У багатьох країнах створено спеціалізовані організації – професійні об'єднання корпоративних секретарів: британський Інститут Сертифікованих Секретарів та Адміністраторів (Institute of Corporate Secretaries and Administrators, ICSA),2 Американське Товариство Корпоративних Секретарів (American Society of Corporate Secretaries, ASCS),3 Канадське Товариство Корпоративних Секретарів (Canadian Society of Corporate Secretaries, CSCS).4 Зазначені організації здійснюють підготовку висококваліфікованих спеціалістів.

Зважаючи на результати проведеного дослідження, вважаємо, що основними напрямками подальших розвідок питання підвищення ефективності і корпоративного контролю в акціонерних товариствах, є уточнення ролі корпоративних секретарів для умов діяльності акціонерних товариств України, розробка типового положення про корпоративного секретаря акціонерного товариства, дослідження найбільш механізмів розкриття корпоративним секретарем інформації про діяльність товариства відповідно до потреб акціонерів.

ЛІТЕРАТУРА:

1. Рішення ДКЦПФР №52 Про схвалення проекту нової редакції Принципів корпоративного управління України, затверджених рішенням ДКЦПФР від 11.12.2003 N 571 [Електронний ресурс] // Режим доступу до ресурсу: http://uazakon.com/documents/date_ee/pg_gtwhou.htm

2. Governance Principles for Corporate Secretaries. Corporate Secretaries International Association// [Електронний ресурс] – Режим доступу до ресурсу: http://www.csiaorg.com/Resources/Documents/CSIA%20Governance%20Principles%20Oct13.pdf

3. The Best Practices Working Group for Online Shareholder// [Електронний ресурс] – Режим доступу до ресурсу: https://www.niri.org/NIRI/media/NIRI/Documents/shareholder_participation_annual_meetings.pdf

УДК 004.056: 341(045)

Юркевич І. І.

старший викладач кафедри кримінального права і процесу

Тернопільський національний економічний університет

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Кінець XX століття ознаменувався стрімким розвитком інформаційних технологій, що почали впроваджуватися в усі сфери життєдіяльності людей. Використання сучасних комп'ютерних технологій забезпечило можливість доступу до інформації, що зберігається у відповідних банках даних незалежно від часу і місцезнаходження особи. Поряд з перевагами, швидкий

розвиток комп'ютерних технологій має ряд негативних наслідків, серед яких є поява якісно нового виду злочинності – кіберзлочинності. Наслідки цієї злочинності зачіпають не тільки інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство в цілому. Кіберзлочини найчастіше ставлять під загрозу життєво важливу інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства.

Питанням суспільно небезпечних діянь у сфері комп'ютерної інформації присвятили наукові праці П. П. Андрушко, М. В. Карчевський, В. В. Кузнецов, А. А. Музика, С. О. Орлов, Н. А. Розенфельд та ін.

Кіберзлочинність - це злочинність в так званому «віртуальному просторі». Віртуальний простір або кіберпростір можна визначити як модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі.

Основними ознаками кіберзлочинності є:

- ці злочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Віртуальний простір – це модульований за допомогою комп'ютера інформаційний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі .
- кіберзлочини вчиняються за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину [5].

Можна виділити такі види кіберзлочинності:

- традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету (шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.),
- нові злочини, що стали можливі завдяки новітнім комп'ютерним технологіям (злочини передбачені Розділом XVI Кримінального кодексу України).

Найбільш розповсюдженою є класифікація кіберзлочинів на: 1) агресивні; 2) неагресивні.

До першої групи належать: кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кібersталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них). Друга група включає: кіберкрадіжка,

кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм [1].

Основна проблема, а вона спільна як для США, так і для України, полягає в тому, що державні спецслужби та відомства цілеспрямовано нагнітають страхи навколо потенційної загрози мережевого тероризму з метою збільшення фінансування своєї діяльності [5]. Так, наводяться цифри – 50 мільярдів доларів щорічно – витрат США на створення інформаційної безпеки [2]. На думку скептиків щодо можливості успішних кібернетичних атак, гіпершвидкий розвиток мережі інтернет спровокував війни у віртуальних світах, що дало підстави футурологам виманювати чималі кошти у військових відомств на боротьбу з імовірними загрозами. Тим часом визначення ступеня ймовірності загроз перебуває у площині суб'єктивній та поза межами громадського контролю. Загроза може бути штучно гіпертрофована, через що одна країна матиме доступ до внутрішніх справ іншої. Створення «образу ворога» завжди було ефективним засобом провадження власної внутрішньої та зовнішньої політики; «холодна війна» переходить у віртуальну площину. Наслідки кібернетичного втручання однієї країни у справи іншої можуть бути різні: від впливу на економічні процеси до розгрому опозиційних рухів, здатних легко «експортуватися» на територію держави-сусіда.

