законспіровані і відомі лише дуже вузькому колу осіб.

Метою забезпечення економічної безпеки підприємства є надійний захист від можливого впливу внутрішніх та зовнішніх загроз, моніторинг рівня економічної безпеки, який передбачає виконання певних етапів щодо попередження небажаних подій, які можуть призвести до негативних наслідків, проводити аналіз якості підбору персоналу, перевіряти надійність партнерів, прогнозування рівня економічної безпеки підприємства, проведення оцінки загроз, які знижують ефективність і якість функціонування підприємства та знижують рівень управління економічною безпекою [1].

Економічна безпека є основною складовою у забезпеченні національної безпеки та важливим підґрунтям її соціально-економічного розвитку. Економічну безпеку країни розглядають як засіб у забезпеченні стабільного розвитку, надійного захисту економічних інтересів підприємств, усіх галузей промисловості, суб'єктів господарювання, розвиток регіонів та держави [2].

Існує багато питань у різних сферах розвитку держави, серед яких виступає макроекономічна, фінансова, енергетична, продовольча, виробнича, інвестиційна, соціальна, інноваційна, демографічна, а також зовнішньоекономічна. Усе це стримує економічний та соціальний розвиток країни, призводить до нестабільного розвитку та зниження національної економічної безпеки.

Таким чином, підприємства, організації, установи, юридичні особи, філії, структурні підрозділи, територіальні одиниці повинні значно посилити свій захист від будь-яких потенційних загроз, як з боку криміногенного формування, так і з боку рейдерських атак, які знижують рівень економічної безпеки національної економіки. Суб'єкти підприємницької діяльності мають створити належний захист економічній безпеці через посилення охорони, застосування сучасних технічних засобів, інформаційного захисту та застосування інноваційних методів управляння підприємством та його ресурсами.

1. Rybalchenko, L., Ryzhkov, E., & Ohrimenco, S. Modeling economic component of national security. *Scientific journal «Philosophy, Economics and Law Review»,* – 2021. -*1*(1), 25-36.

2. Rybalchenko L., Ryzhkov E. Ensuring enterprise economic security. *Scientific bulletin of the Dnipropetrovsk State University of internal affairs*. 2019. Special issue №1.- p.268-271.

Вікторія РОМАШЕНКО
доцент кафедри
тактико-спеціальної підготовки,
кандидат педагогічних наук

Анастасія СУХАНЬ
курсант Донецького державного
університету внутрішніх справ
(м. Маріуполь, Донецька обл., Україна)

ТЕНДЕНЦІЇ РОЗВИТКУ ТА ЗАХОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На сьогодні комп'ютерні злочини – це одна з найрозповсюдженіших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їхня суспільна небезпечність. Це зумовлене тим, що наука й технологія у сфері комп'ютеризації не стоять на місці і постійно розвиваються, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки. Слід зауважити, що український законодавець приділяє значну увагу цій проблемі: новий Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися, що це свідчить про актуальність цієї проблеми в суспільстві [1].

На науково-теоретичному, методичному та практичному рівнях розробкою даного питання займалися такі науковці, як В. Голубєв, А. Долгова, К. Кастельс, Т. Кесарева, Л. Кураков, Р. Лемос, А. Лукацький, які заклали основні поняття, визначили механізм індивідуальної злочнної поведінки та типологію злочинців при вчиненні кіберзлочинів.

Метою даного дослідження є визначення поняття, структури, змісту, шляхів боротьби з кіберзлочинністю, та що потрібно робити правоохоронним органам задля протидії кіберзлочинності.

Термін «кіберзлочинність» часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми.

Кіберзлочин (інформаційний злочин) – незаконні дії спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань. До основних видів кіберзлочинності можна віднести такі: розповсюдження шкідливого програмного забезпечення, крадіжка номерів кредитних карт і банківських рахунків, злом паролів, порушення авторських прав [3].

Аналізуючи наведені статистичні дані Генеральної прокуратури України щодо суб'єктів вчинення даного виду злочину за 2014–2017 рр. на території України, можна встановити, що вчинення даного виду злочину притаманне особам, які раніше вчиняли кримінальні правопорушення, проте ж основним суб'єктом вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є група осіб за попередньою змовою, що пояснюється транснаціональністю кіберзлочинності та полягає у можливості вчиняти злочини одразу на території кількох країн. Можна зазначити, що не зареєстровано вчинення даного виду злочину особами у стані алкогольного сп'яніння, адже це впливатиме на їхню уважність, обачливість, холоднокровність та врівноваженість при вчиненні злочину та неповнолітніми або за їх участю, що пояснюється їх як соціальною, так і розумовою несформованістю та проявляється у легковажності, відсутності цілеспрямованості, життєвого досвіду, небажанням ретельно підготуватися до вчинення злочину [4–5].

Слід зазначити, що для вчинення даного виду злочину притаманна умисна форма вини, окрім злочину, передбаченого ст. 363 ККУ, що передбачає як вчинення в умисній формі, так і через необережність. Необхідно зазначити, що провідні мотиви кіберзлочинців є такі:

- користь, що становить 66 % від усіх вчинених кіберзлочинів;
- політичний мотив (шпигунство, злочини, які посягають на територіальну цілісність та основи національної безпеки України) – 17 %, що у наш час є досить актуальним через складну політичну, економічну та соціальну ситуації в державі;
- дослідницький інтерес, що становить 7 %;
- хуліганські мотиви – 5 %;
- помста – 3 % [6].

Отже, проблема кіберзлочинності на сучасному етапі історичного розвитку набуває глобального виміру та становить загрозу інформаційному суспільству. Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп'ютерних даних, які дуже вразливі за своєю природою і можуть бути швидко знищені. У цій ситуації традиційні механізми правової взаємодопомоги і принцип суверенітету, одним із проявів якого є те, що тільки правоохоронні органи держави можуть проводити слідчі дії на її території, вимагають безліч формальних погоджень, роблячи розслідування транснаціональних кіберзлочинів проблематичним. Таким чином, ефективний контроль негативних явищ у кіберпросторі, таких як злочинність, вимагає набагато більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності. Саме тому, окрім гармонізації кримінально-правових, норм потрібна гармонізація процесуальних інструментів і вироблення нових механізмів міжнародного співробітництва.

1. Голубев В. А. «Кибертерроризм» – миф или реальность? Центр исследования проблем компьютерной преступности: сайт. URL : http://www.crime-research.org/library/terror3.htm.

2. Рассолов И. М. Право и Интернет. Теоретические проблемы. Москва : Норма, 2003. 254 с.

3. Криминология : учеб. для вузов ; под общ. ред. А. И. Долговой. 2-е изд., перераб. и доп. Москва : Норма, 2003. 682 с.

4. Біленчук П. Д. Портрет комп'ютерного злочинця: навч. посібник. Київ : НАВСУ, 1997. 48 с.

5. Косенков А. А. Общая характеристика психологии киберпреступника. *Криминологический журнал БГУЭП*. 2012. № 3. С. 87–94.

6. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 447.