у віртуальному просторі. Відсутність офіційного визначення не означає, що ця сфера залишилась зовсім без уваги. Основним документом є Конвенція Ради Європи «Про кіберзлочинність» мета якої - є захист від таких загроз. Сам термін у науковій літературі трактується як мотивована атака на інформацію, яку містить комп'ютер чи комп'ютерна система, з метою залякування населення, порушення громадської безпеки та ін., що пов'язана з настанням небезпечних наслідків для життя і здоров'я людей, чи інших тяжких наслідків. Це найбільш оптимальне та зрозуміле нам пояснення цього явища, проте воно, як окрема категорія, потребує неабиякої деталізації.

Кібертероризм слід відрізняти від звичайної хакерської атаки за кількома критеріями:

— ціллю мають бути об'єкти критичної інфраструктури, тобто ті, які мають пріоритетне значення для країни;

— мета, а саме можливість загрози не одному серверу чи комп'ютеру, а цілій мережі;

— наслідки, що є негативними для багатьох людей, їх життя і здоров'я, порушують стабільне функціонування держави як інституту влади.

Вищеперераховані ознаки є притаманними лише для кібертероризму. Що ж до основних ознак всіх комп'ютерних атак, то можна виділити такі: дистанційність, анонімність, порівняно недорога вартість та висвітлення в засобах масової інформації. Якщо при аналізі протиправних дій в Мережі ви

бачите симбіоз таких особливих ознак, включаючи загальні, то будьте певні, що така діяльність може називатись кібертероризмом.

Наразі, перейдемо до практики. Чи існує сьогодні такий вид тероризму, чи це просто цілеспрямовані хакерські атаки? Ніхто в світі не скаже Вам напряму, чи здійснює та, чи інша країна подібні дії, проте існують факти, що підтверджують це. Наприклад, всі ми знаємо, що розвиток комп'ютерних технологій у США, має пальму першості, а створення Кіберкомандування (частина збройних сил США) є беззаперечним доказом цього. 2006 рік – початок негласної кібертерористичної операції США та Ізраїля під назвою «Олімпійські ігри». Головною її метою - є знешкодження, чи хоча б виведення з ладу. основної частини ядерних об'єктів Ірану. Можливо, не в повній мірі, але мета була досягнута і операція діє донині. Чи має право правляча верхівка одних держав, вирішувати долю інших? Звісно ні, якщо, по-перше, це не найвпливовіша держава світу; по-друге, якщо, це -направлено на попередній захист від потенційних загроз у цій сфері. В останньому варіанті можна сказати, що мета виправдовує засоби, адже, США переживає за свою безпеку, проте, перший не дає їм таких повноважень.

В нашому світі діють негласні закони, тому результат тих, чи інших дій часто непередбачуваний. Така проблема набула найшвидшого поширення, саме в Україні, і багато експертів сперечаються щодо природи комп'ютерних атак. Чи спостерігаємо ми зараз таке явище як «кібервійна» і чи є шляхи його подолання?

Ми дотримуємось поглядів Джеймса Ендрю Левіса, що у книзі «Кібернетична війна в перспективі: Російська агресія проти України» виданою під егідою НАТО, обґрунтовує свою позицію доволі переконливими фактами. Простіше кажучи, він не бачить єдності особливих ознак кібертероризму, які були зазначені раніше, а отже, і виключає кібернетичну війну як таку. Свої кібернетичні можливості Росія використовує, в основному, для збирання даних та політичного розладу, тобто, виконання

простих хакерських атак [1]. Ніхто не заперечує проти того, що така агресія має випадки кібертероризму, але вони настільки поодинокі, що немає підстав для оголошення кібервійни.

Одна з наймасовіших таких атак, а найголовніше, успішних, була здійснена на систему управління «Прикарпаттяобленерго», що залишила 230 тисяч мешканців на 6 годин без електроенергії.

Підсумовуючи, можемо зробити декілька висновків:

— кібертероризм та хакерська атака – різні речі, вони співвідносяться як частка і ціле;

— мета хакерської атаки – головним чином провокація, а кібератаки – вплив на критичні об’єкти та тяжкі наслідки;

— проведення поодинокого кібертероризму не є підставою для оголошення кібернетичної війни.

Висловимо думку про власне визначення «кібертероризму» - це здійснення певними контрагентами впливу на об’єкти критичної інфраструктури, за допомогою комп’ютерних технологій, з метою заподіяння руйнівних наслідків, що мають значення для окремої держави.

Щодо пропозицій, то можемо висловити думку про те, що чим швидше буде створене спеціалізоване законодавство в цій сфері, тим ефективніше буде регулювання таких процесів.

Список використаних джерел:

1. Kenneth Geers. Cyber war in perspective: Russian aggression against Ukraine. – Tallin.: NATO Cooperative Cyber Defence Centre of Excellence, 2015. – 175 pp. - [Електронний ресурс]. – Режим доступу: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

----------***----------

Вартовнік А., *студент ФСП КПІ*
ім. Ігоря Сікорського.
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

«КІБЕРХВОРОБИ»

Телефони, ноутбуки, комп’ютери грають дуже важливу роль у житті людини XXI століття, оскільки, багато хто з нас не може уявити себе без цих технологій. Особливо це стосується нового покоління. Без сумніву, нові технології і різноманітні гаджети значно спрощують наше життя, роблять його цікавішим і насиченішим. Але, разом з тим, існують непоодинокі випадки зловживання цими технологіями та пристроями, що призводить до виникнення та розвитку нових хвороб, що мають важкі симптоми і серйозні наслідки. Отже, розглянемо кілька видів таких хвороб [1].

1. Синдром фантомного дзвінка. Як стверджують психологи, до 80% усіх користувачів смартфонів були випадки, коли людині здавалося ніби вона чує, як дзвонить телефон і відчуває його вібрацію. Частіше це трапляється, коли людина очікує на важливий дзвінок і концентрує свою увагу на телефоні. Але цей, начебто, не дуже шкідливий синдром може перерости у невроз, при якому людина буде думати, що її телефон дзвонить постійно, варто тільки відвернутися. Такий невроз може перерости в постійну залежність.

2. «Ефект Google» - вчені ведуть дискусії з приводу того, що це. Деякі стверджують, що наркоманія; інші – що психічний розлад. Полягає воно у тому, що людина вважає, що їй не потрібні знання, так як всю необхідну інформацію можна знайти за пару секунд. Цікаво те, що «ефект Google» діє на особу, яка навіть не підозрює про його наявність у себе. Це відбувається, у зв'язку з тим, що мозок людини просто не запам'ятовує інформацію, незалежно від її волі, так як, набагато простіше знайти інформацію на просторах Інтернет, ніж зберігати її [2].

3. Кіберхондрія – це психологічний розлад, при якому людина ставить собі діагноз і запевняє себе, що має певну хворобу на основі того, що вона досліджує на Інтернет-сайтах ознаки хвороби. Близько 60% осіб, що страждають кіберхондрією і запевняють, що вони мають тяжкі і невиліковні хвороби є фізично здоровими [3].

4. Номофобія – психологічний розлад, що характеризується страхом залишитися без мобільного телефону. Вчені стверджують, що близько 75% людей у світі мають цей психологічний розлад. Людина, котра страждає на нозофобію, може відчувати легке занепокоєння, нервозність, а в тяжких випадках, паніку, коли наприклад на телефоні сідає батарея.

5. Facebook-депресія – ця хвороба все частіше входить в лексикон психологів та психотерапевтів, оскільки, сучасні люди дуже залежні від соціальних мереж. Проблема виникає тоді, коли людина бачить фото або відео своїх знайомих, друзів та інших людей в соціальній мережі і в неї складається враження, що їх життя більш гарне і насичене, ніж її. Від цього з'являється невдоволеність, смуток, що потім переростає в затяжну депресію, яка посилюється з кожним відвідуванням соціальної мережі.

6. Селфіманія. Селфі або фотопортрет стали доволі популярними в останні роки. Для того, щоб зробити цікавий знімок люди, які страждають на селфіманію спроможні ризикувати своїм життям і наражати себе на пряму небезпеку [4].

7. Кіберхвороба. Суть феномена у тому, що при перегляді 3D картинок зіниця фокусується на трьохмірному зображені, при цьому, хрусталик продовжує вловлювати світло, що надходить з екрану і продовжує фокусуватися на двохмірній картинці, щоб зберегти ясність зображення. Таким чином, виникає сильне напруження в очах, потім головна біль, запаморочення і нудота. Також, це явище називають «цифровою морською хворобою» [5].

Отже, в умовах сучасності, людина схильна до багатьох нових хвороб і залежностей, оскільки небезпека криється в зловживанні речей і технологій, що так щільно увійшли у її повсякденне життя. Багато вчених рекомендує проводити менше часу в соціальних мережах, не відволікати себе під час роботи телефоном та іншими речами [6]. Спілкуватися «в живу» та насичувати своє життя новими емоціями та подіями.

Список використаних джерел:

1. «New Scientist», № 3 (5), март 2011.
2. 15 болезней вызванных мобильными устройствами. - [Електронний ресурс].- Режим доступу: http://www.lookatme.ru/mag/live/inspiration-lists/199459-idiseases
3. Віртуальна бесіда: «Хвороби цивілізації». - [Електронний ресурс]. - Режим доступу: http://obriy.gdn/pg.php?cl=jUn6o_FejFg
4. Названы восемь новых психических недугов, которые атакуют человека благодаря интернету и гаджетам 17 октября 2013 в 12:44. - [Електронний ресурс]. Режим доступу: https://zn.ua/TECHNOLOGIES/nazvany-vosem-novyh-psihicheskih-nedugov-kotorye-atakuyut-cheloveka-blagodarya-internetu-i-gadzhetam-131068_.html
5. Селфицид. - [Електронный ресурс]. - Режим доступу: https://www.youtube.com/watch?v=o3yxUCUtlEg
6. 80 міжнародна наукова конференція молодих учених, аспірантів і студентів. 2014 рік. - [Електронний ресурс]. - Режим доступу: http://dspace.nuft.edu.ua/jspui/bitstream/123456789/17646/1/118.pdf

----------***----------

Нагорний О. С., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н, доцент.*

КІБЕРТЕРОРИЗМ ЯК НОВА ФОРМА ТЕРОРИЗМУ

Термін «кібертероризм» був введений старшим науковим співробітником американського Інституту безпеки і розвідки (Institute for Security and Intelligence) Беррі Колліном (Barry Collin) в середині 1980-го, для

позначення терористичних дій у віртуальному просторі. Термін відноситься до двох елементів: кіберпростору і тероризму.

Кіберпростір є «віртуальним світом», тобто інформаційним середовищем, яке функціонує за допомогою комп'ютерних систем.

Якщо об'єднати два ці формулювання, отримаємо дієве визначення. Під «кібертероризмом» слід розуміти умисну, політично вмотивовану атаку, на інформацію, яка обробляється комп'ютером, а також атаку на комп'ютерну систему і мережі. Ця діяльність створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту [1].

Кібертероризм - це залякування населення та органів державної влади, з метою досягнення злочинних намірів. Це проявляється в загрозі насильства, в підтримці стану постійного страху з метою досягнення чітких політичних, чи інших цілей, примусу до певних дій, привернути увагу до особистості кібертерориста або терористичної організації, учасником якої він є [1].

Сьогодні, кіберпростір активно мілітаризується і стає ареною військового протистояння між державами. При цьому, держави можуть використовувати спеціальні угруповання хакерів, щоб нашкодити противнику. Атаці можуть бути піддані об'єкти інженерної інфраструктури, атомні і гідроелектростанції та інші особливо важливі об'єкти. Крім того, жертвами кібершпіонажу стають, як державний сектор, так і приватні компанії з виробництва та надання послуг.

В Інтернеті з'являється більше сервісів, більше грошей, більше інформації. У той же самий час, кіберзлочинці теж еволюціонують - вони стають все більш професійними, все більш розумними і все більш жадібними. Якщо раніше питання безпеки в Інтернеті зводилися переважно до захисту особистої інформації і банківських даних, то тепер необхідно думати про

захист від несанкціонованого проникнення до цілих комп'ютерних систем і секретних баз даних.

Поряд із кібершахраями починають з'являтися незалежні групи зломщиків, які можуть завдавати значної шкоди не тільки заради фінансової вигоди, а й заради ідеї. Крім того, нових масштабів набуває кібершпіонаж, і не тільки промисловий. Масованим атакам вже не раз піддавалися не тільки комп'ютерні мережі урядів різних країн, але і корпорації, які займаються виробництвом зброї, атомних реакторів, ударних беспілотників.

Кібертерористи вважають метод використання кібернетичного нападу кращим через багато переваг: це набагато дешевший метод, ніж традиційний; цю діяльність дуже важко відстежити (не кажучи про затримання); вони зазвичай приховують свою особистість і місце розташування; немає ніяких фізичних бар'єрів для здійснення атак; вони здійснюють таку практику віддалено з будь-якої точки світу;вони мають здатність використовувати цей метод, щоб атакувати та вплинути на велику кількість цілей [2].

За даними різних аналітичних структур, загальні світові витрати, пов'язані з кіберзлочинністю, перевищують комбінований вплив на всесвітню економіку від торгівлі наркотиками. Кожну секунду з десяток чоловік стають жертвами якого-небудь кібершахрайства.

Злочини у сфері інформаційних технологій дуже часто є міжнародними, тобто, злочинці діють в одній державі, а їх жертви знаходяться в іншій державі. Тому, для боротьби з такими злочинами особливе значення має міжнародне співробітництво.

— Кібертероризм працює через чотири елементи:

— Хакерство: щоб отримати доступ до комп'ютерного файлу або мережі, незаконно або без дозволу;

— Дезінформація: щоб забезпечити неправдивою інформацією;

— Вірус: комп'ютерна програма, яка є шкідливою для нормального використання комп'ютера. Більшість вірусів працюють, приєднуючись до

іншої програми. Вони можуть стерти всі дані або просто нічого не робити, будучи неактивними до певного часу;

— Комп’ютерний хробак (Worm): шкідлива програма, яка розмножується, поки не заповнить весь простір зберігання на диску або в мережі [2].

Все це дозволяє говорити, що терористична діяльність переходить з реального простору в простір віртуальний. Інформаційні мережі допомагають терористичним угрупованням здійснювати задумані плани, які перетікають в кібертероризм, як в реальну загрозу діяльності для окремих країн і всього світового співтовариства [3].

Проблема кіберзлочинності та кібертероризму є відносно новою для міжнародного співтовариства. Саме тому, на даному етапі будь-які серйозні висновки про її стан і подальші перспективи зробити досить складно.

Зрозумілим є одне, що це явище, яке виникло лише кілька десятиліть тому, охоплює всі сфери діяльності людини, зростає швидкими темпами і вимагає прийняття адекватних і своєчасних заходів реагування, як на національному, так і на міжнародному рівні.

