ЛОГІНОВА Н. І.

Національний університет «Одеська юридична академія»,
в. о. завідувача кафедри інформаційних технологій,
кандидат педагогічних наук, доцент

ПРАВОВІ ОСНОВИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Активне впровадження телекомунікаційних технологій во всі сфери життєдіяльності людини сприяє формуванню інформаційного суспільства, в якому основним товаром та об'єктами інформаційної безпеки є інформація та інформаційні ресурси. Останнім часом відбувається об'єднання реального та віртуального простору людини, виникає «кіберпростір».

Кіберпростір — це складне середовище, яке управляє взаємодією між людьми, програмним забезпечення, Інтернет-сервісів шляхом розподілених технологічних пристроїв і мережевих зв'язків інформаційно-комунікаційних технологій (ІКТ). Взаємодія грає найважливішу роль для забезпечення віртуального середовища [1].

Зміст кіберпростору є у взаємодії користувачів інформаційними ресурсами та ІКТ інфраструктурою.

Важливість введення в оборот терміну «кіберпростір» та його існування підтверджується створенням в багатьох країнах світу спеціальних структурних підрозділів, призначених для організації заходів, спрямованих на здійснення управлінського та деструктивного впливу на автоматизовані інформаційні системи та захисту інформаційних ресурсів [2].

Відповідно, необхідно розробити нові підходи до інформаційної безпеки, виокремити напрям кібернетична безпека (кібербезпека) та організувати захист інформації та інформаційних ресурсів у кіберпросторі.

Інформаційна безпека — це стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах, організацій, держави. Основним об'єктом захисту є інформаційна система, яка реалізує автоматизований збір і обробку даних, та включає в себе: інформацію (інформаційні ресурси), матеріально-фінансові ресурси і людей (персонал), які мають санкціонований доступ до цих ресурсів. Захист будується на основі концептуальної моделі інформаційної безпеки [3].

Кібербезпека — це стан захищеності кіберпростору держави і окремих об'єктів його інфраструктури від ризику стороннього впливу, своєчасне виявлення та запобігання різних зовнішніх втручань через інформаційні системи та мережі, а також загрози національним і особистим інтересам. Об'єктами кібербезпеки є системи збору даних, органи управління та канали інтерактивної взаємодії.

Для забезпечення кібербезпеки потрібно створити комплекс організаційних, технічних та правових засобів захисту інформації в кіберпросторі, які будуть керувати користувачами інформаційних ресурсів, визначати існуючі загрози безпеки та прогнозувати нові загрози.

Щодо правових засобів, то протягом останніх років в Україні формується нормативно-правова база в сфері розбудови інформаційного суспільства, забезпечення інформаційної та кібернетичної безпеки. Серед основних законодавчих документів регулювання цих питань можна виокремити наступні: Закони України «Про інформацію», «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про ратифікацію Конвенції про кіберзлочинність», Укази Президента України «Про Доктрину інформаційної безпеки», «Стратегію національної безпеки», а також окремі постанови Кабінету Міністрів і рішення РНБО України.

У перерахованих законодавчих документах зустрічається термін «інформаційна безпека» та відображені вимоги щодо її забезпечення. Термін «кібербезпека» не визначається в національному законодавстві та став використовуватися лише протягом останніх кількох років.

У 2013 році був розроблений законопроект «Про внесення змін до Закону України «Про основи національної безпеки «України» щодо кібернетичної безпеки України», який спрямований на створення основ державної політики в сфері забезпечення кібербезпеки нашої країни [4].

16 березня 2016 року Президент України підписав Указ про введення в дію рішення РНБО України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [5], основна мета якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства та держави. У Стратегії виокремлені загрози кібербезпеки: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним умовам; недостатній рівень захищеності інформації та інформаційних ресурсів; безсистемність заходів кіберзахисту; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки. Але в даному документі не визначаються поняття «кібербезпека», «кіберпростір», «кібератака», «кіберзагроза» та інші, які вимагають осмислення та створення понятійного апарату в сучасних умовах формування інформаційного суспільства.

Отже, правові основи кібербезпеки закладені в національне законодавство України, але необхідно внести істотні зміни в існуючі нормативно-правові акти та розробити нові.

Список використаних джерел

1. Міжнародний стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity): [Електроний ресурс]. – Режим доступа: https://webstore.iec.ch/preview/info_isoiec27032 %7 Bed1.0 %7Den.pdf.
2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – С. 10.
3. Правовий захист інформації: навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса: Фенікс, 2015. – С. 32- 44.
4. Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України: Проект Закону України від 06.03.2013 р.: [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/1_doc2.nsf/link1/JG1WZ00I.html. – Назва з екрану.
5. Стратегія кібербезпеки України: Затверджено Указом Президента України від 15.03.2016 р. № 96/2016 // Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.

КОЗІН О. Б.

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат фізико-математичних наук, доцент

МЕХАНІЗМИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ В МЕРЕЖІ ІНТЕРНЕТ

Сьогоднішній день можна охарактеризувати постійним збільшенням ролі цифрової інформації у нашому житті. Кількість цієї інформації швидко зростає, її значення також відповідно зростає і збільшується необхідність її захисту. З розвитком Інтернету все більшої актуальності набуває проблема порушення авторських прав в Мережі. Дедалі актуальнішою проблемою постає забезпечення цілісності цифрової інформації, її захист та розробка механізмів, за допомогою яких можна захистити порушені права її авторів або її власників.

Через поганий захист та неприйняття запобіжних заходів, автори творів не можуть відслідкувати порушника та покарати його.

Відомо певне коло технічних механізмів захисту прав авторів цифрових даних, які використовують у світі. Технічні засоби захисту авторських прав цифрових даних можна розподілити на засоби обмеження доступу к цім даним, засоби їх ідентифікації, засоби криптографічних перетворень та інші. Деякі з засобів ідентифікації ми розглянемо окремо.