агресивну поведінку, їх адаптацію до умов життя, визначення індивідуальних здібностей, орієнтації, спрямованості, кризових зон розвитку учасників, їх навчання адекватним емоційним проявам і навичкам взаємодії. Програма передбачає використання інтенсивних методів оволодіння навчальним матеріалом: ділові, імітаційні, сюжетно-рольові, організаційні ігри, тренінги, практичні заняття в діючому соціумі.

Алєксєєнко Ірина Вікторівна –
доктор політичних наук, професор,
зав кафедри міжнародних відносин
та туризму ФСПОУ

Боровенська Анастасія Анатоліївна –
студентка гр. Б-МВ-841, ФСПОУ

*(Дніпропетровський державний
університет внутрішніх справ)*

КІБЕРТЕРОРИЗМ ЯК ВИКЛИК НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ: ОСОБЛИВОСТІ ПРОТИДІЇ

Світова спільнота зіткнулася з проблемою створення безпечного глобального інформаційного суспільства задля ефективності протидії кіберзлочинності та кібертероризму. Для комплексного та узгодженого розвитку правового регулювання цього питання важливим фактором є координація зусиль держав міжнародного політичного простору. З огляду на те, що інформаційна злочинність є міжнародною проблемою і має транснаціональний характер, проведення успішного розслідування злочинів та притягнення до відповідальності вимагає від світового товариства єдиного розуміння проблем, узгодження правової бази та розвитку співробітництва в сфері забезпечення інформаційної безпеки та боротьби з кібертероризмом.

Стрімкий розвиток інформаційно-комунікаційних технологій сприяє налагодженню широкої міжнародної співпраці. Проте окремі досягнення в інформаційній сфері можуть бути використані в цілях, що суперечать підтримці міжнародної безпеки та стратегічної стабільності. Ростуть масштаби кіберзлочинності та кібертероризму [1]. Особливе хвилювання викликає можливість застосування інформаційно-телекомунікаційних технологій для підготовки та здійснення терористичних актів у світі.

Варто зазначити, що правові механізми боротьби зі злочинами в інформаційній сфері були розроблені у декілька етапів, а саме: починаючи з 1970-1980-х рр. на рівні національних законодавств держав, а починаючи з 1990 року - на регіоналному та міжнародному. Резолюції, що стосуються протидії кіберзлочинності, були прийняті Генеральною Асамблеєю ООН, СНД,

БРІКС, ШОС, Радою Європи та Європейським Союзом, підписані багатосторонні й двосторонні угоди з питань забезпечення міжнародної інформаційної безпеки, в яких розглянуті питання протидії інформаційним злочинам[2].

Існує проблема невирішених колізій щодо різних підходів у міжнародній практиці. Зокрема, Будапештська конвенція про кіберзлочинність 2001 року, потребує перегляду та вдосконалення. Багато країн, не беруть участі в ній через неприйнятність одного з основних її положень - про транскордонний доступ до даних при проведенні розслідувань, - яке йде в розріз із принципом державного суверенітету.

Як зазначалося раніше, кібертероризм займає одну з найвищих сходинок основних загроз інформаційній безпеці, тому значне місце у системі міжнародної інформаційної безпеки відводиться вирішенню цієї проблеми. Витоками цієї загрози є діяльність терористичних організацій та причетних до цього осіб, які здійснюють протиправні дії за допомогою інформаційних ресурсів або відносно них.

Світ потребує універсальних міжнародних правових механізмів для активної протидії кібертероризму та іншим злочинам інформаційної сфери на основі взаємовигідної співпраці міжнародної спільноти і приватного сектора, обміну досвідом щодо національних практик та методів боротьби в цілях розробки ініціатив для вдосконалення правового забезпечення міжнародної економічної безпеки.