Він становить загрозу не тільки для України, але і для всього людства. Кібертероризм набагато страшніше, ніж холодна чи хімічна зброя. Кібертерорист здатний загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі. Очевидно, що жодна держава сьогодні не в змозі протистояти цьому злу самостійно. Боротьба з комп'ютерним тероризмом, як втім, і з тероризмом взагалі, не може бути справою окремо взятих держав, тому, необхідно забезпечити взаємодію спецслужб, включаючи національні служби безпеки і спеціальні підрозділи по боротьбі з тероризмом на національному, регіональному та міжнародному рівнях.

Оскільки, сучасний комп'ютерний тероризм являє собою суттєву загрозу, необхідно закріпити на законодавчому рівні обов'язок державних і

приватних структур стосовно прийняття технічних заходів, що забезпечують захист комп'ютерних мереж, як одного з найбільш вразливих елементів сучасного технологічно залежного суспільства.

Таким чином, можна констатувати, що загроза кібертероризму в даний час є дуже складною і актуальною проблемою, причому вона буде посилюватися у міру розвитку і поширення інформаційних технологій.

Список використаних джерел:

1. Владимир Голубев. Кибертерроризм как новая форма терроризма. - [Електронний ресурс]. - Режим доступу: http://www.crime-research.org/library/Gol_tem3.htm
2. Gabriel Weimann. Cyberterrorism How Real Is the Threat? -[Електронний ресурс]. - Режим доступу: https://www.usip.org/sites/default/files/sr119.pdf
3. Kevin Coleman. Cyber Terrorism. - [Електронний ресурс]. - Режим доступу: http://www.crime-research.org/library/Cyberterrorism

----------***----------

Вдовиченко Н., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

НАВІЮВАННЯ – СКЛАДОВА ТЕХНОЛОГІЇ МАНІПУЛЮВАННЯ СВІДОМІСТЮ

Навіювання – вплив однієї людини, або ж суспільства на стан психіки індивіда. Як правило, мова йде, про вплив на емоційну оцінку тих, чи інших подій, на прихильність до тих, чи інших поглядів [1, 2]. Механізми такого впливу на даному етапі розвитку суспільства вивчені недостатньо. Відомо, що людям властиво емоційно реагувати на хвилювання інших людей. Існує навіть специфічний термін – «емпатія», тобто здатність до співпереживання. Все це носить глибоке еволюційне коріння. Ні тварини, ні первісна людина не змогли б без цього вижити; допомога товариша чи партнера в більшості випадків є обов’язковою. Чарльз Дарвін спеціально вивчав вираження емоцій

у тварин. Виявилось, що вони можуть передавати свій емоційний стан через міміку та звукові сигнали: собаки скалять зуби, виляють хвостом і, як запевнює більшість, вміють посміхатися. Людина, разом з її розвинутим мовленнєвим апаратом, наділена великими можливостями впливу на інших людей, зокрема, на їх емоції та погляди.

Існує таке поняття, як приховані або ж пригнічені емоції. Звісно, цивілізована людина в більшості випадків має втримуватися від емоційного прояву, щоб не тиснути на оточуючих, використовуючи їхню здатність до емпатії. Проте, саме така категорія, на наш погляд, заслуговує найбільшої уваги. Зигмунд Фрейд вважав, що негативні емоційні переживання про які ми ладні забути не зникають зовсім, а проникають в підсвідомість, і можуть там знаходитись в прихованому стані. Саме ці пригнічені емоції можуть викликати дискомфорт і бути причиною хвороби. Для того, щоб вилікувати людину, варто знайти цю приховану емоцію, приховане хвилювання. Для усунення проблем із людиною варто поговорити з нею відкрито про таку проблему і намагатися викорінити її.

Вищий центр емоцій та мотивації розташований в проміжному мозку, у так званому гіпоталамусі. Він надсилає сигнали до кори головного мозку й сам відчуває цей регулятивний вплив з боку вищих нервових центрів. В цілому, нервова система здійснює вплив на протікання всіх процесів в організмі, включаючи травлення, дихання, роботу серця, заживання ран і так далі.

Навіювання, до того ж не лише зовнішнє, але й самонавіювання може здійснити серйозний вплив на фізичний стан людини. Кандидат психологічних наук Марія Кисельова із Центру серцево – судинної хірургії в Росії проводила дослідження за участю пацієнтів, котрих очікувала операція на серці. Їх запитували, як вони сприймали інформацію про їх майбутню операцію, і який у них настрій. З'ясовувалося, що у тих, у кого був позитивне налаштування на операцію і віра в те, що вона допоможе, - для них

післяопераційний період був значно успішнішим, причому не на 20-30%, а в кілька разів. Цікаво, що оптимізм у «успішних пацієнтів» поєднувався з розумінням серйозності загальної ситуації і складності майбутньої операції. Легковажне ставлення не приводило до позитивного результату. Відомо, що навіювання і позитивний настрій широко застосовуються психотерапевтами для лікування дуже багатьох хвороб. Безсумнівна і важлива роль навіювання у вихованні та навчанні.

Але є і навіювання іншого роду. Йдеться про, так зване, «маніпулювання свідомістю». Це, наприклад, настирлива реклама («телефонуйте прямо зараз»), вплив різних сект, які пригнічують природні людські емоції, і іноді прямо штовхають людей на злочини. Маніпуляція – це, перш за все, частина технології влади, що замінила в інформаційну епоху такі види влади, як насильство і примус. Вона не тільки спонукає людину, що знаходиться під таким впливом, робити те, чого бажають інші, вона примушує її хотіти це робити. Однією з основних умов успішної маніпуляції є той факт, що в сучасної людини в основному немає ні часу, ні бажання перевіряти правдивість повідомлень, які надходять через канали засобів масової комунікації. Як людина може протистояти таким впливам? Необхідно виховувати в собі звичку думати, критично ставитися до почутого, намагатися ознайомитися з іншого, альтернативною точкою зору і лише потім приймати рішення.

Використана література:

1. Почепцов Г.Г. Информационные войны. – М.: "Рефл-бук"; К.: "Ваклер", 2001. – 576 с.
2. Тоффлер Э. Третья волна. – М.: ООО "Фирма "Издательство АСТ", 1999. – 261 с.

----------***----------

Вінтоник Т. М., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

РОЗУМІННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА, ЯК СОЦІАЛЬНО-ПРАВОВОГО ЯВИЩА

З давніх-давен, люди тягнулися до інформації, шукали спосіб її передачі, навіть в доісторичні часи. Все починалося з вигуків, жестів, міміки; вже пізніше - криків. Недарма, існує 5 інформаційних революцій, які завжди розвивалися з розвитком самої цивілізації.

Реалії сьогодення такі: чим більше людина володіє інформацією, тим простіше їй жити на землі. В сучасних умовах розвитку інформаційного суспільства, не аби яке значення, має вміння індивіда управляти отриманою інформацією.

Відомо, що з початком минулого століття активно почали розвиватися інформаційні технології, але ніхто не міг подумати, що вже сьогодні, будь-хто зможе отримувати різноманітну інформацію, не виходячи з дому. В деякій мірі людство не встигає за розвитком технологій, так само, як законодавець не в змозі удосконалити законодавчу базу врегулювання даної категорії запитань.

Інформаційне суспільство є соціально-правовим явищем, адже оборот інформації здійснюється в соціумі, а отже, потребує регулювання з боку права.

По – перше, кожен з нас в повсякденному житті спілкуючись один з одним, чи переглядаючи інтернет-листи, зустрічається з інформацією, але ми не можемо бути впевнені, що дана інформація є достовірною і не загрожує вона іншим. Тому, держава повинна забезпечувати на правовому рівні, приймаючи законопроекти, про відповідальність за розголошення не правдивої інформації чи конфіденційної інформації.

По-друге, в ст.34 Конституції України говориться, що кожен має право збирати, зберігати, використовувати і поширювати інформацію в будь-який спосіб, але є певні обмеження, щодо інформації, яка загрожує державі. Виходячи з цього можна вважати, що оборот інформації дозволений законодавством.

По-третє, досить часто підписуючи документи, чи укладаючи договори, у нас вимагають персональні дані, зокрема: серію і номер паспорта, сімейний стан та інші. Деякі з цих даних являються конфіденційними, тому, на правовому рівні держава гарантує кожному нерозголошення вищезазначеного.

Виходячи с того, що інформаційне суспільство як соціально-правововое явище, де основним ресурсом виступає саме різноманітна інформація, рівень розвитку права повинен відповідати рівеню доступу до інформації.

----------***----------

Старовойтова А. В., *студент ФСП*
«КПІ» ім. Ігоря Сікорського.
Науковий керівник:
Петряєв С. Ю., *к.ю.н., доцент.*

СУЧАСНЕ «МИСТЕЦТВО» ЯК ТЕХНОЛОГІЯ ІНФОРМАЦІЙНОГО ВПЛИВУ НА СВІДОМІСТЬ

Мистецтво – одна з форм суспільної свідомості, вид людської діяльності, що відбиває дійсність у конкретно-чуттєвих образах, відповідно до певних естетичних ідеалів [1]. Тобто мистецтво формує в свідомості людей певні поняття і протягом тривалого часу встановлює стійкі стереотипи і шаблони.

З даного питання, варто звернути увагу на ідеї Бодіяра про культуру, як симуляцію, на проблеми, які розкриває його концепція. На думку автора, ми самі створюємо симулякри, яким властива повторюваність. Мистецтво вже не виділяється своєю оригінальністю і неповторністю, художні форми не є

новими, а лише варіюються та повторюються. Він стверджує, що мистецтва вже як такого не існує, існують симулякри, які спотворюють реальність. Ці симулякри не несуть ніякого духовного збагачення, не змушують милуватися, а лише є іміджами, методом заробітку і нав'язуванням думок, і позицій, які для когось є вигідними. Таким чином, мистецтво вже не відтворює реальність, як прояв творчості, мистецтво – помирає [2].

В Україні, а саме в Києві є центр сучасного мистецтва «Пінчук арт центр» (далі - ПАЦ.) відомий своєю неординарністю виставок. Так, у минулому році у Центрі проходила виставка львівської художниці Kinder Album, яка створила інсталяцію у вигляді кімнати з телевізором і кріслом навпроти, ліжком з двома матрацами, ванною, наповненою «кривавою» водою, та намальованими на стіні сперматозоїдами. За поясненням «художниці», цей набір є конструктором, яким художниця пропонувала скористатися глядачеві, щоб показати межі своєї інтимності. В додаток, в кімнаті був фотоапарат, на який відвідувачі могли сфотографуватися, та відправити фото на пошту автору інсталяції. В свою чергу, остання повинна була розмістити знімки на своєму сайті у Facebook.

Переглядаючи сайт художниці, ми натикаємось на фотографії наступного змісту: дівчина, що оголює груди; пара, що імітує статевий акт; геї, які лежать голими на дивані з книжками; трансгендер, що позує на краю ванни. А також, на екрані телевізора, який знаходиться у виставковій залі. Художниця пояснила, що в цьому вона не вбачає нічого дурного, а люди які зображені на фото розуміли, що ці світлини потраплять в інтернет, і додає, що більшість фото зроблені представниками секс-меншин, які таким чином, хочуть заявити про свої позиції в суспільстві. За словами художниці, вона зі Львова, де: «Церква тяжіє над суспільством, і всі ці стереотипи сильніше, ніж в решті України» [3].

Засохлі соплі на асфальті, або використаний презерватив у розібраного ліжка, дохла кішка в кімнаті або розчавлена собака на дорозі, - все це музейні

інсталяції сучасного "мистецтва". У переважній більшості музеїв Європи - відомих і не відомих, великих і малих, державних і приватних, обов'язково присутні виставки, так званого, сучасного "мистецтва".

Постає питання в тому чи є такого роду сучасне «мистецтво» корисним і пізнавальним, і чи містить воно в собі ті стереотипи та шаблони високої культури людини, які вироблялись століттями у суспільстві, і які відрізняють культуру від безкультур'я? Зміст такої продукції має скритий антигуманний та антигромадський характер, що призводить до порушення встановлених у цивілізованому суспільстві та закріплених, у міжнародному і вітчизняному праві морально-етичних, ідеологічних принципів, норм пристойності, а також шкодить моральному здоров'ю громадян.

На нашу думку, сучасне «мистецтво» важко віднести до мистецтва у традиційному своєму розумінні, скоріше це можна розглядати або як форму протесту, тоді воно повинне бути оцінено відповідними експертами у сфері етики і моралі, або як навмисне приниження честі і гідності людини, яке свідомо підтримує державна політика, що в свою чергу призведе до культурної руйнації суспільства, а потім самої держави.

У даному контексті варто згадати про теорію «Вікно Овертона», автором якої є американський інженер і політолог Джозеф Овертон. Політологи дотримуються думки, що дана теорія є небезпечною політичною технологією. Відповідно до цієї теорії, свідомість мас постійно в процесі обробки, відбувається зміна настроїв, смаків, моральних принципів - де ми є головними учасниками процесу, не усвідомлюючи цього [4].

В Законі України «Про культуру», в переліку основних засад державної політики у сфері культури є пункт : «визначення естетичного виховання дітей та юнацтва пріоритетом розвитку культури», виходячи з вищесказаного, виникає питання, чи виставки такого характеру є прикладом естетичного виховання, чи не суперечить це закону [5].

Треба звернути увагу на те, що вхід в ПАЦ є вільним, і ніяких вікових обмежень немає. Тобто, навіть школяр може відвідати цей мистецький центр і побачити такі аморальні виставки. На нашу думку, було б доречно на державно-правовому рівні закріпити обмеження на перегляд таких виставок дітьми молодше 16 років, і щоб це було не лише де-юре, але і де-факто.

Список використаних джерел:

1. Короткий енциклопедичний словник з культури. — К.: Україна, 2003. — ISBN 966-524-105-2.
2. Концепція Ж. Бодріяра: культура як симуляція. Теорія симулякрів Ж. Дельоза. - [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/1534122043872/kulturologiya/kontseptsiya_bodriyara_kultura_simulyatsiya_teoriya_simulyakriv_deloza
3. Художница Kinder Album: Из-за меня изменилась реальность PinchukArtCenter. - [Електронний ресурс]. – Режим доступу: http://life.pravda.com.ua/culture/2015/12/11/204617/
4. Окно Овертона: как это работает. – [Електронний ресурс]. – Режим доступу: http://russian7.ru/post/okno-overtona-kak-yeto-rabotaet/
5. Г.М. Красноступ. Основні напрями правового забезпечення державної інформаційної політики . - [Електронний ресурс]. – Режим доступу: доступу: http://old.minjust.gov.ua/30768

----------***----------

Пучинець А. М., *студент ФСП «КПІ» ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

ІНФОРМАЦІЙНЕ НАСИЛЬСТВО

Науково-технічний прогрес у сфері інформаційної діяльності призвів не лише до виникнення комп'ютерних мереж, які прискорили обмін інформацією, але й сприяв вдосконаленню небезпечних для людини технологій. Якщо ще вчора, задля впливу на людину, держава, правлячий клас або окремі особи використовували силу у вигляді матеріальної речі (зброя, отрута, інші засоби примусу тощо), то нині, вплив на волю людини

можливий без використання вогнепальної чи холодної зброї. Вплив на людину сьогодні можливий навіть на дистанційному рівні, без безпосереднього контакту. Такий вплив нині здійснюється за допомогою інформаційно-комунікативних мереж [1].

