спонукає жертву відкрити вкладення. В наслідок чого комп'ютер жертви заражається шкідливою програмою, яка щороку збирає персональну інформацію і відправляє її зловмисникові.

Спам в електронній пошті.

В даний час електронна пошта є найпоширенішим каналом зв'язку між родичами, друзями і комерційними партнерами. Шахраї намагаються обдурити жертв усіма можливими засобами, щоб змусити їх зробити грошовий переказ. Найчастіше це неіснуючі благодійні фонди і волонтерські організації.

Соціальні мережі, спільноти-пастки.

Комп'ютерні та інформаційні технології принесли зручність для спільноти, дозволяючи людям з усіх верств суспільства і різних вікових груп отримувати інформацію з Інтернету і більш тісно взаємодіяти з друзями і родичами.

У той же час користувачами мережі все частіше стають діти і підлітки, які заводять нові знайомства з невідомими, знаючи їх тільки по сторінці в соціальних мережах.

Відповідно юні користувачі соціальних мереж, котрі вступають в різні спільноти не можуть знати достовірно, які цілі переслідує творець цієї групи, і до чого призведе тривале спілкування на даній сторінці. До вкрай негативних наслідків можна віднести спілкування підлітків в так званих «групах смерті».

Кібер злочину, пов'язані з онлайн-іграми.

Кібер злочини пов'язані з онлайн-іграми відносяться до таких кримінальних правопорушень як шахрайство. Покупець або Продавець не отримує будь-яких товарів або платежів після того, як оплата була проведена або товар був доставлений на інтернет-платформу.

Неправомірний доступ до комп'ютерної системи.

Злочин передбачає неправомірний доступ до комп'ютерної інформації, якщо це діяння спричинило знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі в цілому [2].

Інші види кібер злочинів.

Будь-яке інше правопорушення, в електронній сфері, вчинене за допомогою комп'ютерної системи або мережі, або проти них вважається кібер злочином.

Органи влади та представники комерційних фінансових установ регулярно звертаються до громадськості із закликами бути пильними і тим самим уникнути потенційних небезпек кібер злочинів.

Список використаних джерел:

1. On-line журнал «Правознавець» http://pravoved.in.ua/section-kodeks/134-yku/1147-031.html

Мирошниченко В.О.

доцент кафедри економічної та
інформаційної безпеки
Дніпропетровський державний
університет внутрішніх справ
кандидат технічних наук, доцент

НАЦІОНАЛЬНА ПОЛІТИКА В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформація є найціннішим глобальним ресурсом, бо економічний потенціал суспільства визначається у сучасному світі переважно за обсягом його інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Відтак, для розбудови потужної держави необхідно створити відкрите для всіх інформаційне суспільство; сприяти використанню інформації і знань для досягнення погоджених на міжнародному рівні цілей розвитку, зокрема тих, що містяться в Декларації тисячоліття ООН.

Одним із головних нормативних актів України у цій сфері є Закон «Про інформацію». Він закріплює право громадян України на інформацію, визначає правові основи інформаційної діяльності. Ґрунтуючись на Декларації про державний суверенітет України та акті проголошення незалежності, закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації [1, с. 1].

Закони України «Про телебачення і радіомовлення» та «Про інформацію» регулюють відносини, що виникають у сфері телевізійного та радіомовлення на території України, визначають правові, економічні, соціальні, організаційні умови їхнього функціонування, спрямовані на реалізацію свободи слова, прав громадян на отримання повної, достовірної та оперативної інформації, на відкрите й вільне обговорення суспільних питань [2]. Важливим для інформаційного простору є Закон «Про телекомунікації», який визначає повноваження держави щодо управління та регулювання діяльності в цій сфері, а також права, обов'язки й відповідальність фізичних і юридичних осіб, які надають або споживають телекомунікаційні послуги [3].

Однак сучасне інформаційне суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності, тощо [4, 5]. Враховуючи такі небезпечні тенденції світова спільнота здійснює кроки вирішення цієї проблеми. Так Google розширила на весь світ свою послугу фактчекінга - перевірки фактів на достовірність. Тепер в пошуковій видачі і новинному сервісі Google News перевірені факти або матеріали будуть відзначені спеціальним маркуванням. Матеріали в сервісі, які пройшли перевірку адміністраторами, будуть позначені як fact check. У пошуковій видачі під час спроби знайти якийсь факт поряд з посиланнями будуть з'являтися анотації від таких сайтів, як PolitiFact або Snopes, що спеціалізуються на викритті фейків. У них буде повідомлятися, правдивий це факт, або помилковий.

