- бездротових атак;
- атак на веб-сервери і застосування;
- електронної пошти;
- мобільних пристроїв.

Таким чином, можна зазначити, що системне опрацювання засобів, прийомів і методів цифрової криміналістики із їх подальшим використанням при розслідуванні кіберзлочинів дозволить якісно змінити ефективність таких розслідувань.

Використані джерела:

1. National Institute of Standards and Technology Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response. August 2006. doi:10.6028/NIST.SP.800-86.

Орлов В.С.
слухач магістратури Одеського державного університету внутрішніх справ
Ісмайлов К.Ю.
кандидат юридичних наук, майор поліції
завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ

НАЦІОНАЛЬНІ МЕХАНІЗМИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ: СТАН І ПРОБЛЕМИ НОРМАТИВНО-СТРАТЕГІЧНОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

Упродовж 2013–2016 років тематика кібербезпеки дедалі активніше артикулюється в Україні на найвищому рівні, хоча до реальних заходів стратегічного характеру Україна у цій сфері поки що не вдавалася. Загалом механізми, які були задіяні (найчастіше під тиском зовнішніх ініціатив і зобов’язань), були фрагментованимі та несистемними.

Розв’язанню проблеми відсутності реальних кроків України в кіберпросторі жодним чином не сприяє недосконале чинне законодавство, яке досі виходить з парадигми штучного розширення предмета інформаційної безпеки на максимальну кількість сфер. Це, по-перше, розмиває сам предмет інформаційної безпеки, а по-друге, обумовлює відсутність частини кібер у вітчизняних нормативно-правових документах. Натомість використовується в суто пострадянському дискурсі поняття інформаційна безпека та низка інших, тісно з ним пов’язаних: інформаційний суверенітет; інформаційна інфраструктура» [1]; інформаційні впливи тощо. На виправдання зазначеного підходу зазвичай наводиться той аргумент, що терміни з частиною кібер акцентують виключно на формальній стороні інформаційних процесів, ігноруючи сторону змістову.

При цьому поняття інформаційної безпеки досить активно використовується в нормативно-правових документах усіх рівнів. Відповідно до ст. 17 Конституції України «захист суверенітету і територіальної цілісності України, забезпечення її економічної й інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Важко однозначно заперечувати слушність і цінність зазначеного підходу, але, на нашу думку, він не охоплює тих заходів, які в західній науковій та юридичній практиці стосуються саме проблем кібербезпеки. Передусім ідеться про протидію комп'ютерній злочинності й комп'ютерному тероризму. До речі, жодне з цих понять не отримало належного визначення в національному законодавстві, а тому незрозуміло, з чим, власне, пропонується «боротися».

Аналогічний підхід зберігається і в Доктрині інформаційної безпеки України. Доктрина зазначає, що основною метою реалізації її положень є створення в Україні розвиненого національного інформаційного простору та захист її інформаційного суверенітету. Перелік загроз інформаційній безпеці України, що їх визначає документ, є дуже широким: від недостатньої розвиненості інститутів громадянського суспільства та недосконалості партійно-політичної системи до відставання українського кінематографа, книговидання, книгорозповсюдження та бібліотечної справи від рівня розвитку відповідних сфер у розвинутих державах. Таким чином, згідно з Доктриною інформаційна безпека стає всеосяжною «темою», яка може бути віднайдена в будь-якій сфері людського буття.

Стратегія зазначає, що поширення кіберзлочинності є чинником, що загрожує глобальній міжнародній стабільності й негативно позначається на безпековому середовищі України. Увага акцентується й на тому, що на тлі зростання викликів і посилення загроз національній безпеці зберігається невідповідність сектору безпеки і оборони України завданням захисту національних інтересів, що характеризується, зокрема, нездатністю України протистояти новітнім викликам національній безпеці (явищам і тенденціям, що можуть за певних умов перетворитися на загрози національним інтересам), пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам.

На сьогодні зберігається дуже розгалужена (при цьому сталою є тенденцію до зростання кількості суб'єктів) система залучення державних інституцій у забезпеченні кібернетичної безпеки України.

1. Президент України.
2. Рада національної безпеки і оборони України.
3. Кабінет Міністрів України.
4. Служба безпеки України.
5. Міністерство внутрішніх справ України.
6. Державна служба спеціального зв'язку та захисту інформації.
7. Міністерство оборони України.
8. Національна комісія, що займається регулюванням зв'язку та інформатизації.

9. Національний банк України.

10. Державне агентство з питань науки, інновацій та інформатизації.