Залежно від сутності такого впливу, в теорії виділяють «маніпуляцію свідомістю» та «інформаційне насильство». Відмінність їх полягає в тому, що маніпуляція не пригнічує в повній мірі волю людини, людина сама приймає рішення, але здійснюється вплив на спрямованість її волі, її підштовхують до певного кроку. Інформаційне насильство – це насамперед пригнічення волі людини, з метою примушення її до певної дії.

Небезпека інформаційного насильства зумовлена тим, що основною зброєю такого впливу є інформація. Інформація, в свою чергу, є особливою формою буття, яка не належить ані до матерії, ані до енергії, проте вона впливає на людське буття, на події та явища, на стан матерії. Відповідно, інформаційне насильство чинить вплив на свідомість та на людину, на матеріальний світ навколо [3].

Якщо насильство звичайне полягає у впливі безпосередньому, тобто, наслідком є матеріальні та фізичні збитки, то у випадку з інформаційним насильством вплив чиниться перш за все на інтелектуальну та психологічну сфери та виявляється непомітно. Це може бути, наприклад, нав’язування спотвореної інформації. Яскравим прикладом може бути - обман, коли людині повідомляють недостовірну інформацію, не залишаючи при цьому можливості перевірити достовірність такої інформації.

Отже, визначимо наступні ознаки інформаційного насильства:

- По-перше, його нематеріальний характер. Інформаційне насильство здійснюється непомітно, не має матеріальної форми та є невидимим для особи;
- По-друге, особливий зв’язок між причинами та наслідками. Зв’язок між діями, що складають зміст насильства, та його наслідками, не є

прямим. Він може бути опосередкованим. В першу чергу інформаційне насильство спрямоване на інтелектуальну та психологічну сферу буття людини;

- По-третє, між інформаційним насильством та його наслідками може бути тривалий проміжок на часу, на відміну від звичайного насильства, наслідки якого є одразу;
- По-четверте, інформаційне насильство має віртуалізований характер та здійснюється за допомогою інформаційно-комп'ютерних мереж. Така форма впливу не потребує контакту між насильником та потенційною жертвою.

Важливою особливістю інформаційного насильство є його пандемічний характер. Інформація здатна до розмноження та поширення, так само, й інформаційне насильство може мати глобальний, масовий характер та поширюватись швидкими темпами [2, 3].

Отже, з урахуванням вищезазначених особливостей, ми можемо зробити висновок, про особливу небезпеку інформаційного насильства. Обман, спотворення інформація, кібербуллінг (дискримінація чи систематичне насильство з використанням комп'ютерних мереж по відношенню до людини) – все це є реаліями людського буття. Виникає питання: як запобігти інформаційному насильству?

Ця проблема стає особливо актуальною тим, що інформаційне насильство стає складовою тероризму та інформаційної війни. За допомогою різних засобів насильства певні суб'єкти чинять вплив на соціальні групи та окремих осіб, формуючи антисоціальні, терористичні установки, вербуючи людей та змушуючи їх працювати на інші держави чи певні організації.

Одним з найбільш поширених методів боротьби з таким явищем могла б бути цензура, однак, навіть вона тут не здатна бути якісним інструментом. Це зумовлено тим, що важливим середовищем для існування інформаційного насильства є Інтернет. Обмеження чи взагалі позбавлення доступу до нього є

порушенням прав людини. Отже, виникає дилема: права людини чи безпека. Обмеживши ресурси в одній країні, ми не вирішуємо саму проблему, оскільки вона є глобальною.

А тому, на нашу думку, світ має аналізувати ситуацію та шукати шляхи подолання такої проблеми. Ми вважаємо за необхідне, для посилення боротьби з інформаційним насильством перейти до створення системи колективної інформаційної безпеки. Важливим елементом на шляху подолання інформаційного насильство є виховна політика населення. Слід привчити людей до запобігання можливому впливу на них та відверненню інформаційного насильства.

Список використаних джерел:

1. Гусейнов А. А. Возможно ли моральное обоснование насилия? / А. А. Гусейнов // Вопр. философии. – 2004. – No 3. – С. 19–27.
2. Доценко Е. Л. Механизм межличностной манипуляции / Е. Л. Доценко // Вестн. МГУ. – 1993. – No 4. – Сер. 14, Психология. – С. 12–18.
3. Стаття д.ф.н., проф. Данильян О.Г., д.ф.н., проф. Дзьобань О.П.«ІНФОРМАЦІЙНЕ НАСИЛЬСТВО: СУТНІСНІ ПРОБЛЕМИ»

----------***----------

Кузьмич М. А., студент *ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В.М., *к.т.н., доцент.*

ІНФОРМАЦІЙНА НЕБЕЗПЕКА: КІБЕРБУЛЛІНГ

Динаміка розвитку інтернету рухається в дуже бистрому темпі, і цей темп важко контролювати. На користування мережею інтернет вікового цензу не встановлено, тобто, його споживають різні категорії людей від дітей до дорослих; інтернет несе собою інформацію, інформація несе собою позитивний або негативний вплив. Діти, на відміну від дорослих, не взмозі фільтрувати цю інформацію. Сьогодні, в Інтернеті вони проводять більшу

частину часу, ніж в реальному, а отже, це часто призводить до негативних наслідків.

Термін кібербуллінг походити від двох англійськіх слів: «кібер и буллінг». Кібер - означає віртуальне комп`ютерний середовище; «Bull» - означає бик, бугай, галасліва людина, в переносному значенні дуже сильна агресивна людина [1]. Кібербуллінг – це новітня форма агресії, яка передбачає собою напади з метою нанесення психологічної шкоди: насміхання, цькування, маніпулювання, через інформаційно-комунікаційні засоби, а саме: мобільний телефон, електронну пошту, соціальні мережі та інше.

Враховуючи наслідки кібербуллінгу, зі сторони держави та науковців не було приділено достатньо уваги поясненню даному терміну. А отже, приведемо приклад кібербуллінгу та його наслідки:

Так, «*у 2016 році 18 лютого, з дому пропала 15-річна киянка, яка разом із подругою була учасницею «груп смерті» у соціальних мережах. Дівчина мала виконати останнє завдання, а саме стрибнути з багатоповерхівки. Коли Нацполоіція Києва знайшла дівчину, вона була у безпорадному стані, і не могла пояснити для чого це робить*» [2].

Дана ситуація не поодинока у своєму роді, кібербуллінг активно почав набирати оборотів з 2000-х років.

Споживачі мережі інтернет і думки не припускають, що так званий інформаційний ресурс може вести за собою такі наслідки, адже, 97% учнів і 99% студентів користуються інтернетом, і мають можливість входити в інтернет-мережу з дому. Все відбувається дуже просто, тобі, спочатку, пише анонім зробити певну дію, а потім пише, що знає твою домашню адресу; споживач мережі впадає у паніку, адже, не розуміє, як анонім міг дізнатись його адресу? У відповідь, споживач виконує всі дії, які йому надсилаються. Найбільш доступні жертви – це діти віком від 10 – 17 років. Звісно, що жертва може звернутись за допомогою батьків, але належної допомоги не

буде надано тому, що батьки, вчителі, викладачі, психологи не можуть надати адекватну допомогу, вони не розуміють всю глибину проблеми, або не володіють знаннями, як цю проблему правильно вирішити.

Не отримавши допомогу, жертва впадає у відчай, і не знає, що робити - це призводить до пагубних наслідків (суїцид, травмування себе, або когось іншого, психічне захворювання).

На нашу думку можна зазначити три способи реагування на кібербуллінг:

1) активне роз`яснення значення кібербуллінгу в засобах масової інформації;

2) постійний догляд та спілкування за дитиною, цікавитись сайтами, на які вона заходить [3].

Онлайн-спілкування, відокремлене від батьків; батьки там взагалі відсутні, у віртуальному світі, де проводить їх дитина весь вільний час, і споживає різні додатки. Звісно, що відбирати телефон, планшет, комп`ютер і читати листування, переписки в чаті – не можна тому, що це порушує її права, саме тому треба живе спілкування. Коли батьки відкриті з дитиною, вона відкрита до батьків.

Важливо також звертати уваги на емоції дитини та враження після он-лайн режиму. Внаслідок кібербуллінгу: дитина виглядає засмученою, віддаляється від спілкування, що є ознакою нападу. Живе спілкування, сімейні традиції, обговорення проблем, дають змогу моніторингу стану дитини.

3*. Вирішення проблеми*

Якщо дитина показала повідомлення, де є присутнім кібербуллінг, необхідно зберігати спокій, не лякати дитину бурною реакцією. Все, що потрібно – це емоційна підтримка. Спокоєм можна показти дитині, що ця проблема не є суттєвою і її можна подолати. Ніякому разі не слід карати дитину, вона не є винна.

У таких випадках необхідно проговорити ситуацію, і визначити наступні кроки, які не повинні погіршити ситуацію. Репутація і рішучість батьків повинні надати дитині – безпеку. Коли ситуація розрядилась, необхідно довести до дитини наслідки кібербуллінгу.

Список використаних джерел:

1. Кібербулінг. - [Електронний ресурс]. – Режим доступу: https://uk.wiktionary.org/wiki/кібербулінг
2. «Сині кити» убивають дітей? - [Електронний ресурс]. – Режим доступу: https://vestnik.in.ua/2017/02/26/sini-kiti-ubivayut-di
3. Як уберегти дитину від Кібербулінгу. - [Електронний ресурс]. – Режим доступу: http://yakwiki.ru/molod/12484-jak-uberegti-ditinu-vid-kiberbulingu.html

----------***----------

Ісько Д. В., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Мисливий В. А., *д.ю.н., професор.*

СЕЛФОМАНІЯ І СУЇЦИД: КРИМІНАЛЬНИЙ СИМБІОЗ

У сучасному світі важко уявити людину без мобільного телефона чи інших засобів комунікації, користуючись якими, вона звикає до них настільки, що вже не може уявити себе без їх існування. При цьому, останнім часом ця залежність породила таке явище, як селфі. Се́лфі (від *англ.* self – сам) – це вид фотографії, автопортрет, зроблений за допомогою камери смартфону, фотоапарата чи веб-камери. Селфі називають одним з феноменів електронної сучасності, яке з'явилось на початку третього тисячоліття через поширення мобільних пристроїв з фотокамерами[1]. Широка популярність селфі пов'язана з тим, що таке фотографування самого себе дозволяє оперативне розміщення відзнятих матеріалів у соціальних мережах. І хоча, використання цих атрибутів сучасних комунікацій є ознакою технічного прогресу, воно породжує в суспільстві певні небезпеки.

Так, психологи стверджують, що селфі загрожує здоров'ю молодого покоління, оскільки, це захоплення відноситься до психологічних відхилень. Йдеться про «селфоманію», яка переходячи в залежність, призводить до витрат часу для «вдалих» зйомок, викладення зображень в соціальні мережі, очікування їх обговорення та позитивних коментарів. Відтак, увага особи фокусується на власній персоні і бажанні самовираження за рахунок оприлюднення свого чергового селфі. Не випадково Американська психіатрична асоціація офіційно визнала селфі психологічним розладом, оскільки на певній його стадії людині хочеться знімати себе цілодобово, і вона вже не контролює цей стан [2].

Проблема є тому, що вказана залежність настільки розконцентровує увагу людини, що вона стає нездатною сприймати оточуючий світ, а відтак, маніакальна тяга може привести до фатального результату. Для отримання яскравих знімків любителі селфі йдуть на неабиякі ризики: піднімаються на будівлі, башти, мости й інші висотні споруди, на дахи рухомого складу залізниць та метрополітену, фотографуються з небезпечними тваринами тощо.

Найбільш уразливою категорією селфоманів є підлітки, діти з несформованою психікою. У гонитві за ризиковими знімками вони вишукують різноманітні небезпечні декорації. Отже, очевидною є ситуація, що така модель поведінки молоді детермінована потребами визнання її існування у сучасному соціумі, бажанням виділятися в ньому, наражає життя на небезпеку.

Аналіз показує, що найбільш характерним у цьому відношенні є визначення такою особою своєї присутності в суспільстві з використанням ознак певної загальновідомої популярної особистості, визнаної у молодіжному середовищі. Іншою ознакою такої поведінки є підміна дійсної, повсякденної звичайної чи творчої праці іншим способом зростання, який замість суспільно корисної діяльності передбачає актуалізацію власної особи

через множину селфі. За спостереженнями у молодих людей часто вбачається порушення балансу сприйняття, між вигаданим та реальним, в оточуючому середовищі, і як наслідок – відсутність перевіреного досвідом почуття небезпеки.

Таким чином, на наш погляд, проблема селфоманії має розглядатися в рамках кримінологічної науки, оскільки зазначене поводження неповнолітніх, які стають жертвами своєї власної девіантної поведінки, утворює живильне середовище – так зване «фонове явище» для часто завуальованої злочинної поведінки її «модераторів».

У цьому контексті, йдеться про взаємозв'язок, симбіоз селфоманії та суїциду, коли підлітки, переймаючись соціальними мережами, приєднуються до певних угруповань, участь в яких може привести до загибелі, причиною якої може стати як нещасний випадок, так і протиправна поведінка. Зокрема, останнім часом злочинці, використовуючи соціальні мережі Інтернету, створюють так звані групи смерті та надсилають повідомлення, в яких найчастіше пропонують дітям нанести собі тілесні ушкодження або позбавити себе життя. Весь процес такого «спілкування» злочинця і жертви супроводжується відповідним документуванням у вигляді селфі.

Так, за інформацією правоохоронців на сьогодні близько 13 тисяч дітей в Україні віком від 12 до 16 років зареєструвались у соціальних групах «Синій кіт», «Тихий дім», «Розбуди мене в 4:20», учасників яких збуджують до самогубства[3]. Національною поліцією України за даними фактами порушено понад 35 кримінальних проваджень, за якими встановлено 4 факти суїциду та вдалося запобігти 10 самогубств підлітків [4].

Відомо, що ці суспільно-небезпечні діяння набувають транснаціонального масштабу й вже поширюються в країнах європейського та американського континентів, що спостерігається за запитами молоді в соціальних мережах, яка цікавиться правилами цих ігор. Така небезпечна криміногенна ситуація вимагає превентивних заходів, у тому числі, правових.

Проте, притягти до кримінальної відповідальності осіб, які із застосуванням мережі Інтернет використовують новий спосіб доведення жертви до самогубства, досить складно, оскільки, доведення до самогубства, передбачене у ст. 120 Кримінального кодексу України, не містить указаних дій, що спонукають потерпілих до самогубства чи замаху на нього.

Усе це актуалізує необхідність внесення до кримінального законодавства відповідних змін, спрямованих, на реагування кримінально-правовими засобами на виклики з боку злочинців, та вжиття кримінологічних заходів щодо запобігання вказаним суспільно небезпечним діянням.

