Козич І.В.

Доцент кафедри кримінального права Прикарпатського національного університету імені В.Стефаника, кандидат юридичних наук, доцент

Kozych I.V.

Associate Professor of Criminal Law Chair of Precarpathian National University named after V. Stefanik, PhD, Associate Professor

КРИМІНАЛЬНО-ПРАВОВІ ЗАСОБИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: ПИТАННЯ КЛАСИФІКАЦІЇ

У сучасному інформаційному суспільстві центральне місце займає державна інформаційна політика, яка покликана забезпечувати захист національних інтересів та інформаційну безпеку особистості, суспільства і держави. Державна інформаційна політика України як діяльність держави, спрямована на формування та регулювання середовища, в якому задовольняються інформаційно-комунікативні потреби громадян України, суспільства і держави, на сьогодні перебуває в стадії формування, пошуку і випробування нових методів, способів і технологій державного управління, ефективних в умовах сучасного інформаційного суспільства. Особливого значення в сучасних умовах набувають проблеми інформаційної безпеки.

Для створення передумов інформаційної безпеки України, в першу чергу слід забезпечити такий стан інформаційного суспільства, при якому не допускатимуться негативні впливи на неї з боку сторонніх суб'єктів. Ключовим у даній проблеми є визначення загроз інформаційній безпеці України.

У проекті Концепції інформаційної безпеки України від 8 червня 2015 року (надалі - Концепція) (проект відкритий для обговорення на сайті Міністерства інформаційної політики України) загрозами інформаційній безпеці визнаються наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері [1].

У статті 4 Концепції дається класифікація таких загроз інформаційній безпеці: «…забезпечення сталого розвитку інформаційного простору України з метою досягнення ним такого рівня, який завдяки своїм власти-

востям міг би протистояти **зовнішнім та внутрішнім загрозам**…» (виділено мною – І.К.).

Дещо по іншому визначаються загрози у ст. 8 Концепції: «Загрозами національній безпеці України в інформаційній сфері є: - **загрози комунікативного характеру** в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації; - **загрози технологічного характеру** в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору» (виділено мною – І.К.).

Якщо стосовно другої класифікації позиція авторів проекту є доволі зрозумілою (тим більше, що у ч.3 цієї ж статті проведено розширену класифікацію), то поділ загроз на внутрішні і зовнішні потребує деталізації, оскільки в подальшому з тексту Концепції не зрозуміло, які ж загрози слід вважати зовнішніми, а які внутрішніми.

На сьогоднішній момент цілий ряд загроз інформаційній безпеці отримують кримінально-правовий інструментарій для протидії їм. Тут слід враховувати, що окрім зовнішнього чи внутрішнього характеру загрози, важливий вплив на кримінально-правову норму має характер інформації, щодо якої здійснюється кримінально-правова охорона. Мова, в першу чергу, йде про вхідний чи вихідний характер інформації.

Типовими прикладами захисту вихідної інформації (інформація, яка є наявна у певного суб'єкта, і, власне, розповсюдження її назовні, серед інших суб'єктів, і становить загрозу) від зовнішніх та внутрішніх загроз інформаційній безпеці держави є:

- ст.111 - Державна зрада. Незрозумілим, правда, залишається питання про те, чому діяння, умисно вчинене на шкоду інформаційній безпеці, може вчинити тільки громадянин України. При цьому словосполучення «інформаційна безпека» вживається виключно у цій статті;

- ст.114 – Шпигунство;

- ст.ст. 328-330, 422, що стосуються виходу інформації з закритим чи обмеженим доступом;

ст. 238 - Приховування або перекручення відомостей про екологічний стан або захворюваність населення (специфічна вихідна інформація, яка не відповідає дійсності і тим самим становить загрозу).

Серед кримінально-правових засобів захисту вхідної інформації (інформація, яка знаходиться поза межами, ззовні, правового поля державної інформаційної політики; попадання такої інформації в інформа-

ційний простір і становить загрозу), що виникає внаслідок внутрішніх і зовнішніх загроз, можна виділити ч. 2 ст.109, ч. 1 ст. 110, ст.ст. 258-2, 295,436, ч. 2 ст.442 - різного роду публічні заклики до дій, що створюють або можуть створити реальну загрозу для держави, суспільства, особи. Окремим прикладом захисту вхідної інформації є ст. 436-1 - внаслідок специфіки предмета та об'єктивної сторони даного складу злочину.