11. Науково-дослідні установи, неурядові структури, оператори і провайдери телекомунікацій.

Крім цього, в Україні діє спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України – CERT-UA (Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) [2]. Ця команда є частиною CERT (Computer Emergency Response Team) та акредитованим членом FIRST (Forum for Incident Response and Security Teams – Форум команд реагування на інциденти інформаційної безпеки). Одним з основних завдань CERT-UA є координування діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ та організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Водночас, незважаючи на значну кількість відомств, задіяних у забезпеченні кібербезпеки держави, основні функції належать обмеженому колу виконавців: Службі безпеки України, Міністерству внутрішніх справ України, Державній службі спеціального зв'язку та захисту інформації, Міністерству оборони України.

Традиційно у структурі Служби безпеки України інтереси держави у сфері інформаційної безпеки було покладено на Департамент контррозвідувальної діяльності. Однак Указом Президента України від 25 січня 2012 року № 34/2012 створено спеціальний Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. Його основними завданнями є «сприяння концентрації сил і засобів, вирішенні завдань із захисту законних інтересів держави і прав громадян в інформаційній сфері від розвідувально-підривної діяльності іноземних спецслужб, протиправних посягань організацій, груп та осіб» [3]. Крім того, до функцій Департаменту також належить «захист урядових телекомунікаційних систем, державних інформаційних ресурсів, критичних об'єктів інформаційної інфраструктури держави; боротьба з кібертероризмом; боротьба з кіберзлочинністю, що становить загрозу життєво важливим інтересам держави; контроль за обігом спеціальних технічних засобів негласного одержання інформації».

Увагу СБУ до проблематики кібербезпеки засвідчують ті факти, що Службу в цій рольовій функції часто згадують у виступах її очільників, а проблематика кібербезпеки дедалі частіше висвітлюється її керівниками. Так, в одному з інтерв'ю екс-голова Служби безпеки України І. Калінін, зазначив, що «статистичні дані свідчать про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів» [4].

Крім того, СБУ також ініціювала розвиток контактів у сфері протидії комп'ютерної злочинності із Францією, Білоруссю, Італією, Ізраїлем, Швецією,

Румунією, Молдовою, Угорщиною, Єгиптом, Японією, Алжиром та Спеціальним комітетом НАТО. На регулярній основі відбуваються експертні консультації експертів Україна – НАТО з питань кіберзахисту.

Важливу частину роботи з убезпечення громадян від найбільш поширених кіберзлочинів здійснює МВС, у структурі якого створено спеціальне Управління боротьби з кіберзлочинністю, на яке покладе но низку завдань, поміж яких участь у формуванні та забезпеченні реалізації державної політики щодо попередження і протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням (далі – сфера боротьби з кіберзлочинністю) [5]. У тому числі: кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (далі – протиправного контенту); економіки, яка включає в себе фінансові й торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері (далі – електронної комерції); надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище кримінальних правопорушень) [6].

Оскільки питання кібербезпеки є для України відносно новими т а зачіпають інтереси не лише державних інститутів, а й приватного сектору, громадянського суспільства та кожної особи зокрема, доцільно використати відповідну європейську кібербезпекову практику [7].

Хотів би зауважити, проте, що для вітчизняної політичної практики подібні механізми вироблення політики з певного питання є доволі новими, а набутий у цій сфері досвід не завжди був успішним. Українські державні структури мають досвід написання «білих книг» (особливо з питань реформування державних органів), однак їх реальний вплив на зміни у відповідних сферах був мінімальним.

Своєрідним наслідком відсутності цілісного обговорення кібербезпекових питань у якомога ширшому колі є відсутність в Україні системних нормативних документів, що описували б загрози Україні в кіберпросторі, визнавали їх існування й формували цілісну державну політику кібербезпеки.

Пріоритетним у полі створення цілісного законодавства з кібербезпеки є прийняття Стратегії забезпечення кібернетичної безпеки України, зобов'язання щодо розроблення якої Україна взяла на себе перед закордонними партнерами. Цей документ має визначити основні поняття у сфері, загрози, принципи та напрями забезпечення кібербезпеки й, зокрема, заходи щодо вдосконалення

державного управління та нормативно-правового поля у сфері кіберзахисту [8]. Це саме той шлях, яким активно просуваються провідні країни світу, передусім країни – члени НАТО.