У зв'язку з цим, вважаємо доцільним викласти диспозицію вказаної кримінально-правової норми у такій редакції:

«Стаття 120. Доведення до самогубства

1. Доведення особи до самогубства або до замаху на самогубство шляхом жорстокого з нею поводження, систематичного приниження її людської гідності, примусу до протиправних дій, шантажу, підкупу, обману, умовляння або іншого схиляння до вчинення самогубства;

2. Те саме діяння, вчинене щодо особи, яка перебувала в матеріальній або іншій залежності від винуватого, або щодо двох чи більше осіб;

3. Діяння, передбачене частинами першою або другою цієї статті, якщо воно було вчинене щодо неповнолітнього або з використанням соціальних мереж Інтернету.

Список використаних джерел:

1. Селфі. Вікіпедія. - [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D0%BB%D1%84%D1%96.
2. Ільченко Н. В. Селфі і ваша безпека / Н. В. Ільченко [Електронний ресурс]. – Режим доступу : http://nmc-kiev.org/367-selfi-i-vasha-bezpeka.
3. «Синий Кит». Минимум 13 тысяч подростков Украины сидят в «группах смерти» [Електронний ресурс]. – Режим доступу: http://hyser.com.ua/community/167019-167019.

4. Киберполиция выявила в соцсетях почти тысячу «групп смерти» [Електронний ресурс]. – Режим доступу: https://journalist.today/kiberpoliciya-vyyavila-v-socsetyax-pochti-tysyachu-grupp-smerti.

----------***----------

Панічик Л., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

REMIND MI LATER

Ви зайняті. Ви втомилися. Ви хочете зіграти в Pokémon Go або відкрити сторінку в інтернет-мережі вашої компанії. Причина не має значення. Клацаючи Remind me later (Нагадати пізніше) у вікні із запитом про встановлення оновлень, ви спрощуєте завдання для авторів програм-вимагачів.

Але, це лише один із шляхів проникнення таких програм в вашу систему. Зловмисники широко застосовують шкідливу рекламу, фішингові листи і навіть складні схеми на основі USB-накопичувачів. Розглянемо докладніше один з найпоширеніших сценаріїв.

Ви клацаєте **Remind Me Later**

Програмне забезпечення недосконале. Розробники регулярно виявляють помилки у власних програмах і випускають відповідні виправлення.

Відкладаючи оновлення плагінів і додатків, ви даєте зловмисникам можливість скористатися відомими даними. Приклад: в 80% випадків атака із застосуванням одного з відомих комплектів експлойтів виявлялася успішною, оскільки своєчасно не були усунені уразливості Flash. Будь то Flash, Silverlight або Google Chrome, необхідно регулярно встановлювати виправлення та оновлення.

Ваша система заражається

Опинившись на вашому пристрої, програма-вимагач бере під контроль відповідні системи. Потім, програма шифрує ваші файли за допомогою асиметричного алгоритму шифрування. Ваші дані зашифровані без вашої участі, при цьому, ключ до шифру є тільки у зловмисника. Деякі види програм-вимагачів поширюються по мережі самостійно. За даними експертів, здатність ПО-агресора до саморозповсюдженння зустрічається все частіше і частіше.

Відображається повідомлення з вимогою викупу

Після закінчення зараження, програма видасть повідомлення з вимогою виплатити викуп в біткоіни. Натомість, буде обіцяно відновлення доступу до даних. Як правило, сума викупу становить від 200 до 10 000 дол. США, проте в деяких випадках, компаніям доводилося втрачати набагато більші суми. Одна з каліфорнійських клінік виплатила 17 000 дол. США, щоб відновити доступ до даних. При цьому, кожну добу клініка втрачала близько 100 000 дол. США, оскільки, робота установи була частково паралізована.

Експерти з інформаційної безпеки не рекомендують платити викуп. Деякі програми-вимагачі не здатні коректно розблокувати файли. Іноді файли автоматично знищуються. За даними дослідницької групи Talos, кількість випадків з повним знищенням файлів поступово збільшується.

Мова йде про цілісність даних. Зловмисники не гарантують цілісності і коректного відновлення зашифрованих даних. Зокрема, спотворення медичних записів або проектної документації, може мати найсерйозніші наслідки.

Крім того, виплачуючи викуп, жертва фінансує діяльність злочинної організації. Прибутковість цих схем є стимулом до розробки нових, ще більш потужних видів програм-вимагачів.

Як захиститися від програм-вимагачів

З програмами-вимагачами найбільш ефективний багаторівневий підхід. Оборону можна зміцнити кількома простими способами. Спеціалісти

рекомендують звернутися до постачальника послуг аварійного відновлення, який допоможе зберегти працездатність організації в разі несприятливого розвитку подій. Однак, можна діяти і простіше: організуйте регулярне, резервне копіювання важливих даних. Встановіть засоби блокування реклами і обов'язково оновлюйте програмне забезпечення при появі відповідного запиту.

Скляр Н. В., *студент ФСП КПІ*
ім. Ігоря Сікорського.
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

ГАРАНТІЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ – ІНФОРМАЦІЙНЕ ЗАКОНОДАВСТВО

Правова система України належить до романо-германської, в якій законодавство виступає засобом регламентації важливих сфер суспільних відносин. Інформаційна сфера сьогодні є базовою для розвитку суспільства і держави в цілому. При цьому визначальним завданням держави стає забезпечення безпечних умов для розвитку суспільства і кожної людини окремо, що досягається збалансованою державною політикою, інформаційна частина якої має важливе значення в сучасних умовах. Не останнє місце в цьому аспекті займає інформаційне законодавство, формування якого є динамічним, але складним процесом.

Досягнення режиму законності в інформаційній сфері, який є правовим виміром інформаційної безпеки не є успішним на даний момент, тому що інформаційна сфера наповнена низкою нормативно-правових актів з неоднаковим змістом, число яких зростає, а це в свою чергу має наслідком неефективну їх реалізацію.

Дійсно, деякі рекомендації науковців стосовно нормативних проблем і шляхів їх вирішення в даній сфері були певним чином реалізовані з

прийняттям і вдосконаленням нормативно-правових актів, зокрема, законів України "Про доступ до публічної інформації", "Про інформацію" та ін., але окремі недоліки в даному питанні лише посилюються.

Аналізуючи чинне законодавство слід відмітити перелік проблем, які, на нашу думку, є досить масштабними, гострими та актуальними:

— термінологічні розбіжності, поняття і категорії однакові за формою та назвою мають різне тлумачення, що призводить до проблем при застосуванні на практиці, тобто їх розуміння є неоднозначним;

— відсутнє закріплення базових, фундаментальних дефініцій (зокрема, інформаційна безпека), значна кількість абстрактних, розмитих понять;

— значна кількість підзаконних нормативно-правових актів та законів у інформаційній сфері, що призводить до ускладненого процесу їх пошуку, аналізу та реалізації;

— прийняття підзаконних нормативно-правових актів та законів (що регулюють суспільні відносини, в яких інформація виступає об’єктом) з великою різницею у часі, що спричиняє неузгодженість понятійного апарату;

— існування розбіжностей в нормах, які викликають колізії в процесі їх реалізації, а також взагалі дублювання норм;

— неузгодженість та суперечливість нових правових актів в досліджуваній сфері з раніше прийнятими. Це призводить до правового хаосу;

— відсутність систематизованого спеціального інформаційного законодавства, що виступає правовим фундаментом в інформаційній сфері та забезпеченні інформаційної безпеки;

— недостатньо розроблена законодавча база щодо встановлення та притягнення до відповідальності у сфері забезпечення інформаційної безпеки;

— відсутність у сфері забезпечення інформаційної безпеки України законодавчого розмежування повноважень суб’єктів тощо.

Однозначно, сьогодні є необхідність удосконалення інформаційного законодавства України. Вважаємо, що воно повинно відбутися за трьома загальними умовними напрямами:

1. кодифікація нормативно-правових актів інформаційного законодавства;

2. дослідження та удосконалення норм законодавства, які закріплюють питання юридичної відповідальності за порушення в інформаційній сфері;

3. розробка та формування низки нормативно-правових актів, що будуть відображати цілісну модель державної політики стосовно забезпечення інформаційної безпеки (зокрема, розкрити зміст і закріпити поняття "інформаційна безпека", розкрити особливості об’єктів інформаційної безпеки, визначити суб’єктів забезпечення інформаційної безпеки та їх повноваження; створити міцне підґрунтя для формування відповідних актів, тобто стратегії, доктрини тощо).

----------***----------

Бесчасна А. Г., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

ПОСИЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ШЛЯХОМ ВДОСКОНАЛЕННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ

Розвиток інформаційного суспільства створює нові загрози інформаційній безпеці. Інформаційний захист реалізується через інформаційний вплив, як з розкриттям інформації, так і з її вилученням.

Розвиток Інтернет-технологій повинен спростити процес появлення, збереження, доступності й використання інформації, що потребує суспільство на етапі свого розвитку.

Однак, підготовка до цього потребує фінансових, мотиваційних (і певно, що це є головним) та політичних факторів. Одним із політичних і мотиваційних елементів прогресу є встановлення безвізового режиму. Так, це стало передумовою обов'язкового запуску Єдиного державного реєстру декларацій, що входить у сферу захисту особистої інформації, а також, до сфери протидії корупції. Введення такого реєстру в обов'язковому порядку, одночасно, розкриває персональні дані посадових осіб й виявляє інформацію, що може тягти й юридичну відповідальність за зловживання такими особами своїм положенням.

Якщо розглядати внутрішнє законодавство то, що повинно стати мотивацією у зміні чи доповненні до кодексів у частині захисту інформаційної безпеки? Так, діючий Кодекс про адміністративні правопорушення[1] відповідає на захист певних інформаційних правопорушень, проте не відповідає сьогоденню, оскільки, в ньому відсутнє регулювання відповідальності юридичних осіб в сфері інформації, не вказана відповідальність за порушення, які виникли у зв'язку з розвитком Інтернет-мережі.

На основі Господарського кодексу України [2] маємо: загрози пов'язані з недостатнім рівнем інформатизації в економічній сфері; викривлення інформації й несанкціонований доступ в галузях національної економіки; використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації, недостатній рівень розвитку національної інформаційної інфраструктури; прояви обмеження свободи слова та доступу громадян до інформації; комп'ютерна злочинність та комп'ютерний тероризм; спроби маніпулювання суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої

інформації. Автоматизовані інформаційні системи у господарській діяльності об’єднують в собі сукупність даних, обладнання, програмних засобів, персоналу, стандартних процедур, які призначені для автоматичного збору, обробки, розподілу, зберігання, представлення інформації згідно з вимогами пошуку і видачі інформації. Такими системами, наприклад, є Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, Єдиний ліцензійний реєстр, Державний реєстр речових прав на нерухоме майно та ін. [4]

Недосконаліть відповідальності за адміністративні й господарські правопорушення у сфері інформаційного захисту веде до того, що не несе превентивного характеру для захисту особистості, суспільства й держави від негативних наслідків інформаційного впливу.

Пріоритетами державної політики в інформаційній сфері на 2017 рік є:

1. забезпечення інформаційної безпеки;
2. забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію;
3. відкритість та прозорість держави перед громадянами;
4. формування позитивного міжнародного іміджу України. [3]

Доктрини інформаційної безпеки розроблені Міністерством інформаційної політики України на поточний рік і відповідають нагальним потребам суспільства в інформаційній безпеці, такі як, захист в інформаційній війні від держави-агресора, взаємодія органів державної влади, розвиток інформаційно-комунікаційних технологій та інформаційних ресурсів, захищеність державної таємниці та ін..

Отже, для створення ідеальної моделі захисту інформації й посилення відповідальності за порушення необхідно створити певні умови, наприклад:

1. Відповідність законодавства до міжнародних Конвенцій, договорів та ін., як термінології, так і основних засад, які зарекомендували себе в інших державах.

2. Повна систематизованість внутрішньодержавного законодавства, його чіткість, відсутність суперечностей та колізій.

3. Дотримання принципу рівності перед законом, визначення відповідальності фізичних та юридичних осіб у сфері адміністративної відповідальності в інформаційній сфері.

4. Протидія комп'ютерній злочинності та інформаційного тероризму, маніпулювання суспільною свідомістю й встановлення за невиконання більш жорсткої відповідальності.

5. Доступ громадян до інформації, що зробить безпечнішим їх життя. З розвитком новітніх технологій, повинен бути спрощений механізм появлення офіційної інформації в електронному вигляді для забезпечення прав людини, якщо це не суперечить іншим законам про державну таємницю, захист персональних даних, не порушує безпеку й ін. При цьому дотримуватись розмежування персональних даних за схемою законодавства більшості країн ЄС, де персональні дані класифікуються за критерієм «вразливості» на: а) дані загального характеру (П.І.Б., дата та місце народження, громадянство, стать, місце роботи, робочий телефон/факс/e-mail, місце проживання тощо); б) вразливі персональні дані, тобто дані, які за своєю природою можуть порушити основні свободи і таємницю приватного життя (до таких належать відомості про стан здоров'я, етнічну належність, релігійні погляди, політичні переконання, власність, заробітну плату та інші джерела доходу, ідентифікаційні коди, біометричні записи, реквізити документів та платіжних карток, номерні знаки транспортних засобів, дактилоскопічні відбитки, зразки почерку, записи голосу, фото- та відеоматеріали, кредитна історія, інформація про судимість і т. д.) [5, 6].

Список використаних джерел:

1. Кодекс України про адміністративні правопорушення від 07.12.1984. Електронний ресурс: http://zakon0.rada.gov.ua/laws/show/80731-10/print1477902429027612

2. Господарський кодекс України від 16.01.2003. Електронний ресурс: http://zakon2.rada.gov.ua/laws/show/436-15/print1459520943299793
3. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» Електронний ресурс: http://www.president.gov.ua/documents/472017-21374
4. Про державне підприємство "Інформаційний центр" Міністерства юстиції України : Постанова Кабінету Міністрів України від 14.07.99 р. № 1272.
5. Брижко В.М.. е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко та ін. – К.: НДЦПІ АПрН України, 2007 р. – 28 с.
6. Обуховська Т. І. Персональні дані: теорія та реальність / Т. І. Обуховська, В. П. Шуляк // Електронне урядування. - 2011. - №

----------***----------

Шахкалдієва Г. Е., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В.М., *к.т.н., доцент.*

ПРАВА ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

В сучасні часи, коли інформація вже стала інструментом повноцінної життєдіяльності глобального інформаційного суспільства, нажаль, одне з найперших місць посідає проблема реалізації одного із основних принципів в міжнародному праві – принципу поваги до прав і свобод людини. Створені людством новітні технології, за допомогою яких долаються економічні та політичні межі, пронизують всі сфери нашого життя та розширюють можливості, але одночасно і здатні створювати середовище та умови для порушення інформаційної безпеки, можуть сприяти деформації комунікативного простору та містити загрозу безпеці кожного з нас. Тому одним з основних пріоритетів будь-якої демократичної держави повинно бути дотримання рівноправ'я між інтересами особистості, суспільства і держави, виходячи при цьому з примату прав і свобод особистості.