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» і мереж електрозв'язку; двічі положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві.

Та все ж кіберзлочинність не зупиняють державні кордони. Її транснаціональний характер спричинює проблему кваліфікації злочинів, яку слід розв'язувати шляхом уніфікації національних кримінальних законодавств. На це спрямовано дію Міжнародної конвенції про кіберзлочинність, яку укладено 23 листопада 2001 р. в м. Будапешті й до якої нещодавно приєдналась Україна [3] Конвенція стала важливим правовим документом, на базі якого держави, що приєдналися до неї, розбудовують власні системи протидії кіберзлочинам.

Швидкі темпи поширення інформації серед усіх верств населення, відсутність захисних заходів населення з боку департаментів державних органів безпеки по боротьбі із кіберзлочинністю відносно місцевих інтернет провайдерів, доступність інформації про методи скоєння кіберзлочинів. Перераховані вище проблеми повинні стати пріоритетними напрямками роботи відповідних державних органів як в Україні, так і в тих країнах, де кіберзлочинність має велику питому вагу у відношенні до кіберзлочинів, що вчиняються у всьому світі. Також потрібна організована робота департаментів багатьох країн через транснаціональність кіберзлочинності.

ЛІТЕРАТУРА :

1. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : моногр. / Азаров Д. С. – К. : Атіка, 2007. – 304 с.

2. Гриняев С. Концепция ведения информационной войны в некоторих странах мира // Зарубежное военное обозрение. – 2002. – № 2. – С. 11–15.

3. Конвенція про кіберзлочинність [Електроний ресурс]. – Режим доступу http://zakon2.rada.gov.ua/laws/show/994_575.

4. Ленюк Я. С. Практика протидії злочинам загально кримінальної спрямованості з використанням Інтернет-мережі / Я. С. Ленюк // Спеціальна техніка у правоохоронній діяльності : матеріали V міжнар. наук.-практ. конф. (Київ, 25 листоп. 2011 р.). – К. : Нац. акад. внутр. справ України, 2012. – С. 211-214.

5. Морозов І. Політичний екстремізм в Інтернеті // Политическая коммуникация в постсоветской России: проблеми формирования и парадигми развития : материалы секции «Политическая коммуникация» Третьего всерос. конг. политологов [28–29 апреля 2003 г.]. – М. ; Улан-Уду : Изд-во ОАО «Республиканская типография», 2003.

УДК 547.022

Яцюк В. М.
к.х.н., заступник завідувача відділу досліджень матеріалів, речовин і виробів
Тернопільський науково-дослідний експертно-криміналістичний центр МВС України

МОДИФІКОВАНІ ЕПОКСИДНІ КОМПОЗИТИ ЯК ПЕРСПЕКТИВНІ ЛАКО-ФАРБОВІ ПОКРИТТЯ ІЗ ПОКРАЩЕНИМИ ФІЗИКО-МЕХАНІЧНИМИ ВЛАСТИВОСТЯМИ

З розвитком виробництва металів та сплавів зростає попит на використання покриттів, як засобів захисту матеріалів від корозійного руйнування. Серед відомих захисних покриттів (металевих і неметалевих) за властивостями, наявністю сировинної бази зв'язувачів і компонентів на території України, простотою технології формування і нанесення та, враховуючи експлуатаційні характеристики, найбільш перспективними є використання покриттів з покращеними властивостями. Важливе значення при експлуатації і ремонті засобів транспорту, у тому числі й річкового та морського, має застосування полімерних композитних матеріалів (КМ) та захисних покриттів на їх основі [1].

У першу чергу, актуальними є питання, що стосуються підвищення надійності роботи й відповідно експлуатаційних характеристик елементів технологічного обладнання, які піддаються статичним та динамічним навантаженням, що є першопричиною їх зношування і корозії. Широкий спектр зовнішніх та внутрішніх факторів, які впливають на характеристики структури деталей, і, як наслідок, визначають їх надійність, передбачає використання нових матеріалів, що відзначаються комплексом підвищених характеристик. Перспективою використання таких матеріалів є можливість їх застосування у критичних умовах експлуатації деталей та механізмів, що є важливим і актуальним при ремонті засобів морського та річкового транспорту в умовах рейсу [2].