Виданням, що публікуються в Google News, щоб отримати маркування fact check, необхідно використовувати спеціальні інструменти, які надають schema.org, Duke University Reporters Lab і Jigsaw. Також потрібно буде відповідати всім правилам Google News Publisher, призначеним для видавців.

Сьогодні проявом небезпечного характеру інформаційних технологій для України стало фактичне захоплення Росією інформаційного простору Криму, Сходу та Півдня України, що створило передумови для російської окупації АРК та організації збройного конфлікту в Донецькій і Луганській областях. Нині цілеспрямована діяльність Росії дає змогу провокувати напруженість і в інших регіонах, підтримувати антиукраїнські настрої серед власного населення, дискредитувати Україну та виправдовувати свою політику в державах – членах ЄС. Елементом реагування на цю проблему є створення загальнодержавної системи інформаційної (зокрема кібернетичної) безпеки України наступальної спрямованості як з питань захисту суверенітету, так і просування українських національних інтересів. В зв'язку з цим Укази Президента України від 15 березня 2016 року № 96/2016 та від 25 лютого 2017 року № 47/2017 є вкрай актуальними та своєчасними [6, 7]. Вони визначають національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері та передбачають:

– розробку й удосконалення нормативно-правової бази в сфері інформаційної безпеки, яка нині є фрагментарною та не повною мірою відповідає нагальним потребам;

– створення (визначення) керівного та координаційного органу системи інформаційної безпеки України в структурі державних органів виконавчої влади;

– визначення (уточнення) переліку суб'єктів, які відповідають за стан інформаційної безпеки;

– проведення досліджень та визначення потреб у технічному, фінансовому й кадровому забезпеченні функціонування системи; – активізація заходів у Міністерстві оборони та Генеральному штабі Збройних Сил України зі створення власної системи інформаційної безпеки як складової національної системи інформбезпеки.

До речі, в США, які беззаперечно є демократичною державою, саме Інтернет контролюється досить жорстко. Будь-хто, шукаючи в мережі інформацію негуманного характеру, ризикує потрапити під приціл спецслужб. Так виявляють педофілів, терористів, неофашистів й інших осіб із нестійкою психікою, що становлять потенційну небезпеку для суспільства.

Тим часом національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах:

– пріоритетності науково-технічного та інноваційного розвитку держави; формування необхідних для цього законодавчих і сприятливих економічних умов;

– всебічного розвитку загальнодоступної інформаційної інфраструктури, інформаційних ресурсів та забезпечення повсюдного доступу до телекомунікаційних послуг та інформаційних комп'ютерних технологій (ІКТ);

– сприяння збільшенню різноманітності та кількості електронних послуг, забезпеченню створення загальнодоступних електронних інформаційних ресурсів; поліпшення кадрового потенціалу;

– посилення мотивації щодо використання ІКТ; широкого впровадження ІКТ в науку, освіту, культуру, охорону здоров'я, охорону навколишнього середовища; забезпечення інформаційної безпеки.

Отже, з усього вищезазначеного можна зробити висновок, що інформаційні технології дуже глибоко ввійшли в наше життя, але задля досягнення інформаційної безпеки на державному рівні потрібні кваліфіковані кадри, які зможуть вирішити поставлені задачі по реалізації Доктрини інформаційної безпеки України.

Список використаних джерел:

1. Про інформацію: Закон України від 1 грудня 2002 року / Верховна Рада України. – Офіц. вид. – К.: Парлам. вид-во, 2002. – 24 с. – (Серія «Закони України»);
2. Про телебачення і радіомовлення: Закон Украї- ни від 12 вересня 2008 року / Верховна Рада України. – Офіц. вид. – К.: Парлам. вид-во, 2008. – 54 с. – (Серія «Закони України»);
3. Про телекомунікації: Закон України від 19 січ- ня 2007 року / Верховна Рада України. – К.: Парлам. вид-во, 2007. – 64 с. – (Серія «Закони України»);
4. Про захист суспільної моралі: Закон України від 20 листопада 2003 року/ Верховна Рада України. – Офіц. вид. – К.: Парлам. вид-во, 2003. – (Серія «Закони України»);
5. Інформаційна безпека суспільства / А. Суббот // Віче. - 2015. - № 8. - С. 29-31 . - Режим доступу: http://nbuv.gov.ua/UJRN/viche_2015_8_7;
6. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про Доктрину інформаційної безпеки України»;
7. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Михалок О.І.
здобувач вищої освіти, 5 курс, група С-ЮЗ-6113 факультету заочного навчання Дніпропетровського державного університету внутрішніх справ
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного