забезпеченою можливістю одержувати певні матеріальні блага за рахунок монопольного використання результатів інтелектуальної діяльності. Законодавства багатьох країн, крім майнових прав, наділяють творців також певними майновими пільгами. Така увага до творців нового зрозуміла, адже використання результатів інтелектуальної діяльності у значній, а може навіть вирішальній мірі, визначає рівень соціально-економічного прогресу [4, с. 64].

Для держави кінематографія – це стратегічний ресурс соціально-економічного, культурного, духовного та ідеологічного розвитку суспільства, забезпечення національних інтересів у середині країни та за її межами, зміцнення міжнародного авторитету й формування позитивного іміджу нашої держави, забезпечення інформаційної безпеки України та захисту української ідентичності [3].

Список використаних джерел:

1. Україна стала «безпечною гаванню» для інтернет-піратів [Електронний ресурс]. – Режим доступу: http://ipress.ua

2. Коваль А. Проблеми додаткової кваліфікації порушень авторського права і суміжних прав / А. Коваль // Юридична газета. – 2005. – № 15(51). – С. 18.

3. Проект: «Національна стратегія розвитку кіноіндустрії України на 2015–2020 роки» Державне агентство України з питань кіно – 2015 р.

4. Підопригора О.А Право інтелектуальної власності // О.А. Підопригора, О.Д. Святоцький. – К.: Видавничій Дім «Ін Юре», 2002. – 624 с.

5. Беззуб І Боротьба з інтернет-піратством в Україні: оцінки експертів [Електронний ресурс]. – Режим доступу: http://nbuviap.gov.ua

Савінкін М.Ю.

студент,
Начально-науковий інститут інформаційної безпеки України,
Національна академія Служби безпеки України

ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ – НАГАЛЬНА ПОТРЕБА УКРАЇНИ

Одним з найбільш актуальних питань для безпеки будь-якої держави є питання забезпечення інформаційної безпеки країни, зокрема, кібербезпеки. Україні заходи з протидії викликам і загрозам у зазначеній сфері знаходяться на початковому етапі та не мають комплексного характеру. При цьому, нормативно-правова база у сфері протидії злочинам в кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, які необхідні для ефективної протидії кіберзлочинам всіх рівнів складності.

Важливим кроком стало прийняття Стратегії національної безпеки України [1], яка поряд із загрозами інформаційної безпеки: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства визначила також загрози

кібербезпеки: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Крім того, зазначеним документом окреслено пріоритети для забезпечення кібербезпеки, зокрема: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого в Російській Федерації; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Останнім часом зростання кількості та потужності кібератак, вмотивованих інтересами окремих держав, груп та осіб, обумовлюють виникнення нових загроз в національній та міжнародній безпеці. Все більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет [2]. Слід зазначити, що деякі загрози, пов'язані з використанням сучасних інформаційно-комунікаційних технологій можуть мати значно більш широкі та більш комплексні наслідки для об'єктів атаки (тобто виходити далеко за межі конкретної цілі атаки) [3]. Більш того, особливістю сучасних кіберзагроз є їх подальша інтеграція із суто гуманітарними аспектами безпеки (вплив на громадську думку, залякування населення тощо), що відповідно потребуватиме внесення суттєвих змін до чинного законодавства, зокрема до Кримінального кодексу України.

Розвиток та безпека кіберпростору, створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави визначено, як головна мета Стратегії кібербезпеки України [4].

Разом з тим, сьогодні, фахівці виділяють три основні проблеми, які тісно пов'язані між собою, і як наслідок ускладнюють боротьбу проти злочинів у кіберсфері [5]:

1) відсутність чітких визначень таких ключових термінів як: «кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», «кіберінфраструктура», «критична кіберінфраструктура», що можуть ефективно застосовуватись в практиці правоохоронної діяльності;

2) не сформованість у повній мірі та відсутність систематизованості чинного нормативно-правового поля;

3) відсутність Єдиної загальнодержавної системи протидії кіберзлочинності із відповідним нормативним забезпеченням відповідних установ (боротьба із кіберзлочинністю та протидії кіберзлочинам залишається організаційно розпорошеною).

Щодо розв'язання першої проблеми слід зазначити, що на сьогодні спостерігається вільне використання значної кількості термінів із префіксом «кібер» (та їх синонімів), що часто не узгоджені між собою. Враховуючи зазначене, підготовлено на повторне друге читання Верховною Радою України законопроект, розроблений за участю міжнародних експертів США, Канади та ЄС.