Резолюцією 217 А (ІІІ) Генеральної Асамблеї ООН, 10 грудня 1948 року, основоположні права людини вперше проголошені на світовій арені, та закріплені у «Загальній декларації прав людини» від 10 грудня 1948 року [2]. Механізм забезпечення основоположних прав людини відображено в «Конвенції про захист прав людини і основоположних свобод», прийнятої членами Ради Європи від 4 листопада 1950 року. Дана Конвенція ратифікована 17 липня 1997 року Верховною Радою України, та набрала чинності 11 вересня 1997 року [3].

Конституція України [1], та окремі закони України відповідають положенням міжнародних Конвенцій, являють собою гарантії свободи слова та гарантії доступу до інформації для кожного громадянина (свобода публічних висловлювань; гарантії безперешкодного отримання повної та неупередженої інформації). Основний закон є нормативно-правовим підґрунтям для інформаційного законодавства України - ст.ст.3, 34-та, а також статті: 10, 15, 17, 23. 28, 29, 31, 32, 40, 50, 53, 54, 55, 57. Зокрема, стаття 3 Конституції України проголошує: “Людина, її життя і здоров’я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов’язком держави”.

В міжнародних актах, зокрема в Загальній декларації прав людини та Міжнародному пакті про громадянські і політичні права (Стаття 19), йдеться про дотримання свободи слова, дотримуються яких країни-учасниці ОБСЄ, а також і Україна. Стаття 19 Загальної декларації проголошує те, що “Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідей будь-якими засобами і незалежно від державних кордонів”. Це ж саме положення закріплене у

Міжнародному пакті про громадянські та політичні права. У Статті 10, Європейської конвенції про захист прав людини та основоположних свобод, передбачена свобода слова: “Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів.

Дані положення передбачають і покладання обов’язків, а саме - правоохоронного, який передбачає можливість реалізації прав, та правозахисного щодо захисту порушених прав, так, наприклад, обов’язок ліцензування діяльності на радіомовні, телевізійні та кінематографічні підприємства. Надані свободи, нерозривно пов’язані з обов’язками і відповідальністю, і виражаються в обмеженнях та санкціях, закріплених в законі, і є необхідними для розвитку демократичного суспільства, для забезпечення національної безпеки в цьому суспільстві, територіальної цілісності держави, громадської безпеки, для охорони здоров’я та життєдіяльності населення, захисту репутації окремих осіб, та запобігання розголошення конфіденційної інформації.

В представлених нормативно-правових актах правові засади регламентовані достатньо аби підтримувати гідний рівень розвитку суспільства, якого наразі в нашій країні недостатньо з багатьох причин. Але на шляху до досягнення упередження, уникнення «інформаційних деформацій» та відновлення бажаних для людини, суспільства та держави прав і свобод, а також сприятливих умов для виконання національних та міжнародних норм щодо дотримання інформаційних прав і свобод людини, - потрібно визнати на міжнародному рівні більш вдосконалений понятійно-категоріальний апарат, та імплементувати його в національне законодавство. Адже наразі постають такі важливі питання, що стосуються розвитку інформаційного суспільства, а саме - проблема відсутності визначеного чіткого розуміння на науковому, і на державному рівні які саме права мають

захищатись в межах інформаційної безпеки особи, і як похідне - суспільства вцілому. Ситуація ускладнюється невизначенням що таке «інформаційне суспільство», який рівень впливу інформаційно-комунікаційних технологій здійснюється на сферу життя людини, а також відсутністю у правовій площині загальноприйнятого, законодавчо закріпленого визначення «інформаційні права людини» та групи «інформаційних прав», що пов’язані із використанням інформаційно-комунікаційних технологій.

Походження терміну "інформаційне суспільство" зазвичай співвідноситься з Японією як головним конструктором локального технологічного розвитку. Цьому підтвердженням є доповідь Ю. Хаяші - професора Токійського технологічного інституту та звіти японського уряду. Деякі дослідники відзначають, що термін введено в науковий обіг на початку 60-х років Ф. Махлупом у США і Т.Умесао в Японії [5] .

Влучним вважаємо визначення про те, що справжнє «інформаційне суспільство» - це громадянське суспільство яке має можливість повністю реалізувати свої інформаційні права, суспільство з розвинутим інформаційним виробництвом і високим рівнем інформаційно-правової культури, в якому ефективність діяльності людей забезпечується розмаїттям послуг, заснованих на інтелектуальних інформаційних технологіях та технологіях зв’язку [6, с. 12].

Під інформаційними правами людини, як складової інформаційного суспільства, на нашу думку, слід вважати гарантовані та забезпечені державою можливості особи задовольнити її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для повноцінної життєдіяльності об’єму інформації.

Також, наприклад, за визначенням американської національної інформаційної інфраструктури, поняття «інформаційне суспільство» виступає як суспільство, в якому мають місце такі аспекти: 1) найкращі навчальні заклади, викладачі та курси стають доступними всім учням незалежно від

географічного розміщення, ресурсів і рівня працездатності, 2)величезний багаж знань з мистецтва, літератури і науки стає доступним не тільки організаціям, бібліотекам, музеям; 3) послуги охорони здоров'я та соціальні гарантії доступні в інтерактивному режимі кожному своєчасно і в необхідному місці; 4) у кожного з'являється шанс жити в будь-якому місці та без упущення можливостей повноцінної роботи в офісі через електронні мережі; 5)невеликі компанії можуть отримувати замовлення з усього світу через мережу Інтернет; 6) кожний може дивитися останні фільми, обслуговуватися в банку чи магазині зі свого помешкання; 7) коли кожен може отримувати державну інформацію прямо або через місцеві бібліотеки, легко вступати в контакти з державними службовцями; 8)державні, ділові структури можуть оперативніше обмінюватися інформацією електронним шляхом, знижуючи обсяг паперової роботи і поліпшуючи якість послуг [7].

Багатоманітність формулювання іноді по суті одних і тих же термінів породжує складність сприйняття, а інколи призводить і до колізій в правозастосуванні. Але якщо припустити, що навіть всі питання в даній галузі будуть на нормативному рівні визначені, то зі зростанням науково-технічного прогресу в світі завжди будуть з'являтися нові сфери суспільних відносин, де право ще не буде одразу все досконало врегульовувати, і тоді потрібно одразу працювати над визначенням понять на законодавчому рівні, та дотримуватись основоположних принципів міжнародного права, як основ підтримання законності.

Тому, коли країни з високим рівнем інформатизації вирішують сьогодні питання визначення норм поведінки у кіберпросторі, для нас, нажаль, на сьогодні потрібно якнайшвидше вирішувати питання захисту прав людини та дотримання законності в цій сфері.

З усього вище зазначеного можна вважати що, якщо буде відсутній розвиток реформування правової системи щодо інформаційного суспільства, то наша країна буде беззахисною перед країнами з високим рівнем

дотримання принципів прав і свобод людини, а це означає беззахисність вітчизняного суспільства перед злочинними посяганнями з боку інших суб'єктів інформаційних відносин.

Список використаних джерел:

1. Конституція України [Електронний ресурс] : закон України від 28. 06. 1996 р. № 254к/96-ВР із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду : за станом на 04. 02. 2011 р. № 2952-17. – Режим доступу : http://zakon1.rada.gov.ua .
2. Загальна декларація прав людини ООН. Документ 995_015, поточна редакція — прийняття від 10.12.1948 [Електронний ресурс] – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_015
3. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. Документ 995_004, чинний, поточна редакція — редакція від 01.06.2010, підстава 994_527 [Електронний ресурс] – Режим доступу : http://zakon5.rada.gov.ua/laws/show/995_004
4. Пилипчук В.Г. Актуальні проблеми становлення і розвитку правової науки в інформаційній сфері // Інформація і право. – № 1(4) – 2012. – С. 15-22
5. Иноземцев В. Современное постиндустриальное общество: природа, противоречия, перспективы. – М.: Логос, 2000. – 302 с.
6. Арістова Ірина Василівна. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: Дис... д-ра юрид. наук: 12.00.07 / Національний ун-т внутрішніх справ. - Х., 2002. - 476арк. - Бібліогр.: арк. 409-444
7. Мовсесян А.Г. Некоторые особенности экономики США на рубеже веков // США. Канада: Экономика, политика, культура. – 2001. – № 4. – С. 64-75.

----------***----------

Бесараба Л. О., *студент ФСП, КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Цирфа Г. О*., к.і.н., доцент.*

АВТОРСКОЕ ПРАВО И КОМЕРЧЕСКАЯ ТАЙНА В СФЕРЕ IT-ТЕХНОЛОГИЙ

С развитием технического прогресса и этапом становления, так называемого «информационного общества» (посредством принятия

множества законопроектов и внедрения специальных программ; на национальном и международном уровнях) все чаще возникают вопросы о регулировании авторского права и торговой тайны в сфере информационных технологий. Каждый автор или владелец уникальной технологии стремится защитить свое исключительное право, если таковое было нарушено. Но в современных реалиях, много кто сознательно нарушает *авторское право*, выдавая чужие идеи за свои (путем хитрости или под предлогом угроз) или раскрывая важные торговые тайны.

Ярким примером может послужить исковое заявление Британской конструкторской фирмы *BladeRoom Group* (далее - *BRG*)[1], специализирующейся на проектировании и строительстве дата-центров (англ. *data center*) к компании *Facebook* 23 марта 2015 года.

Суть обвинения состоит в том, что компанией *Facebook* был построен дата-центр в шведском Лулео, по дизайну разработанному *BRG*.

Британская компания акцентирует внимание не просто на воровстве торговых тайн, но и на полноценном нарушении авторских прав, потому, что *Facebook* выдала *документ BRG Methodology* (в публичном доступе, в рамках проекта *Open Compute Project*)[3] за свои идеи. Не было предпринято никаких попыток указать на заслуги *BRG* при разработке инновационного подхода в строительстве дата-центров. *Facebook* в свою очередь, было заявлено, что именно им был разработан данный подход.

BladeRoom Group утверждает, что помимо всего прочего, так же владеет интеллектуальными правами на помещения. А так же, и *сами дата-центры*.

BRG приводит доводы, что Facebook обманным путем заманила представителей BRG на переговоры по строительству будущего *data center*. Под предлогом возможного заключения контракта о будущем сотрудничестве, они обманным путем выведали у BRG торговые секреты и затем свернули переговоры, использовав полученную информацию о

модульных технологиях *BladeRoom*. В свою очередь, представители Facebook обращают внимание на то, что BRG не предприняла достаточно усилий для защиты своих технологий. Таким образом, выдачу этих секретов можно считать добровольным разглашением торговой тайны со стороны BRG.

Компания *BladeRoom Group* требует от Facebook возмещения ущерба за незаконное завладение торговыми секретами и нарушение авторских прав. Дело передано на рассмотрение окружному суду Северной Калифорнии. И согласно результатам предварительного слушанья: действия *Facebook* можно трактовать как нарушение закона о торговых секретах - *California Uniform Trade Secrets Act*[4].

Исходя из всего вышеизложенного, прежде всего, стоит поставить вопрос следующего характера: может ли дата-центр сам по себе быть объектом права интеллектуальной собственности? (По утверждениям *BladeRoom Group).* Или его стоит рассматривать с точки зрения совокупности авторских прав и торговых секретов?

Дата-центры *сами по себе не* являются объектом права интеллектуальной собственности, т.к. они представляют собой лишь скопище серверов, хранилище каких-либо данных (о составе которых сам владелец дата-центров часто даже не знает). Это одна из причин, по которой ответственность за запрещенный контент на серверах дата-центров, несет пользователь, который этот контент туда загрузил. Дата-центр всего лишь потенциально может хранить интеллектуальную собственность, но не является ею. Но *технология* строительства дата-центров является как авторским правом, так и торговой тайной.

На международном уровне отсутствует единый стандарт, который бы непосредственно регулировал деятельность дата-центров и определял их в качестве объекта права интеллектуальной собственности. Но есть определенные стандарты и требования на счет оформления помещений дата-центров, обеспечения качественного предоставления услуг. В США был

принят *ANSI/TIA-942 (Telecommunications Infrastructure Standard for Data Center)*[5], в котором есть перечень рекомендаций на счет размещения, строения и деления дата-центров за типами. *ANSI/TIA-942* фактически является единственным стандартом для дата-центров во всем мире. Однако, он давно не подвергался существенным изменениям и доработкам.

Вместе с тем, существует еще один стандарт, который был принят в 2010 году. *ANSI/BICSI 002-2011 (Data Center Design and Implementation Best Practices),* последующие изменения в который были внесены в 2011 году[6]. Данный стандарт определяет порядок обработки данных и внедрению новых технологий в дата-центрах.

В свою очередь аналогами *ANSI/TIA-942/EIA* являются и *EN 50173, EN 50174 (CENELEC*), *ISO 11801*, регулирующие уровни надежности в дата-центрах.

Опираясь на все вышеизложенное, можно сделать вывод, что упорядочивание деятельности дата-центров, принятие единого и более совершенного стандарта, дадут возможность избежать возникновения подобных споров в будущем. А так же позволит авторам, выработать более совершенный механизм защиты их авторского права и торговых тайн в сфере IT-технологий.

Список использованных источников:

1. Redacted version of document sought to be sealed. - [Електронний ресурс]. – Режим доступу: https://assets.documentcloud.org/documents/3462771/Bladeroomsuitfacebookservers.pdfLuleå goes live. - [Електронний ресурс]. – Режим доступу: https://www.facebook.com/notes/lule%25C3%25A5-data-center/lule%25C3%25A5-goes-live/474321655969861Take control of your technology future. - [Електронний ресурс]. – Режим доступу: http://opencompute.org/
2. UNIFORM TRADE SECRETS ACT WITH 1985 AMENDMENTS. - [Електронний ресурс]. – Режим доступу: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf

3. Telecommunications Infrastructure Telecommunications Infrastructure Standard for Data Centers Standard for Data Centers ANSI/TIA ANSI/TIA - 942 - [Електронний ресурс]. – Режим доступу: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf
4. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices Committee Approval: January 2011 First Published: March 2011 SAMPLE COPY – NOT FOR RESALE. - [Електронний ресурс]. – Режим доступу: https://www.bicsi.org/uploadedfiles/bicsi_002_sample.pdf

----------***----------

Гаврилюк А. С., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Цирфа Г. А., *к.і.н., доцент.*

ПРОБЛЕМИ ПРАВОВОЇ ОХОРОНИ КОМП'ЮТЕРНОЇ ПРОГРАМИ ЯК ОБ'ЄКТА ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Наше суспільство маленькими кроками рухається у майбутнє. Хто б міг подумати 50 років тому назад, що технології розвинуться до такого рівня. Люди в наш час не уявляють життя без «технологічних помічників». Вони супроводжують нас щодня, щохвилини, протягом всього життя.

Комп'ютерні програми стали популярними серед різних верств суспільства, таких як бізнесмени, підприємці, звичайні люди та навіть діти. З кожним роком наше суспільство все більше залежить від нових технологій, які полегшують наше життя. Практично, вони нам не є новизною, але на законодавчому рівні не всі відносини в інформаційній сфері врегульовані в повній мірі. Існує багато прогалин, зокрема у сфері інноваційних технологій.