Наведені приклади стосуються, в першу чергу, інформаційної безпеки держави. У законі про кримінальну відповідальність є й інструментарій і для захисту інформаційної безпеки фізичних та юридичних осіб. Є також цілий розділ щодо загроз технологічного характеру – мова йде про т.зв. комп'ютерні злочини.

Певний, хоча і не зовсім досконалий, інструментарій для потреб кримінально-правового забезпечення охорони інформаційного суспільства, як бачимо, є. Однак саме від законодавця, від концептуальної платформи інформаційної безпеки, зараз буде залежати можливість його реального використання в умовах інформаційної війни.

В цілому слід зазначити, що ефективне створення передумов для безпечного інформаційного суспільства залежить від чіткого розуміння зовнішніх і внутрішніх загроз, з врахуванням специфіки інформації, що є предметом певних відносин, суб'єктів, на які поширюється дана інформація, та наслідків. Подальший розвиток державної інформаційної політики повинен відбуватися у тісному взаємозв'язку з кримінально-правовою політикою.

1. *Proekt Kontseptsii informatsii bezpeky Ukrainy // Elektronnyi resurs / [Rezhym dostupu]: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf*

Козич І.В. Кримінально-правові засоби протидії загрозам інформаційній безпеці: питання класифікації

Державна інформаційна політика України як діяльність держави, спрямована на формування та регулювання середовища, в якому задовольняються інформаційно-комунікативні потреби громадян України, суспільства і держави, на сьогодні перебуває в стадії формування, пошуку і випробування нових методів, способів і технологій державного управління, ефективних в умовах сучасного інформаційного суспільства. Особливого значення в сучасних умовах набувають проблеми інформаційної безпеки.

Для створення передумов інформаційної безпеки України, в першу чергу слід забезпечити такий стан інформаційного суспільства, при якому не допускатимуться негативні впливи на неї з боку сторонніх суб'єктів. Ключовим у даній проблеми є визначення загроз інформаційній безпеці України.

Ефективне створення передумов для безпечного інформаційного суспільства залежить від чіткого розуміння зовнішніх і внутрішніх загроз. Подальший розвиток державної інформаційної політики повинен відбуватися у тісному взаємозв'язку з кримінально-правовою політикою.

Козыч И.В. Уголовно-правовые средства противодействия угрозам информационной безопасности: вопросы классификации

Государственная информационная политика Украины как деятельность государства, направленная на формирование и регулирование среды, в которой удовлетворяются информационно-коммуникативные потребности граждан Украины, общества и государства, в настоящее время находится в стадии формирования, поиска и испытания новых методов, способов и технологий государственного управления, эффективных в условиях современного информационного общества. Особое значение в современных условиях приобретают проблемы информационной безопасности.

Для создания предпосылок информационной безопасности Украины, в первую очередь следует обеспечить такое положение информационного общества, при котором не будут допускаться негативные воздействия на нее со стороны посторонних субъектов. Ключевым в данной проблемы является определение угроз информационной безопасности Украины.

Эффективное создание предпосылок для безопасного информационного общества зависит от четкого понимания внешних и внутренних угроз. Дальнейшее развитие государственной информационной политики должно происходить в тесной взаимосвязи с уголовно-правовой политики.

Kozych I.V. Criminal legal means to counter threats to information security: the classification

State Information Policy of Ukraine as a state activity, aimed the development and regulation of the environment in which catered information and communication needs of the citizens of Ukraine, society and the state, currently is in the stage of formation, search and testing of new methods, techniques and technology governance, effective in the modern information society. A problem of information security becomes particular importance in modern conditions.

To create the preconditions of Ukraine it should first be provided the status of the information society, which does not be allowed negative impact on it from outside entities. The key to this problem is to determine the threats to information security of Ukraine.

Effective creation of preconditions for safe information society depends on a clear understanding of internal and external threats. Further development of the state information policy should take place in close relationship with the criminal legal policy.