Черниш Роман Федорович
кандидат юридичних наук, доцент
Житомирський національний агроекологічний університет

Забезпечення інформаційної безпеки держави, як одна із складових перемоги у «гібридній війні»

З березня 2014 р. (*моменту анексії російськими військами території АР Крим, а також неофіційної участі військового контингентна РФ у військових діях на сході України*), в державі фактично розпочалася "гібридна війна". Реалії сьогодення вимагають докорінної перебудови усього державного механізму, в т.ч. й оптимізації діяльності правоохоронних органів та вдосконалення національного законодавства. Особливої актуальності вищевказане набуває на фоні активізації протиправної діяльності бойовиків терористичних організацій ДНР/ЛНР, постійних спроб останніх по розширенню площ захоплених територій (*всупереч т.зв.* "*Мінським угодам*"), підготовки на території РФ, за сприяння представників спеціальних служб зазначеної країни, диверсійних груп для вчинення терористичних актів майже у всіх регіонах (*Донецька*, *Луганська*, *Одеська*, *Харківська, Запорізька і т.д. області*), направлених на дестабілізацію суспільно-політичної ситуації, а також дискредитацію вищого керівництва держави, особовий склад до яких підшукується в т.ч. й за допомогою Інтернет ресурсів.

Поряд з тим, Інтернет-простір активно використовується з метою прихованого психологічного, політичного, комерційного та фізичного примусу, викривлення сприйняття реальності. Серед способів та технологій, які застосовуються з вищевказаною метою, виділяються наступні: пряме підтасовування фактів; замовчування невигідної інформації; упередженість інтерпретації фактів; надання сфальсифікованої інформації; навішування ярликів для компрометації політиків тощо.

Для доведення вигідної інформації до суспільства, перевага, як правило, надається електронним засобам масової інформації (*Інтернет-виданням*), які використовують новітні інформаційні технології для розповсюдження новин.

Окремою технологією маніпулювання можна виділити т.зв. маніпулювання на форумах. Даний вид технології полягає в коментуванні, в т.ч. анонімному, тієї чи іншої проблематики та ситуації різними користувачами Інтернет-ресурсу, що є

ознакою демократизму і плюралізму Інтернету. Водночас, зацікавлені особи можуть активно втручатися у форуми, коментуючи, начебто й неупереджено, ті чи ті події. Насправді ж "голос народу" виявляється звичайним пропагандистським засобом, іноді провокативним, але завжди дієвим, бо здається об'єктивним. Маніпулювання на Інтернет-форумах соціально шкідливе, оскільки розповсюдження неправдивої інформації дискредитує сам інститут громадської думки, робить його вразливим та недієздатним.

У зазначеному контексті, нами виокремлено ряд негативних чинників, своєчасне усунення яких дозволить удосконалити нормативно-правову базу у сфері забезпечення в Україні загальнодержавної системи кібербезпеки та сприятиме її ефективному використанню.

Зокрема, аналіз наявної інформації свідчить, що законодавчі акти у вищевказаній сфері здебільшого перебувають на стадії розробки або доопрацювання, внаслідок чого ускладнюється процедура правового реагування та впливу на діяльність суб'єктів інформаційного поля держави.

Так, відсутність низки законодавчо-закріплених понять у вказаній сфері негативно впливає на прийняття рішень слідчими при кваліфікації відповідних протиправних діянь.

Диспозиція ст. 111 КК України передбачає відповідальність за діяння, умисно вчинене громадянином України, в т.ч. на шкоду інформаційній безпеці, хоча в національному законодавстві відсутнє тлумачення терміну "інформаційна безпека" (*в окремих коментарях до ст.111 ККУ також вживається поняття "інформаційної експансії"*), що створює підґрунтя для правих маніпуляцій з боку зацікавлених сторін кримінального процесу (*зазначений термін розуміється ними на власний розсуд через призму суб'єктивності*).

Іншим негативним аспектом забезпечення інформаційної безпеки є те, що процеси впровадження в органах державної влади нових інформаційно-телекомунікаційних проектів відбуваються без попереднього їх забезпечення відповідною нормативною та організаційно - режимною базою, створення сучасних систем технічного/криптографічного захисту інформації, а також відсутності належного фінансування.

Також, серед актуальних проблемних питань залишається неналежне забезпечення операторами/провайдерами телекомунікацій під час надання органам державної влади та місцевого самоврядування доступу до мережі Інтернет відповідного рівня захисту систем та мереж від зовнішніх втручань, резервування каналів на випадок блокування основних та, навпаки, створення ними через нехтування вимог із захисту інформації можливостей прихованого моніторингу сторонніми особами інформації, яка передається зазначеними каналами.

На нашу думку, з метою розбудови в Україні ефективної системи інформаційної безпеки, на рівні Кабінету Міністрів України першочергові зусилля повинні бути спрямовані, насамперед, на реалізацію загальнодержавних проектів інформатизації та вдосконалення положень національного законодавства. А саме:

- створення національної інформаційно-телекомунікаційної системи (державного провайдера/оператора телекомунікацій);
- розвиток системи національних інформаційних ресурсів;
- інформатизацію стратегічних напрямів розвитку економіки держави, її безпеки та оборони, соціальної сфери.