Сьогодні Україна стоїть в одному кроці від вступу до Європейського Союзу, а тому питання охорони об'єктів інтелектуальної власності, а тим більше в інноваційних сферах є все більш актуальним.

У статті першій Закону України «Про авторське право і суміжні права» дається наступне позначення терміну : «комп'ютерна програма» - набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які

приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [1]. Це визначення має в собі складні терміни. Тяжко зрозуміти їх сенс без допомоги спеціаліста в цій сфері. Тобто воно є досить складним для правильного розуміння його не тільки звичайними людьми, а й судами, що створює певні перешкоди при вирішенні спорів.

Положення Бернської конвенції про охорону літературних і художніх творів, стаття 18 Закону «Про авторське право та суміжні права», пункт четвертий статті 433 Цивільного кодексу України визначають, що комп'ютерні програми прирівнюють до літературних творів.

На мою думку, законодавцю слід ретельно проаналізувати чи є комп'ютерна програма літературним твором, адже сам текст програми (вихідний код) не несе в собі змісту чи суті без використання комп'ютера. В порівнянні з літературним твором, будь-яка особа не зможе його сприйняти без технічної допомоги.

В зарубіжних країнах, зокрема в Америці, комп'ютерна програма захищається патентом. Однак в Україні на комп'ютерну програму патенту не видається, єдиним захистом даного об'єкта від неправомірного використання та привласнення є авторство. Як і в будь яких способах захисту, в даному є як переваги, так і недоліки. Перевагою є те, що авторство має дуже довгу тривалість, а саме 70 років після смерті автора(а також протягом всього його життя). Хоча через те, що технології достатньо швидко розвиваються в наш час, ця перевага не значна. Ще одна перевага авторства полягає в реєстрації об'єкта. Вона здійснюється тільки за бажанням автора. Ця процедура не є складною та обов'язковою.

Хоч законодавець намагається врегулювати дану сферу, в повній мірі це зробити не можливо. Злочинці та недобросовісні користувачі комп'ютерів

та Інтернету завжди знайдуть шлях видати авторську програму за свою, шляхом часткової зміни тексту коду.

Оскільки правом інтелектуальної власності передбачено захист форми, а не алгоритму, то трохи переробивши програму, суть залишається такою самою, а форма зміниться, тому на законодавчому рівні це зовсім нова комп'ютерна програма. Через це на просторах Інтернету неймовірна кількість однакових, або схожих програм. В цьому і є недолік авторства(як способу правового захисту).

Ще одною великою проблемою всього суспільства є піратство на просторах Інтернету. Проблема стоїть навіть не на національному, а на міжнародному рівні.

Піратство представляє собою незаконне та неліцензійне поширення різних комп'ютерних програм в мережі Інтернет. Купуючи за гроші ліцензійну версію програми, особа завантажує її на комп'ютер та в Інтернет. Гіршим є тільки те, що сам співробітник компанії, яка створює ці програми може вчинити подібні дії. Таким чином особа, яка завантажує з Інтернета програму, бере її безкоштовно, тим самим створює збитки автору.

Відповідно до спеціального звіту 301 *United States Trade Representative,* у 2016 році Україна стоїть на першому місці по піратству з країн усього світу. Як сумно це не звучить, але торговий представник США заявляє це не вперше.

Законодавця можна зрозуміти щодо прийняття законів, а саме в складності цієї діяльності, та військовим станом в країні. Але протягом декількох років наша держава не зробила ніяких, хоч найменших кроків до вирішення цієї проблеми. Наші закони тільки на стадії розробки, що обурює американців.

Для «закордонних піратів» Україна стала чудовим місцем для здійснення незаконної діяльності, тому за останні роки деякі сервери інших країн було перенесено саме на українські землі. Через те, що українці

поширюють в Інтернеті неліцензійні програми, їх виробники зазнають колосальних збитків.

На висновок можна сказати , що Україна скрізь стоїть на першому місці. Перше місце в світі по корупції, перше місце по піратству. Але ми ще молода держава. Україна потребує законодавчого врегулювання, вдосконалення законодавства, та нарешті створення нових законів.

Навіть встановлення авторства на комп'ютерну програму викликає безліч запитань.

Злочинці як були завжди, так завжди і будуть. З кожним століттям, з кожною новою сферою люди знайдуть спосіб обійти закон.

Найкращим варіантом вирішення проблем щодо права інтелектуальної власності є запозичення законодавства з інших, більш розвинених країн.

Список використаних джерел:

1. Про авторське право і суміжні права Верховна Рада України; Закон від 23.12.1993 № 3792-XII
2. Бернська конвенція про охорону літературних і художніх творів ВО інтелектуальної власності; Конвенція, Міжнародний документ від 24.07.1971
3. Цивільний кодекс України Верховна Рада України; , Закон, від 16.01.2003 № 435-IV
4. Сайт офісу United States Trade Representative. - [Електронний ресурс]. – Режим доступу: https://ustr.gov/

----------***----------

Тавберідзе І. Н., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Золотар О. О*., к.ю.н., с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.*

THE DARK WEB ЯК ПРОСТІР ДЛЯ СКОЄННЯ ЗЛОЧИНУ

The Dark Web – це прихована частина сайтів в Інтернеті, яка не індексується, тобто, не знаходиться, звичайними пошуковими системами та інтернет-браузерами [1]. Для доступу до неї використовують Tor Hidden Service Protocol, яка використовує власні сервери для серфінгу по Dark Web [2].

Для анонімного користування Dark Web потрібно використовувати проксі, тобто, непрямі запити через декілька інших серверів. Якщо не дотримуватись цієї умови, можливо стати як мінімум, об'єктом розіграшу, як максимум – особою, притягнутою до відповідальності.

І якщо внаслідок першого особі доведеться лише розрахуватись за піцу [2], то другий понесе за собою кримінальне розслідування. Як це пояснити?

Оскільки Dark Web – повністю анонімне середовище, це створює неабияку спокусу для розгортання злочинної діяльності без страху бути розсекреченим. Саме тому, в цьому пласті Інтернету існує багато пропозицій придбання наркотиків та зброї, перегляду забороненої порнографії, наприклад, дитячої, або актів насильства та навіть замовлення послуг кілера.

Авжеж, Dark Web складається не тільки з вищеперерахованого та його аналогів, а й звичайних, наприклад, форумів для людей, які бажають зберігати анонімність. Але не факт, що продивляючись теми, ви не знайдете щось на кшталт: «Чим зробити евтаназію, щоб не помітив патологоанатом?» або «Синтез ЛСД в домашніх умовах» [3].

Цей факт, у випадку деанонімізації, може призвести до того, що ви будете вважатися за особу, яка здійснює готування до певного злочину.

Наприклад, шукаєте зброю для вбивства. Або вже користуєтесь інформацією, щодо виготовлення наркотичних речовин. Навіть, якщо ви, зайшли у Dark Web через цікавість, а не злочинний умисел, сама сутність та можливості цього ресурсу дають підстави притягнути вас до відповідальності.

Прикладом злочинця у просторі Dark Web є Рос Ульбріхт, якого у 2015 році засудили до довічного позбавлення волі. Він був засновником «Silk Road» – найбільшої мережі по продажу та доставці наркотичних речовин від звичайного канабісу до героїну. Згідно даних прокуратури США, прибуток від продажу складав близько 214 мільйонів доларів США [4].

Не зважаючи на створення спецслужб США, таких як, наприклад, DARPA (Defence Advanced Research Projects Agency) [1], Ульбріхта було знайдено через його самовпевненість. Він залишив повідомлення на форумі спеціалістів по криптовалюті Dark Web – BitCoin – та прорекламував там свій драг-ресурс [5].

Таким чином, можна зробити висновок, що існування такого криміногенного та, що є дуже важливим, анонімного середовища, провокує маргінальних осіб до скоєння злочинів. Хотілося б сказати, що анонімність забезпечує лише відчуття безкарності, але, нажаль, судячи по тому, як рідко такі кіберзлочини розкриваються, вона дійсно скриває особистості злочинців і не дає притягнути їх до відповідної кримінальної відповідальності.

Список використаних джерел:

1. Порно, кокаин, убийцы. Что такое Deep Web и почему его лучше не открывать [Електронний ресурс] – Режим доступу: http://fakty.ictv.ua/ru/lifestyle/20170404-porno-kokayin-vbyvtsi-shho-take-deep-web-i-chomu-jogo-krashhe-ne-vidkryvaty/
2. Adrián Lamo What is the deep/dark web and how do you access it? [Електронний ресурс] – Режим доступу: https://www.quora.com/What-is-the-deep-dark-web-and-how-do-you-access-it
3. Что такое Deep Web и Dark Web [Електронний ресурс] – Режим доступу: http://answit.com/chto-takoe-deep-web-i-dark-web/#Dark_Web

4. Sam Thielman Silk Road operator Ross Ulbricht sentenced to life in prison [Електронний ресурс] – Режим доступу: https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced
5. Оружие, наркотики и копрофилия: как я провел выходные в тёмном интернете [Електронний ресурс] – Режим доступу: http://www.furfur.me/furfur/culture/culture/176811-dark-internet

----------***----------

Баранова В. О., Потапенко В. А.,
студенти ФСП КПІ ім. Ігоря Сікорського.
Науковий керівник:
***Золотар О. О**., к.ю.н., с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.*

ПІРАТСТВО ЯК ЗЛОЧИН У ГАЛУЗІ АВТОРСЬКОГО ПРАВА ТА СУМІЖНИХ ПРАВ: ПОГЛЯД НА ПРОБЛЕМУ

На сьогоднішній день, в Україні має місце високий рівень злочинності в галузі авторських та суміжних прав. Відповідно до Закону України «Про авторське право і суміжні права» [1] піратство у сфері авторського права – це 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), фонограм, відеограм і програм організацій мовлення.

Отже, суть інтернет-піратства полягає у відтворенні і розповсюдженні мережею Інтернет фільмів, музичних творів, комп'ютерних програм, іграшок, інших об’єктів інтелектуальної власності, без дозволу автора, або іншої особи, яка має авторське право, і/або суміжні права, або без виплати винагороди за використання творів у встановленому законом порядку.

В Україні рівень піратства досяг досить великих масштабів, боротьба з чим розпочалася лише після того, як у 2001 р. наша держава потрапила до списку «Special 301» і була змушена сплачувати суттєві штрафні санкції – 75 млн дол. щорічно. На зростання рівня піратства вплинуло:

- По-перше, це відсутність якісних сервісів з належним контентом, які б задовольняли культурні потреби українців;

- По-друге, нестабільність економічної ситуації в державі, що впливає на здатність громадян сплачувати досить високу ціну за ліцензійований перегляд фільмів та серіалів, тим паче, коли є можливість переглянути їх у вільному доступі.

В Україні відсутні законодавчі механізми врегулювання цієї проблеми. У процесі захисту авторських прав від Інтернет-піратства в порядку цивільного судочинства, виникають проблеми ще навіть на етапі подання позову до суду. Це обумовлюється тим, що найчастіше відповідач є невідомим, адже, у таких справах ним виступають власники веб-сайтів або ж провайдери, які здійснюють незаконне розміщення контенту на своїх сервісах. Також, проблему захисту авторських та суміжних прав ускладнює те, що при подачі позовної заяви необхідно мати інформацію про місцезнаходження відповідача, яке в більшості випадків є невідомим.

Отже, ми вважаємо слушною пропозицією на шляху боротьби з піратством створення Державного антипіратського бюро у сфері захисту авторських та суміжних прав, на яке будуть покладені наступні функції:

По-перше: здійснювати контроль за діяльністю власників веб-сайтів. Задля полегчення процесу подачі позову та прозорості вставити вимогу щодо зазначення власника сайту або ресурсу та його місцезнаходження.

По-друге: встановити санкції за порушення авторських та суміжних прав.

Так, наприклад, у Японії покарання за скачування нелегального контенту передбачає штраф у розмірі 25 тисяч доларів або ж ув’язнення терміном на два роки. Звичайно, для України такі заходи є вкрай радикальними, проте, на нашу думку, санкції всеодно мають бути встановлені. Для власників сайтів за розміщення на їх ресурсах піратського контенту – штраф 10 тисяч доларів. Для користувачів, які скачують

нелегальні файли – штраф 1000 грн. Але на сьогоднішній день звичайному українцю дуже важко розпізнати чи легальним сайтом він користується. Тож, Державне антипіратське бюро має створити Державний реєстр легально існуючих в країні сайтів. Відповідно до цього реєстру громадяни України мають відслідковувати якими сайтами вони користуються [3].

Отже, в умовах сьогодення інформаційна сфера потребує ефективного державного контролю і врегулювання. Ми вважаємо, що створення нового державного механізму стане ефективним засобом на шляху подолання проблеми піратства в Україні.

Список використаних джерел

1. Закон України «Про авторське право і суміжні права»: за станом на 9 травня 2011 р. / Верховна Рада України. – Офіц. вид. – К. : Парлам. вид-во, 1993.
2. Електронний ресурс. – Режим доступу : http://www.wired.com (офіційний сайт журналу «Wired»)
3. Електронний ресурс . – Режим доступу : http://www.crime-research.ru/library/Gorb6.htm (стаття Р. Горбенко «Компьютерное пиратство на Украине стало «культурным»)

----------***----------

Волкова В. І., Охота Г. О., *студенти ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Золотар О. О.*, к.ю.н., с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.*

ЦЕНЗУРА В УКРАЇНІ

Після здобуття незалежності Україною в законодавстві протягом 12 років чіткого визначення поняття цензури не було, проте після парламентських слухань «Проблеми інформаційної діяльності, свободи слова,

дотримання законності та стану інформаційної безпеки України» стало зрозумілим, що законодавцю необхідно чітко окреслити заборону цензури.

На сьогодні, стаття 15 Конституції України проголошує заборону цензури. Тож виникає питання, що ж являє собою це поняття? Відповідь слід шукати в статті 24 Закону України «Про інформацію», де сказано, що ***заборона цензури*** – це будь-яка вимога, спрямована, зокрема, до журналіста, засобу масової інформації, його засновника (співзасновника), видавця, керівника, розповсюджувача, узгоджувати інформацію до її поширення або накладення заборони чи перешкоджання в будь-якій іншій формі тиражуванню або поширенню інформації.

У сучасному світі під цензурою варто розуміти контроль влади за змістом та поширенням інформації, тобто мова йде про дії держави, що спрямовуються на встановлення певних обмежень інформації, яку дана держава вважає шкідливою та непотрібною.

Велика кількість науковців, які досліджували цю тему, виділяють два основних види цензури:

1) попередня цензура (полягає у створенні умов, при яких в державі ускладнена свобода преси та ведення бізнесу в інформаційній сфері);

2) наслідкова цензура (виражається у формі тиску, що виникає як наслідок появи того чи іншого матеріалу).

У першу чергу цензура стосується не тільки друкованих ЗМІ, а й телерадіоорганізацій, і більше того, має відношення до інформації, поширеної інформагентствами.

В Україні спостерігаються наступні тенденції цензури:

- замовчування інформації;
- маніпулювання інформацією за рахунок недотримання балансу думок та не відокремлення фактів від коментарів та оцінок;
- перешкоджання поширенню інформації.