В Україні жодного разу не проводилися комплексні навчання з проблеми кібербезпеки (на кшталт навчань «Кіберштурм», що проводяться у США, або аналогічних навчань, що проводяться ЄС) із залученням усіх відомств, які належать до системи забезпечення кібербезпеки держави.

Майже відсутні поліпрофільні науково-дослідні інститути, задіяні в комплексних дослідженнях інформаційної безпеки. Переважно дослідження з відповідної тематики стосуються проблеми обмеження доступу до інформації чи забезпечення технологічної безпеки; про соціально-гуманітарний компонент, а надто поєднання технологічних та гуманітарних складників, не йдеться.

Ще одна проблема полягає в тому, що, незважаючи на зусилля спеціально уповноважених відомств, Україна (особливо телекомунікаційний компонент її інформаційної інфраструктури) й досі є принципово уразливою до кіберзагроз і не останньою чергою через надміру широке транслювання іноземних програмних продуктів і використання матеріально-технічної бази іноземного виробництва. Пошук можливих «закладок» у цій продукції практично унеможливлюється через залежність Української держави від згаданих продуктів, що вийшла на дійсно загрозливий для національної безпеки рівень на всіх рівнях і в усіх сферах.

Суттєвою проблемою взаємодії держави з приватним сектором є недовіра між бізнесом та урядом. Бізнесові структури не переконані, що уряд не передасть дані (або створить умови для їх отримання) про кібератаки компаніям-конкурентам або третім особам або оприлюднить їх. Можливість не повідомляти урядові структури про кібератаки обумовлена латентним характером останніх. Відповідно, держава не вживає необхідних заходів [9].

На жаль, в Україні сфера державно-приватного партнерства є найбільш нереалізованою, і тут спостерігаються певні національні особливості, пов’язані з тим, що в Україні майже відсутні дійсно фахові НДО безпекового спрямування. Наявні організації натомість мають надто широку сферу діяльності, що унеможливлює налагодження з ними конструктивних відносин щодо проблем кібербезпеки. В окремих випадках ідеться про вкрай низький рівень аналітичних матеріалів, підготовлених профільними НДО, які до того ж не напрацювали дійсно ефективних механізмів донесення своїх розробок і пропозицій до посадових осіб. Не останньою проблемою є й надто тісна залежність більшості вітчизняних НДО від іноземних (переважно американських) джерел фінансування. Кіберпростір як новий вимір геополітичного суперництва

Таким чином, для України актуальною є ціла низка проблемних питань, розв’язання яких потребуватиме часу та певних зусиль як з боку держави, так і бізнесу/НДО.

Використані джерела:

1. Дубов Д. Модернізація інформаційної інфраструктури як чинник забезпечення національних інтересів України / Д. Дубов // Стратегічні пріоритети. – 2013. – № 2. – С. 90–96.

2. Дубов Д. Стратегічні аспекти кібербезпеки України / Д. Дубов // Стратегічні пріоритети. – 2013. – № 4. – С. 119–126.

3. Дубов Д. Сучасні тенденції забезпечення кібербезпеки на міжнародному рівні / Д. Дубов // Стратегічні пріоритети. – 2011. – № 4. – С. 5–11.

4. Зовнішньополітичні пріоритети [Електронний ресурс]. – Режим доступу: http://mfa.gov.ua/ua/about-ukraine/foreign-policy

5. Кибербезопасность [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/ecosoc/itu/cybersecurity.shtml

6. Пояснювальна записка до проекту Закону України «Про внесення змін до деяких законів України щодо структури та порядку обліку кадрів Служби безпеки України» [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=41867

7. СБУ: Головні проблеми для України – тероризм і кіберзлочинність [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285/

8. Управління боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/pub lish/article/544754293

9. Про Концепцію Національної програми і інформатизації: закон України від 4.02.1998 р. № 75/98-ВР) [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/75/98-%D0% B2% %80

Пекарський С.П.
доцент кафедри СД та АД
Донецького юридичного
інституту, к.ю.н.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ НАВЧАЛЬНИХ ДИСЦИПЛІН З ГРИФОМ ОБМЕЖЕНОГО ДОСТУПУ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Питання правових, організаційних, фінансових засад функціонування системи вищої освіти, поєднання освіти з наукою, забезпечення потреб суспільства, ринку праці та держави у кваліфікованих фахівцях регулюються вимогами Закону України «Про вищу освіту» [1]. Окрім того зазначаємо, що у даному законодавчому акті використовується термін вищий навчальний заклад зі специфічними умовами навчання під яким слід розуміти вищий навчальний заклад державної форми власності, який здійснює на певних рівнях вищої