5. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монограф. / О. П. Єрменчук. Дніпро : Дніпроп. держ. ун-т внутр. справ, - 2018. - 180 с.

6. Гаврильців М.Т. Інформаційна безпека держави у системі національної безпеки України / Гаврильців М.Т. // Юридичний науковий електронний журнал. - 2020. - № 2. - С. 200-203.

УДК 343.98

Онищенко Ю.М.
кандидат наук з державного управління, доцент
Світличний В.А.
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ

ПІДХОДИ ДО УДОСКОНАЛЕННЯ ДЕРЖАВНИХ МЕХАНІЗМІВ БОРОТЬБИ З КІБЕРЗЛОЧИННОСТЮ

Сьогодні економічна, соціальна та військова безпека будь-якої держави значною мірою залежить від гарантування безпеки в інформаційній сфері. Державна політика захисту інформації та кібернетичної безпеки, її повнота та ефективність забезпечують стабільність у суспільстві, дотримання прав і свобод громадян. В основному Законі України у ст. 17 відзначається, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу [1].

Паралельно зі стрімким розвитком інформаційних технологій (далі – ІТ) та активним їхнім використанням у всіх сферах життя сучасного соціуму, збільшується кількість використання ІТ та глобальної мережі Інтернет з протиправними намірами.

Незважаючи на зовні різну природу двох найпомітніших останніми роками соціальних феноменів – глобалізації злочинності та появи глобального інформаційного мегасередовища, виявляється дуже жорсткий їх зв’язок і тенденція до його зміцнення. Взаємозалежність цих суспільних проявів виходить далеко за межі електронно-кримінального явища, що визначається терміном «комп’ютерна злочинність» або «кіберзлочинність».

Глобалізація інформаційних процесів і поява глобального інформаційного простору, який за своєю суттю є нематеріальним і поки що в повному обсязі не є законодавчо врегульованим (сама можливість подібного врегулювання – дуже суперечливе питання), призводить не лише до появи нових об’єктів злочинних посягань – комп’ютерів і комп’ютерних мереж. З’являються нові способи скоєння злочинів, наприклад здійснення розкрадань шляхом зміни або блокування комп’ютерних даних. Інші наслідки повсюд-

ного поширення ІТ – майже безперешкодне формування і пропаганда кримінальної ідеології, використання інформаційного простору в кримінальних цілях – для зв'язку і обміну досвідом, координації дій тощо.

Кіберзлочинність є однією з найактуальніших проблем сучасності, оскільки негативно впливає на діяльність органів державної влади та органів місцевого самоврядування, а завдана нею шкода стосується різних сфер суспільної життєдіяльності, зменшує рівень довіри до державного апарату в цілому. Ефективність запобігання і протидії кіберзлочинності засобами державного управління безпосередньо залежить від узгодженості дій та заходів усіх суб'єктів, наявна система яких, їх функціональна та організаційно-штатна структура є недосконалими. З урахуванням цього можна стверджувати, що серед актуальних проблем сучасного державного управління чільне місце належить дослідженню механізмів запобігання і протидії кіберзлочинності.

Проблематику забезпечення державного управління у сфері запобігання і протидії кіберзлочинності в Україні в умовах світової глобалізації не систематизовано, щобільше, подекуди не визначено й найбільш суттєвих загроз. А це, у свою чергу, призводить до нехтування досвідом передових країн світу, які вже мають напрацювання та формалізовані методики боротьби з кібератаками, кіберінцидентами, кіберзлочинами, нарешті – кібертероризмом.

До основних напрямів подальшого розвитку державних механізмів боротьби з кіберзлочинністю в Україні можна віднести удосконалення: правового механізму забезпечення взаємодії між органами державної влади в частині впорядкування нормативно-правових актів за схемою: концепція → стратегія → пакет нормативно-правових актів; інституціонального механізму – шляхом проведення відповідних організаційно-штатних змін для оптимізації структури державних органів, що опікуються забезпеченням кібербезпеки.

Дослідження проблем боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні та технологічні засоби забезпечення інформаційної безпеки (технічний захист інформації) в умовах інформатизації, у тому числі профілактики кіберзлочинів, не має значного успіху [2].

Чим складніше стає комп'ютерне програмно-математичне забезпечення, тим більше уразливими виявляються традиційні організаційні заходи і засоби інженерно-технічного захисту інформації в автоматизованих (комп'ютерних) системах, зокрема відносно несанкціонованого доступу.

Проблемою наступного порядку також є і те, що з розвитком сучасних електронних засобів інформації розвиваються й технічні засоби перехоплення і доступу до інформації, яка обробляється і передається в електронних системах зв'язку. Доступ до цих засобів не створює проблеми для злочинних формувань.

Найбільшу небезпеку для суспільства і держави складає трансгранична організована кіберзлочинність: комп'ютерний тероризм; диверсії, інші прояви антагоністичної інформаційної боротьби кримінальних формувань з державою, правоохоронними органами; крадіжки інформації з комп'ютеризованих баз даних і порушення права інтелектуальної власності на комп'ютерні програми; шахрайства з використанням комп'ютерних технологій, особливо у сфері міжнародних економічних відносин (кредитно-фінансова, банківська) тощо.

Трансграничний характер кіберзагроз змушує країни вступати в тісну міжнародну співпрацю, яка потрібна не лише для ефективної підготовки до захисту від кібератак, але і для своєчасної реакції на них, ліквідації наслідків.

Література

1. Конституція України // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. – URL:https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 09.03.2021).

2. Орлов О.В. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю / О.В. Орлов, Ю.М. Онищенко // Державне управління: удосконалення та розвиток. – 2014. – № 5. – URL:http://www.dy.nayka.com.ua/?op=1&z=715 (дата звернення 09.03.2021).

УДК 355.40:358.12

Оніщук В.С.
Національний університету оборони України
імені Івана Черняховського

ОСОБЛИВОСТІ ВВЕДЕННЯ ПСИХОЛОГІЧНОГО ВПЛИВУ

Коли розповсюдження інформації про негативну громадську думку впливає на політичні концепції людей, це часто призводить до того, що в першу чергу люди мають різні думки про правлячу групу. Неорганізовані та неузгоджені політичні відносини між людиною та правлячою групою неминуче призводять до конфліктів. Основні засоби масової інформації почали критикувати або ставити під сумнів неоконсервативну глобальну стратегію та політику. Є багато книжкових видань, таких як "Занепад влади Сполучених Штатів", "Кінець американської ери", "Смуток імперії: кінець мілітаризму, таємність і республіканізм", "Пузир верховенства США", "Вибір: глобальне домінування або глобальне лідерство", "Надмірність імперії: чому Захід втратить війну з тероризмом" та інші бестселери. AssociatedPress також повідомила, що 20-річне покоління молодих людей навколо Сполучених Штатів Америки розглядає військове зловживання ув'язненими на телебаченні і "Записали, як вони сумні, ганебні та розчаровані". Все це сильно стимулювало протистояння між громадськістю США