Яскравим прикладом цього явища виступила нещодавна заборона на використання російських ресурсів (Вконтакті, Однокласники, 1С, Doctor Web та інші). Проте, на наш погляд, досягнути мети заборони такого виду цензури досить важко. Адже, по-перше, пропагандисти у будь-якому випадку знайдуть інші способи впливу на свідомість українців. А, по-друге, цензура є небезпечним явищем через те, що, почавши з російських ресурсів, згодом можуть дістатись і до опозиційних українських.

Підсумовуючи усе вище сказане, ми вважаємо, здійснення контролю та дозування інформації є присутнім в будь-якій сучасній державі. Але, на нашу думку, слід закріпити юридичні акти, для того аби на свободу мас-медіа ніхто не зазіхав. А також вжити заходів для уникнення прямої чи прихованої, класичної чи трансформованої цензури щодо ЗМІ.

Отже, цензура – це спосіб управління інформаційним простором. І ця система вже практично створена в країні. Чи буде бажання у влади використовувати цю систему - питання риторичне.

Список використаних джерел:

1. Бойко В. Свобода слова і заготівля кормів / В. Бойко // Вітчизна. – 2003. - № 7/8. – С. 4-28
2. Закон України «Про інформацію» // Відомості Верховної Ради України (ВВР) 1992, №48, ст.650

----------***----------

Діденко Ю., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Золотар О. О., *к.ю.н., с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.*

ОСНОВНІ ІНДИКАТОРИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

Сьогодні створення інформаційного суспільства (ІС), поширення технологій в усі сфери діяльності людини, стали необхідним елементом подальшого розвитку і трансформації соціуму. Насамперед, ново відкриття у ІТ-сфері створюють основу добробуту людства, а перехід до інформаційного суспільства спонукає до виникнення нових суспільно-політичних відносин, можливостей для спілкування, бізнесу, управління.

Дивлячись на історію розвитку науки в нашій державі, можемо зазначити, що Україна у першій половині 50- х років 20 століття мала неабиякий потенціал до встановлення ІС: на її теренах було зібрано третій після Великобританії та США комп'ютер; створено під керівництвом С.Лебедєва і В.Глушкова школу кібернетики й обчислювальної техніки; засновано такі наукові напрями, як штучний інтелект, теорія самоорганізації, системний аналіз[1]. На жаль, в ході міграційних процесів країну залишила частина інтелектуального потенціалу, а населення перетворилося у дешеву робочу силу для більш розвинених країн світу.

Наразі розвиток інформаційного суспільства характеризують через ІКТ-індекси або, як їх ще називають, е-індекси: індикатори стану доступу до телекомунікаційної інфраструктури: доступ населення й суспільства до радіо, телефону, персональних комп'ютерів (ПК), Інтернету. Найвідомішими з них є індекс цифрової спроможності; індекс цифрового доступу; індекс мережевої готовності; індекс інформаційного суспільства[2]. За даними різноманітних ІКТ-індексів Україна займає з 60 по 70-ту рейтингову позицію серед інших

країн. Так, за індексом мережевої готовності у 2009 р. Україна посіла 62 місце (у попередньому році – 70), у 2016 – 64 (нижче Шрі-Ланки).

На території України поступово будується інформаційна інфраструктура: введено в експлуатацію міжнародні канали зв'язку, розвивається мобільний зв'язок (практично всі адміністративні центри України мають мобільне покриття, кількість абонентів та операторів продовжує стрімко зростати), збільшується кількість Інтернет-користувачів. Проте, можливість формування саме цивілізованого ІС спирається, в першу чергу, на зміну суспільної свідомості та існуючих стереотипів разом із введенням технологічних інновацій та розбудовою телекомунікаційних систем.

Індикаторами розвитку ІС можна назвати, також, мережу освітніх та наукових закладів та рівень комп'ютеризації в них, рівень якості мережного зв'язку, різноманітні бази даних, розвиток права інтелектуальної власності (патенти, ліцензії). З цього приводу, Європейський план дій стосовно переходу до інформаційного суспільства передбачає загальні застосування ІКТ в практичному житті: дистанційна освіта, послуги для бізнесу (відео-конференції, електронна пошта, е-бізнес тощо), автоматизоване управління транспортними засобами та послугами, онлайн-торгівля, посилення мережевого зв'язку між університетами, дослідницькими центрами та підприємствами.

Заважають розвитку ІС, по-перше, більш слабкі передумови розвитку інформаційного суспільства у регіонах України, не дивлячись на те, що існує людський потенціал, по-друге, законодавча база в країні сформована, але є затримка в реалізації на практиці, по-третє, існує потреба в зміцненні мережі освітніх та навчальних закладів із зміною пріоритетів навчання відповідно до укладених міжнародних угод у сфері інформаційного суспільства. Зберігається відставання в темпах впровадження ІТ в різні сфери, у

технологічному розвитку, у рівні безпеки та обороноздатності порівняно з розвиненими країнами.

Отже, для подальшого розвитку інформаційного суспільства в Україні необхідно розширити використання мережевих технологій та забезпечити вільний доступ до ІТ-послуг, підвищення ролі самої держави у реалізації передбачених програм розвитку інформаційного суспільства, інформованості осіб щодо впливу ІТ-галузі на економічний та інші потенціали країни, затвердження інформаційних технологій як основи національної безпеки.

Список використаної літератури:

1. Постанова Верховної Ради України від 01.12.05 №3175-IV «Про Рекомендації .парламентських слухань з питань розвитку інформаційного суспільства в Україні». Режим доступу: http://zakon2.rada.gov.ua/laws/show/3175-15?test=dCCMfOm7xBWMpd0EZixTRgXIHI4d.s80msh8Ie6
2. Постанова Кабінету Міністрів України від 28.11.2012 № 1134 «Про запровадження Національної системи індикаторів розвитку інформаційного суспільства». Режим доступу: http://zakon3.rada.gov.ua/laws/show/1134-2012-%D0%BF

----------***----------

Михайленко М. В., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Золотар О. О., *к.ю.н., с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.*

ІНФОРМАЦІЙНИЙ ВИБУХ

Обсяг інформації, яким оперує суспільство на певному етапі історії, завжди визначав рівень його розвитку. Було підраховано, що з початку нашої ери для подвоєння знань людству знадобилося 1500 років. Щодо другого подвоєння, воно відбулося через 250 років (до 1750 р.), третє – за 150 (до 1900 р.), четверте – за 50 років [1, с. 274]. Також, слід зазначити, що ситуація є

дуже динамічною і швидко змінюється. Так, ще декілька років тому фахівці були впевнені, що подвоєння знань відбувається з проміжком в 3-5 років, але на сьогодні вони стверджують, що знання як мінімум подвоюються, а може і потроюються щорічно. З огляду на наведені дані, якщо обсяги інформації будуть зростати в такій же прогресії до 2043 року, то кількість знань повинна збільшитися в мільйон разів. Це означатиме, що людство володітиме у 128 мільйонів разів більшою кількістю інформації ніж 2 тисячі років тому.

Частина дослідників таку аномальну швидкість збільшення кількості інформації називають «Інфомаційний вибух» і пояснюють її більш широким використанням, доступністю та складністю інформаційних технологій [2].

З огляду на вищесказане слід задатися питанням: «Чи здатне людство обробити всю цю інформацію і як таке стрімке зростання кількості інформації впливає на сучасну людину?». Вченими доведено, що людська психіка має певні обмеження. Мозок звичайної людини здатен сприймати і обробляти інформацію зі швидкістю 40 біт на секунду [3]. При такій швидкості поглинання інформації людина за життя може прочитати не більше трьох тисяч книг. А в літературі та науці випускаються мільйони книг і наукових статей. Деякі з них є бездарними чи неактуальними, але фактом є те, що усю цю інформацію опрацювати фізично неможливо, через що справді геніальні думки і ідеї можуть залишитися поза увагою.

На жаль, це не єдина проблема, яку спричиняє така кількість інформації. Наразі, кожен піддається впливу інформаційного перевантаження, але особливо до нього вразливі діти. Вчені Російської академії медичних наук дуже стурбовані станом учнів і, провівши дослідження, оприлюднили статистику, яка каже, що до школи приходить близько 20% дітей, які мають порушення психічного здоров’я межового характеру, в кінці 1 класу кількість таких дітей становить 60–70% [4; с. 87]. Слід зазначити, що погіршення стану психічного здоров’я спостерігається і у учнів середньої та старшої школи. Це спричинено невиправдано складними і широкими програмами навчання, які

змушують учнів шукати та опрацьовувати надвеликі обсяги інформації. Дорослі люди, хоч вони, і стійкіші, також страждають від перенавантаження інформацією. Так, внаслідок надзбудження нервової системи через певний час людина енергетично виснажується. Вітчизняна дослідниця О. Виговська зазначає, що у таких людей втрачаються комунікативні навички, творче мислення, концентрація уваги, а також спостерігаються порушення сну, виснаження, підвищена сприйнятливість до інфекційних захворювань [5, с. 50].

Одним із соціальних наслідків інформаційного вибуху є зростання психічних і психо-неврологічних захворювань. Цьому питанню приділяється увага з боку Всесвітньої організації здоров'я і на часі постало питання розробки «Концепції Загальнодержавної програми охорони психічного здоров'я в Україні на період до 2025 року». Зараз проект документа перебуває на громадському обговоренні і опрелюднений на веб-сайті Міністрества охорони здоров'я України, куди кожен фахівець і громадянин може надати свої зауваження і пропозиції.

Список використаних джерел:

1. Уилсон Р. А. Психология эволюции [Текст] / Р. А. Уилсон // Янус, 1999 / – Москва: Символ, 1999. – 320 с.
2. English Oxford Living Dictionaries [Електронний ресурс] – Режим доступу до ресурсу: https://en.oxforddictionaries.com/definition/information_explosion
3. Information explosion & product proliferation [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://blog.kissmetrics.com/information-explosion/?wide=1
4. Безруких М. М. Школьные факторы риска и здоровье детей [Текст] / М. Безруких // Педагогіка толерантності. – 1999. – № 3/4.
5. Виговська О. Професіоналізм учителя як гарант збереження його здоров'я [Текст] / О. Виговська // Директор школи, ліцею, гімназії : Науково-практичний журнал для керівників закладів освіти: Фахове видання з педагогічних та психологічних наук затверджено ВАК України з 2001р. - 2005. – 2005. – №2.

----------***----------

Моргун Г. В., с*тудент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Золотар О. О., *к.ю.н., с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.*

ВПЛИВ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА НА ЛЮДИНУ: ПОГЛЯД ЗСЕРЕДИНИ

Основним ресурсом в інформаційному суспільстві є інформація. Вона набуває соціального значення тільки за умови її ефективного сприйняття людським мозком. Крім очевидної і необхідної функції мозку стосовно управління людським організмом для забезпечення біологічного виживання, цей орган також допомагає особі вижити в соціальному розумінні. Маю на увазі те, що за допомогою напрацьованого способу мислення, розвитку своїх розумових здібностей, людина має змогу реалізувати себе і стати повноцінним, унікальним та корисним членом суспільства, зокрема, інформаційного. Коли мова йде про вплив суспільства на людину, розпочинати перш за все потрібно із неї самої. Отже, дамо відповідь на першочергове питання: «яким чином особа сприймає та аналізує інформацію?», а вже потім з'ясуємо «як інформаційне суспільство і процеси, що відбуваються у ньому впливають на його членів?». Людина отримує інформацію із зовнішнього світу, обробляє та зберігає її за допомогою головного мозку, що складається з двох півкуль, кожна з яких виконує певну функцію. Олександр Лурія запропонував теорію, щодо якої умовно мозок людини можна поділити на три блоки. Перший блок регулює активність процесів, що відбуваються у свідомості людини; другий – виконує функцію прийому, обробки, за необхідності, переробки та збереження інформації, і останній блок – мислення, програмування, контроль поведінки на свідомому рівні. Діяльність головного мозку людини є фізіологічним, біохімічним явищем, а свідомість – її результатом. До речі, на сьогоднішній день, група

американських нейробіологів разом з Крістофом Кохом виявили, що свідомість породжує клауструм – це спеціальна речовина в мозку всіх ссавців, включно з людиною.

Двоїстість категорії інформаційне суспільство проявляється через її переваги і недоліки. Одним з його «побічних ефектів» є так званий інформаційний стрес - явище, що виникло віднедавна і вже встигло закріпитись і поширитись. Суть його полягає в неспроможності людини швидко робити вибір, приймати рішення та невідповідності фізичних і розумових можливостей людини інформаційним навантаженням. Особа, перебуваючи у стані інформаційного стресу, проходить три стадії – тривогу, опір та виснаження. Інформаційний стрес викликаний нестабільним емоційним станом, що в свою чергу спричиняється активацією у головному мозку людини сигналів у відповідь на збудник. Негативними наслідками перебування особи тривалий час в такому стані є погіршення загального стану здоров'я (проблеми з ШКТ на стадії тривоги), послаблення функціонування ЦНС та розвиток проблем з психікою. Оскільки потік інформації в сучасному суспільстві є безперервним і неконтрольованим, тобто містить значний обсяг неправдивої інформації, інформації маніпулятивного характеру, особа в силу неспроможності охопити і критично проаналізувати всю «вхідну інформацію», просто сприймає її, вважаючи що ці дані бути нею почуті та забуті. Однак це не зовсім так, адже вся отримана мозком інформація, яку особа вирішила не брати до уваги і в подальшому не використовувати надходить до підсвідомості і зберігається там незалежно від бажання самої людини. Таким чином, закладена у підсвідомість інформація впливає на хід думок особи, що призводить до стандартизації мислення людей у суспільстві, а як наслідок до втрати ними своєї ідентичності. Крім того, негативна інформація, що її отримує людина, як правило, викликає погіршення настрою, агресію і т.д. Однією з особливостей інформаційного суспільства є широке використання інформаційних технологій у всіх сферах

життя людини, тож більшість свого часу особа проводить під дією електромагнітних полів та в однаковому нерухомому положенні. Це призводить до проблем із серцево-судинною системою, ведення пасивного способу життя, а як наслідок появи зайвої ваги, уповільнення росту та розвитку у дітей та багато інших негативних впливів на здоров'я. Інформаційне суспільство розвивається швидкими темпами, і не за горами день, коли організм людини почне змінюватись, пристосовуючись до умов і темпів життя в соціумі. Зокрема, аналізуючи щоденні потреби і дії особи, можна сказати, що в людини майбутнього будуть більші очі, що викликано тривалим сидінням перед монітором і активною зоровою діяльністю, стануть більш витягнуті та довгі пальці, прилаштовані для швидшого і зручнішого набору тексту на клавіатурі, однак становити значну небезпеку може те, що наші нащадки матимуть менший мозок, не в значенні розміру, а в сенсі спрощення зв'язків між нейронами.