Характер новації в системі міжнародного кримінального права в даний час набули злочини в інформаційній сфері, які підпадають під поняття "транскордонна злочинність". У зв'язку з цим для ефективної боротьби зі злочинами в інформаційній сфері необхідно враховувати зарубіжний досвід, оскільки забезпечення безпеки комп'ютерної інформації і технологій кримінально-правовими засобами сьогодні є однією з актуальних проблем в більшості зарубіжних держав.

Наразі світова спільнота розбудовує засади загального та безпечного інформаційного простору та протидії однііій з основних загроз міжнародної інформаційної безпеки, пов'язаної з використанням інформаційних технологій для вчинення злочинів, в тому числі пов'язаних з неправомірним доступом до комп'ютерної інформації, зі створенням, використанням і поширенням шкідливих комп'ютерних програм.

Аналіз законодавства держав міжнародного політичного простору свідчить про основні напрямки боротьби з кіберзлочинністю.

Так, ще в 1993 році в Нідерландах був прийнятий Закон про комп'ютерні злочини, що доповнює Кримінальний кодекс новими складами: несанкціонований доступ в комп'ютерні мережі; несанкціоноване копіювання даних: комп'ютерний саботаж; поширення вірусів; комп'ютерне шпигунство.

У Німеччині діє Кримінальний кодекс, який передбачає відповідальність за інформаційні злочини і злочини у сфері інформаційних технологій.

У Великій Британії діє закон про зловживання комп'ютерами.

Кримінальний кодекс Франції включає цілий ряд складів злочинів в інформаційній сфері. Зокрема, встановлюється відповідальність за злочини, що посягають на системи автоматизованої обробки даних, такі як незаконний доступ до автоматизованої системи обробки даних або незаконне перебування в ній; перешкоджання роботі або порушення роботи системи; введення обманним шляхом в систему інформації, а також зміна або знищення даних.

У Сполучених Штатах Америки політика захисту від сторонніх вторгнень в інфраструктуру промисловості, фінансової сфери, науки і освіти була побудована саме на спільній координаційній роботі.

Аналізуючи законодавство України з інформаційної безпеки, слід відмітити ряд положень які визначають позицію нашої держави щодо перспектив міжнародного співробітництва в сфері інформаційній безпеці.

Так, основними напрямами діяльності у зовнішньополітичній сфері є:

- якісне вдосконалення інформаційного супроводу державної політики, діяльності українських громадських організацій та суб'єктів підприємницької діяльності за кордоном за пріоритетами стратегічного партнерства та економічної доцільності;

- посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення національної безпеки України за умов повноправного партнерства з країнами - членами ЄС та Північноатлантичного альянсу;

- інтеграція в міжнародні інформаційно-телекомунікаційні структури та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету [3].

З урахуванням динаміки розвитку негативних тенденцій в цифровому середовищі на даному етапі, доцільно перевести правову дискусію з запобігання кібертероризму в практичне русло з виходом на конкретний результат.

Отже, з огляду на високу здатність інтеграції інформаційних засобів з іншими традиційними та технологічно новими видами військового озброєння, потенційні наслідки безконтрольного застосування багатошарового інформаційного простору можуть виявитися катастрофічними для національної безпеки держави так і для існування людства в цілому.

Гарантування протистояння викликам кібертероризму можливе лише на основі плідного співробітництво держав у сфері міжнародної економічної безпеки та впровадження пакету заходів на основі виважених міжнародних нормативно-правових актів з урахуванням специфіки національних законодавств держав-учасниць.

---

1. Бойченко О. В. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки / О. В. Бойченко // Форум права. – 2009. – № 2. – С. 56–URL : hhttp://www.nbuv.gov.ua/ejournals/FP/2009-2/09bovzou.pdfH.

2. 2.Білорус О. Г. Глобалізація і безпека розвитку : монографія / О. Г. Білорус, Д. Г. Лук'яненко. – К. : КНЕУ, 2001. – 733 с.

3. Указ Президента України «Про Доктрину інформаційної безпеки України» : від 08.07.2009 р., № 514/2009 // Офіційний вісник України. – 2009. – №5 2. – Ст. 1783.