Законопроектом пропонується запровадити нову для національного законодавства термінологію, зокрема понять «кібернетична безпека (кібербезпека)» та «кібернетичний простір (кіберпростір)» та ряд інших пов'язаних термінів, визначення правових та організаційних засад державної політики у цій сфері, основних принципів і напрямів забезпечення кібербезпеки. Разом з тим, слід також відмітити наявність багатьох зауважень та слушних пропозицій до законопроекту профільних центральних органів влади та наукових установ які працюють у цій сфері [6].

Щодо розв'язання другої та третьої проблем, що тісно пов'язані між собою, слід зазначити, що спостерігається розпорошеність та велика кількість нормативно-правових актів різних рівнів, що прямо та/або опосередковано охоплюють проблеми забезпечення кібербезпеки України. Проте, відсутність затвердженої чіткої термінології, не систематизація та невпорядкованість нормативно-правового поля державними профільними центральними органами влади у цій сфері, відсутність на законодавчому рівні координації їх діяльності, правового унормування зон їх відповідальності, процедур взаємодії, стають нагальною проблемою в умовах сьогодення. Разом з тим зроблені відповідні кроки, зокрема, створено Національний координаційний центр кібербезпеки [7] на засіданні якого керівництвом визначені певні заходи, спільні дії та окреслено інформаційний обмін в режимі реального часу для суб'єктів забезпечення кібербезпеки під час виявлення кібератак і кіберінцидентів [8].

Підсумовуючи, можна зробити висновки, що:

1) незважаючи на широке використання в науковій, публіцистичній та офіційній літературі різних термінів із префіксом «кібер», термінологічне поле сфери кібербезпеки держави все ще залишається фрагментарним, що унеможливлює формування дієвих нормативно-правових документів із протидії кіберзагрозам;

2) незважаючи на наявність цілої низки чинних вітчизняних та міжнародних нормативно-правових актів щодо проблем забезпечення безпеки кіберпростору держави, вони вкрай розпорошені, не систематизовані та не охоплюють всього спектру сучасних загроз кібербезпеці держави;

3) єдина загальнодержавна система протидії кіберзлочинності із відповідним нормативним забезпеченням все ще знаходиться на шляху становлення та не працює в повну силу. Нагальною є проблема координації діяльності та правового унормування зон відповідальності та підзвітності відомств у цій сфері, процедур взаємодії та засобів комплексного як реагування

на самі загрози кібербезпеці держави, так і значної роботи із попередження таких злочинів.

Висновок: комплексне вирішення вищезазначених проблем надасть можливість створити якисне підгрунття для забезпечення інформаційної безпеки нашої країни, зокрема, кібербезпеки.

Список використаних джерел:

1. Указ Президента України від 26.05.2015 № 287/2015 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» – [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015.

2. Александра Ёлкина. 5 самых громких кибератак, приписываемых российским хакерам – [Електронний ресурс]. – Режим доступу: http://www.dw.com/ru/5-%D1%81%D0%B0%D0%BC%D1%8B%D1%85-%D0%B3%D1%80%D0%BE%D0%BC%D0%BA%D0%B8%D1%85-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA-%D0%BF%D1%80%D0%B8%D0%BF%D0%B8%D1%81%D1%8B%D0%B2%D0%B0%D0%B5%D0%BC%D1%8B%D1%85-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%BC-%D1%85%D0%B0%D0%BA%D0%B5%D1%80%D0%B0%D0%BC/a-19550145.

3. Информационное агентство «ЛІГАБізнесІнформ«. Президент Болгарии: Россия пытается расколоть Европу – [Електронний ресурс]. – Режим доступу: http://news.liga.net/news/world/13489205-prezident_bolgarii_rossiya_pytaetsya_raskolot_evropu_kiberatakami.htm.

4. Указ Президента України від 15.03.2016 № 96/20162 « Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» – [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/962016-19836

5. Аналітична записка Національного інституту стратегічних досліджень «Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування». – [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/454/

6. Текст проекта Закону про основні засади забезпечення кібербезпеки України, підготовлений до другого читання – [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126a&skl=9

7. Указ Президента України від 07.06.2016 № 242/2016 «Про Національний координаційний центр кібербезпеки» – [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/2422016-20141

8. Олександр Турчинов. «Протистояння в кіберпросторі є складовою гібридної війни» – [Електронний ресурс] – Режим доступу: http://ua.korrespondent.net/ukraine/3754515-turchynov-zaklykav-shvydko-reahuvaty-na-kiberzahrozy/