Список використаної літератури:

1. Бодров В. А. Інформаційний стрес: навчальний посібник для вузів. — М. 2000.
2. Лизь Н. А. Розвиток безпеки особистості: психолого-педагогічний підхід // Педагогіка. — 2006.
3. Аносов В. Д. Лепський В. Е. Вихідні посилки проблематики інформаційно-психологічної безпеки // Проблеми інформаційно-психологічної безпеки / під ред. А. В. Брушлинского, В. Є. Лепського. — М. 1996.
4. Електронний ресурс – режим доступу: http://dobryjlikar.com/article/201705/3419-nareshti-vcheni-diznalysya-mozku-zhyve-svidomist

----------***----------

Герасимчук А., с*тудент ФСП КПІ*
ім. Ігоря Сікорського.
Науковий керівник:
Фурашев В.М.*, к.т.н., доцент.*

КЕРУВАННЯ МОБІЛЬНИМИ ДАНИМИ У КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

Механізм керування даними, як такий, пропонує процедури по відновленню на випадок збою і, що більш важливо, - способи оптимізації виконання запитів. З іншого боку, мобільні обчислення – це галузь комп'ютерних наук, що пов'язана із мобільністю та має справу із апаратурою, програмним забезпеченням та комунікаційними системами. Керування мобільними даними знаходиться на перехресті цих галузей, а саме намагається вивчити дані, створені в мобільному світі.

Для розуміння всієї важливості цієї галузі варто усвідомити, що сьогодні мобільність – частина буденного життя. Ми носимо із собою смартфони чи мобільні телефони, оснащені сенсорами. Вони володіють могутніми процесорами, різними способами підключення і , що не менш важливо, надають нам доступ до обширного резервуару програмного забезпечення, котрий індивідуалізує досвід, що дозволяє нам вирішувати більш складні інтелектуальні завдання.

В області мобільних обчислень існують певні складності, які ми намагаємося вирішити за допомогою досліджень. Перша проблема - це великі дані. Так як смартфони і мобільні пристрої обладнані безліччю сенсорів, які постійно проводять величезну кількість інформації, існуюча інфраструктура не є готовою для адекватної обробки і аналізу цих даних своєчасно. Таким чином, складність тут полягає у виробленні розподілених і паралельних алгоритмів для аналізу цих даних без затримок. Друга проблема - це конфіденційність. Так як мобільні пристрої знаходяться в руках реальних власників, деякі програми можуть знати ваше місцезнаходження. Наприклад,

уявіть собі додаток, яке завжди знає, де ви знаходитесь. Складність тут полягає в розробці методів і алгоритмів, що надають нові можливості, але разом з тим дозволяють користувачеві контролювати кількість доступної третім особам інформації. Наступна проблема полягає в тому, що комп'ютери можуть дуже ефективно зберігати та обробляти дані, та все рівно вони відчувають труднощі з певними задачами, до прикладу, вирахування місця знаходження корабля на супутникових знімках. У зв'язку з цим користувачі смартфонів могли б надавати доступ до певної категорії інформації, покращуючи можливості комп'ютера. В такий спосіб вони будуть передавати складні задачі на виконання людям. Четверте питання – енергозбереження. В силу того, що дані пристрої обладнані джерелом енергії, то варто розробляти енергоефективні алгоритми, адже в іншому випадку такі програми не зможуть функціонувати.

Уявімо собі певний геометричний простір, де знаходяться точки. Ними можуть бути, до прикладу, точки розташування користувачів мобільної системи, результат роботи додатку по аналізу даних чи машинного навчання, послідовність ділянок ДНК в біоінформації. Даний метод називають «к» найближчих сусідів, що дозволяє визначити про яких саме сусідів йде мова, зв'язану з ними дистанцію завдяки якій можна буде порівняти проміжки між об'єктами із запита та рештою об'єктів системи. Розширення цієї ідеї іменується методом «к» всіх найближчих сусідів для кожної точки в даному геометричному просторі.

Існують деякі алгоритми, але вони працюють доволі повільно в таких ситуаціях, адже в них квадратична складність. Не дивлячись на те, що науковий осередок запропонував способи з використанням ітераційного занурення, де для кожної точки збільшується радіус пошуку, - ця задача все рівно залишається складною в силу того, що значно ростуть об'єми даних. У випадку із великими даними, на наш погляд, варто сегментувати задачу по знаходженню всіх «к» найближчих сусідів на кластер комп'ютерів.

В майбутньому варто вивчити більш детально випадок високої просторової розмірності. Добре відомо, що при розгляді багатовимірних задач виникає «прокляття розмірності»: методи, що працюють в низьких розмірностях, не працюють досить добре при збільшенні кількості вимірювань. Іншою важливою частиною подальшої роботи є спроба просунутися від фундаментальних досліджень, від формулювання завдання до розробки алгоритмів і реалізації реальних систем. Ідея в тому, щоб розробити соціальну мережу, в якій люди могли б зв'язатися з найближчими, що знаходяться поруч користувачами. Наприклад, якщо людині потрібна допомога, то він міг би миттєво оповістити найближчих користувачів.

----------***----------

Мишаста Т. Ю., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М., *к.т.н., доцент.*

КІБЕРЗЛОЧИН ЯК ОДИН ІЗ НАЙНЕБЕЗПЕЧНІШИХ ВИДІВ ЗЛОЧИНІВ

Живучі в сучасних умовах, мабуть, кожен із нас вже не уявляє свого існування без інформаційно –комунікаційних технологій, в підґрунті яких лежить широке використання комп’ютерної техніки та новітніх засобів комунікацій. Глобальна комп’ютеризація, стрімкий та інтенсивний розвиток цифрових технологій, які максимально спрощують людині всі технологічні та виробничі процеси, полегшили її існування та вкрай змінили уявлення про роботу, кар’єру, дозвілля, спосіб спілкування, фінанси і навіть особисте життя, але ніхто не зважає на те, що за такою перспективою приховується новий вид злочинності, як кіберзлочинність, що несе за собою серйозну небезпеку та невідворотні наслідки. Наслідки цієї злочинної діяльності стосуються не тільки інтересів окремих осіб, що стали жертвами, але й

великих компаній, підприємств, організацій і суспільства в цілому, також зростає рівень їх антисоціальної спрямованості.

Напевно кожен з нас вже чув про цей вид злочинності, а то й особисто зіштовхувався з нею. Науковці ж називають кіберзлочинність як сукупність злочинів, що вчинюються у так званому «віртуальному просторі» за допомогою комп'ютерних систем чи за допомогою використання комп'ютерних мереж та інших засобів доступу до віртуального простору, цей доступ є несанкціонованим. «Кібербезпека», «кіберзлочинність», «кібертероризм», «кіберполіція» «хакери», цими термінами вже давно нікого не поставиш в глухий кут. Проблеми та ускладнення запобігання злочинам у сфері використання комп'ютерної техніки, активно розглядається юристами-науковцями, не так швидко як хотілося б, але також розвивається практика законодавства, щодо встановлення норм, які б могли забезпечити безпеку громадян у користуванні комунікаціями.

Порівнюючи кіберзлочинність з іншими видами злочинності такими як: шахрайство, крадіжка, вбивство та ряд інших, вона є досить новою, але це не є показником її суспільної небезпечності. Такі властивості, як глобальність, трансграничність, анонімність користувачів, охоплення широкої аудиторії, дозволяють швидко та непомітно злочинцям скоювати нові злочини і залишатися при цьому безкарними.

Зважаючи на рівень небезпечності та швидкість розповсюдження цього виду злочину, вітчизняний законодавець вирішив не зволікати і не лишати без покарання злочинців, створивши новий Кримінальний кодекс України, де вперше передбачив самостійний розділ про ці злочини - розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж», вже близько двох раз положення цього розділу змінювалися і доповнювалися, а це свідчить про актуальність та серйозність цієї проблеми в Україні.

Широкого розголосу та масового обурення серед української спільноти

набрав нещодавній Указ Президента України Петра Порошенка, щодо заборони доступу до декількох найпопулярніших веб-сайтів, які належать російським компаніям. Серед них опинилися, російські соціальні мережі VK і «Однокласники», поштова служба Mail.ru і пошукова система «Яндекс», всі чотири входять в десятку найвідоміших сайтів в Україні, також під забороною опинився російський сайт кібербезпеки «Лабораторія Касперського», а також програмне забезпечення для багатьох бізнес компаній 1С. Президент цей указ пояснив тим, що Україна неодноразово зазнавала кібератак з боку Росії, тому таку санкцію вважає необхідною.

Я, як активний користувач, тепер вже заборонених онлайн-сервісів та медіа-платформ можу сказати, що свідомо розумію що таке рішення прийнято в інтересах національної інформаційної безпеки держави та громадян і захист національної безпеки є прерогативою українського уряду. Але з іншого боку ці аргументи не є достатніми. Адже встановлені заходи боротьби з кібератаками чи рядом інших загроз не повинні нести негативного впливу на фундаментальне право та на свободу вираження думки, на свободу доступу до публічної інформації. А це саме виглядає як пряма суперечка демократизму в державі. Такі заборони не відповідають ні принципу пропорційності, тобто відповідності між порушенням та покаранням, ні принципу свободи вираженню думок і свободи засобів масової інформації, це своєрідна атака на свободу інформації. Не може дати однозначної думки стосовно цього питання і європейська спільнота, одні говорять що це є прямим порушенням норм права, інші дають лише схвальні відгуки. Тому складно стверджувати , що буде далі з рішенням Президента і чи матиме воно не лише формальне , а й реальне застосування в державі, бо для реалізації як стверджують спеціалісти можуть знадобитися великі гроші і не мала кількість часу. І як стверджує представник уповноваженого Верховної Ради з прав людини Михайло Чаплига, що згідно українського законодавства блокування будь-яких інтернет-ресурсів можливе лише в судовому порядку.

Отже, хочу підсумувати. Інтернет-банкінг, купівля товарів через мережу, платіжні картки, онлайн знайомства і тому подібне вже давно для кожного з нас є невід'ємною частиною способу життя, але, на жаль, поряд з цим задоволенням знаходяться злочинці. Кіберзлочинці, які зі своїм знаряддям злочину, троянськими програмами, крадуть паролі та конфіденційну інформацію, яку надалі використовують для атаки своїх жертв. Кіберзлочинність – це вид новітньої злочинності, який виник і стрімко розвивається у зв'язку з приходом цифрової доби та впровадження інформаційно-комунікаційних технологій. Причиною прогресування кіберзлочинності як бізнесу, є його значна прибутковість, без особливого ризику. Тому на сьогодні для України і світу це є проблема номер один. Для того щоб не стати черговою жертвою потрібно бути дуже обережним, а державі готувати кваліфікованих спеціалістів, діяльність яких буде спрямована на противагу злочинців.

----------***----------

Мамед О. Ю., *студент ФСП КПІ ім. Ігоря Сікорського.*
Науковий керівник:
Фурашев В. М.*,к.т.н., доцент.*

ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ПРОБЛЕМАТИКА ТА ЗАГРОЗИ

Інформаційні технології та і взагалі інформація в цілому визначають розвиток суспільства все більше та обширніше. Стрімкий розвиток інформаційного суспільства впливає на багато сфер життєдіяльності людей, а саме: політичну, екологічну а також соціальну. Саме тому глобальна інформатизація суспільства охопила майже всі країни світу ні на сучасному етапі розвитку людства є провідним напрямком соціально-економічного а також науково-технічного розвитку. Інформаційна безпека є невід'ємною

частиною безпеки в цілому яка в свою чергу є наслідковим явищем яке виникло внаслідок глобальної інформатизації.

Доцільно буде розпочати з самого поняття інформаційної безпеки а вже далі давати характеристику її об'єктам. Беручи до уваги що це поняття розглядається з багатьох сторін, в цілому, інформаційна безпека — це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

До об'єктів інформаційної безпеки відносять : свідомість, психіку людей; суспільство; державу та управління.

Інформаційна безпека свідомості та психіки людей, а саме особистості, характеризується як визначений стан захищеності індивіда, особистості, різноманітних видів соціальних груп та об'єднань громадян від спектру впливів, котрі здатні проти їх волі мають можливість своїм впливом змінювати психологічні стани людини, змінювати її поведінку та перешкоджати свободі вибору та певним чином обмежувати її. Одним з джерел загроз, що атакують інформаційну безпеку особистості частина інформаційного середовища яка спотворює достовірну інформацію про оточуючий людину світ. За такого впливу людей поділяють за ступенем легкості до різноманітних способів впливу на них.

На суспільство, як об'єкт інформаційної безпеки, негативний вплив має втручання в особисте життя, право власності, дезінформація. В такій ситуації потужним захисником повинна бути держава, що забезпечує інформаційну безпеку такими заходами як: правильна оцінка інформації що надходить до інформаційного простору держави . В свою чергу особистість сама повинна оберігати себе від зайвої інформації та від інформації яка може на неї вплинути негативно. Одним із способів такого захисту є вміння зважено ділитися інформацію про себе та про особисте життя.

Відповідний рівень інформаційної безпеки забезпечений економічними, політичними також організаційними заходами що мають на меті попереднє виявлення та попередження а також нейтралізація обставин та наслідків, що можуть завдяки своєму впливу завдати певних збитків або ж протистояти реалізації права на вільний доступ до інформації та інших інформаційних прав суспільства.

Якщо говорити про інформаційну безпеку держави, як об'єкту такої безпеки, то це є станом певної захищеності від інформаційних операцій які мають негативний вплив на державні та національні інтереси. До таких можна віднести: зовнішня інформаційна агресія, інформаційний тероризм, незаконне отримання інформації, комп'ютерні злочини, тощо.

Провівши аналіз теоретичних матеріалів з даної на розгляд теми можна зробити наступні висновки.

По-перше, з впевненістю можна сказати про те що дійсно, в сучасному світі інформатизація світу впевнено рухається вперед і починає впливати на низку сфер діяльності людини та держави.

По-друге, глобалізація інформації як потреби людства переміщується вперед переважаючи навіть основні потреби людини.

Ці дві риси підкріплюються науково-технічним прогресом та прагнення людини до самореалізації в інформаційному просторі. Така діяльність людини впливає на політичну, економічну та науково-технічну сфери.

Не абияким чинником глобалізації є інтеграція державної діяльності та інформації до єдиної системи що знаходиться у доступному інформаційному просторі . До таких систем включається інформація щодо суспільного життя та навіть щодо державного управління.

Вплив інформатизації породжує інформаційну безпеку. Об'єктами інформаційної безпеки є: особистість, суспільство, держава.

Особистість, як об'єкт інформаційної безпеки характеризується як визначений стан захищеності індивіда, особистості, різноманітних видів

соціальних груп та об’єднань громадян від спектру впливів , котрі здатні проти їх волі мають можливість своїм впливом змінювати психологічні стани людини, змінювати її поведінку та перешкоджати свободі вибору та певним чином обмежувати її.

Суспільство, як об’єкт інформаційної безпеки має на увазі можливість суспільства реалізовувати сої конституційні права, а саме ті що безпосередньо пов’язані з безперешкодним одержанням, створенням, обробкою, збереженням та поширенням інформації та захищеність від шкідливого впливу через інформацію.

Якщо говорити про інформаційну безпеку держави, як об’єкту такої безпеки, то це є станом певної захищеності від інформаційних операцій які мають негативний вплив на державні та національні інтереси.

----------***----------