сподівається на запобігання їм, але його сподівання є легковажним, недостатньо обдуманим і свідчить про його необачність.

Протиправна необачність — це вид необережної вини, за якої особа, що вчинила адміністративне правопорушення, не передбачала настання шкідливих наслідків свого діяння, хоча повинна була та могла їх передбачати. Ця форма вини характеризується непередбаченням можливості настання суспільно шкідливого результату при обов'язковості та можливості такого передбачення.

Суть цієї форми вини полягає в тому, що особа, яка має реальну можливість передбачати шкідливі наслідки своїх діянь, не перетворює можливість запобігти цим наслідкам на дійсність, не напружує свій інтелектуальний або фізичний потенціал для вчинення вольових дій, які були б спрямовані на таке запобігання.

На відміну від усіх вищезазначених видів вини при вчиненні правопорушення з необачності особа-правопорушник не передбачає і шкідливих наслідків свого діяння. Таке непередбачення наслідків свого діяння свідчить про зневажання особою вимогами законодавства, своїми посадовими або громадськими обов'язками, інтересами суспільства в цілому або окремих його верств тощо.

Кібербезпека як новий виклик сучасності

Ключник Т.П. - студентка навчально-наукового інституту права та психології Національної академії внутрішніх справ

Науковий керівник: професор кафедри загально-правових дисциплін, навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, доцент - **Камінська Н.В.**

За останні 5-7 років глобальний кіберпростір усе більшою мірою розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів. Стає все очевиднішою і подальша мілітаризація кіберпростору.

Це визначило політичну необхідність контролю і подальшого регулювання взаємовідносин у цій царині та дало підстави стверджувати про особливу актуальність процесу створення надійної системи кібернетичної безпеки (стану захищеності кіберпростору держави в цілому або окремих об’єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам), відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони [1, 2].

В Україні ці механізми все ще знаходяться на етапах становлення. Деякі з них потребують вдосконалення, однак для розробки більшості та їхніх окремих елементів передусім бракує концептуального обґрунтування. Крім того, в Україні досі відсутні критично важливі елементи національної системи кібербезпеки. Відповідно, актуальність дослідження даної теми зумовлена необхідністю подолання суперечності між наявним станом стрімкого зростання важливості кібербезпекової проблематики та часткової готовності Української держави відповісти.

У європейському (а власне, і вже традиційному для світової спільноти) розумінні зміст поняття «інформаційна безпека» викладений в оновленій редакції Стратегії національної безпеки України «Україна у світі, що змінюється» [3], яка більшою мірою зосереджується на кібербезпеці та навіть артикулює завдання створення національної системи кібербезпеки.

Не можна сказати, що кібербезпека в Україні перебуває поза увагою інституцій безпекового сектору. Говорячи про механізми практичного забезпечення кібербезпеки держави, передусім звертається увага на зусилля декількох основних відомств.

Важливу частину роботи з убезпечення громадян від найбільш розповсюджених кіберзлочинів здійснює МВС. У його структурі створено спеціальне Управління боротьби з кіберзлочинністю, на яке покладено низку завдань. Зокрема, до основних завдань Управління відноситься організаційне та практичне забезпечення реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, що вчиняються з використанням інформаційних технологій та телекомунікаційних мереж (у сфері інформаційно-телекомунікаційних технологій, у сфері електронних платежів і господарської діяльності, зокрема, порушення прав інтелектуальної власності та заняття гральним бізнесом, злочини проти інформаційної безпеки, у тому числі незаконні дії зі спеціальними технічними засобами негласного отримання інформації), а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень [4]

Але проблемою залишається те, що, незважаючи на зусилля спеціально уповноважених відомств, Україна досі залишається принципово уразливою у сфері використання сучасних ІТ, й не останньою чергою через надмірно широке запровадження іноземних програмних продуктів та використання матеріально-технічної бази іноземного виробництва.

В Україні досі відсутні системні нормативні документи, які описували б загрози Україні саме в кіберпросторі, визнали б їх і стали основою для цілісної державної політики з кібербезпеки.

Тому слід наголосити, що необхідна достатня фахова підготовка фахівців з інформаційної і кібербезпеки та керівного складу органів державного управління з цих питань для потреб як силових структур, так і виробничої та банківської сфери, яка має проводитись у єдиній системі освіти України, а спеціальна підготовка офіцерського складу ЗС України та інших силових структур із загальних питань інформаційної і кібербезпеки має проводитись у системі командирської підготовки та на курсах підвищення кваліфікації. І тільки тоді Україна зможе впевнено відчувати себе на рівні європейських країн у питаннях кібербезпеки.

Список використаної літератури:

1. A Solution-based Examination of Local, State, and National Government Groups Combating Terrorism and Cyberterrorism. By: Matusitz, Jonathan; Breen, Gerald-Mark. Journal of Human Behavior in the Social Environment, Feb2011, Vol. 21 Issue 2, p. 109-129, 21 p. [Електронний ресурс]. - Режим доступу: http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN.
2. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. - Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-r.pdf.
3. Про Стратегію національної безпеки України: указ Президента України від 12.02.2007 р. № 105/2007 (із змінами від 8.06.2012 р. № 389/2012) [Електронний ресурс]. - Режим доступу: http://zakon4.rada.gov.ua/laws/show/105/2007
4. Управління боротьби з кіберзлочинністю // Міністерство внутрішніх справ України [Електронний ресурс]. - Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754

Правові реформи адміністративних правопорушень за корупцію

Лук'янчук В.О. - студентка навчально-наукового інституту права та психології Національної академії внутрішніх справ

Науковий керівник: доцент кафедри загально-правових дисциплін навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент - **Лазаренко Л.А.**