***Н.Костюк**, студентка 4 курсу спеціальності «Міжнародна інформація» Східноєвроопеського національного університету імені. Лесі Українки*

Науковий керівник: к.. філол. н., доц. кафедри міжнародної інформації СНУ ім. Лесі Українки Карпчук Н.П. (Україна, м.Луцьк)

Транскордонний обмін інформацією як засіб протидії кіберзлочинності

Роботу виконано на кафедрі міжнародної інформації СНУ ім. Лесі Українки

Протягом останнього десятиліття питання що стосуются врегулювання кібернетичного простору втрачають статус «внутрішньодержавних» для багатьох країн. З кожним днем виникають нові загрози, такі як хакерські атаки за політичними чи економічними мотивами, використання мережі терористичними організаціями , злочинними групами чи кібертерористами-одинаками, тому світова спільнота не може не вживати заходів для запобігання таких речей. Кіберзлочинність - це злочинність у так званому «віртуальному просторі» [2].

Занепокоєність світових геополітичних гравців прослідковується кількістю проведених зустрічей , в тому числі і на найвищому рівні. На таких зустрічах вносяться пропозиції прирівнювати кібер - зброю до ядерної зброї та визнати кібер - війни не менш потужними та такими що приносять величезні збитки.

До останнього часу кібербезпеці було приділено не надто багато уваги, допоки вона не стала пріоритетною для більшості країн світу.

Європейська спільнота була змушена подвоїти свої зусилля для того щоб полегшити інформаційний обмін між

силовими відомствами своїх країн-членів, оскільки виникла потреба в ефективних розслідуваннях різноманітних транскордонних злочинів та дотриманні закону та правопорядку, що в свою чергу значно ускладнюється наявністю терористичних атак, як силових, так і кібернетичних. Таким чином активно працюють розвідувальні служби та служби безпеки країн – членів, щоб протидіяти власним загрозам, а також гарантувати безпеку іншим. Стає зрозумілим, що потрібно не лише підтримувати на такому рівні, а й підвищувати ефективність обміну інформацією між силовими структурами, керуючись загальним принципом доступності [1].

Інформацію, що стосується питань правопорядку, яка належить одній країні, потрібно зробити доступною і для іншої країни - члена. В такому випадку виникає потреба пошуку балансу між безпекою та конфіденційністю в обміні інформацією між судовими та силовими структурами країн-членів. Зрозуміло, що цього досягнути нелегко, оскільки тероризм та боротьба з ним є проблемою світового масштабу, та є потужні гравці, які не є членами Європейського Союзу, та які диктують свої правила протистояння. Відсутність єдиного законодавства ускладнює процес захисту даних, які структури використовують у своїх цілях.

Проблема захисту даних стосується не лише судових та силових структур. Серйозні проблеми виникають і в таких випадках обміну персональними даними, коли дві країни гармонізували законодавство щодо обміну персональними даними до систем захисту даних різних міжнародних організацій, або коли одна країна має потужну систему захисту даних, а інша не таку досконалу, або вона взагалі відсутня. Будь-яка міжнародна ініціатива в області захисту даних - чи то Керівні принципи OECD. Конвенція 108 Ради Європи чи Директива ЄС - допускає для своїх країн-учасниць передачу персональних даних тільки в країни з подібним рівнем правового захисту даних. Ось як трактується це

питання в ст. 24 (1) Директиви ЄС 1995 р. про захист персональних даних: "Країни-члени ЄС повинні передбачити у своєму законодавстві те, що передача в якусь третю країну, як на тимчасовій, так і на постійній основі, персональних даних, які піддаються обробці або були зібрані з метою обробки, може мати місце, тільки якщо ця країна забезпечує адекватний рівень захисту " [2].

Це положення Директиви породжує загальні і безперестанні проблеми, яким чином порівнювати (якщо це взагалі можливо) несумірні системи захисту з точки зору їх оцінки перед відправкою даних у цю країну. Якщо передача персональних даних відбувається між публічними секторами обох країн, то тоді оцінити закони країни-реципієнта цілком можливо, оскільки в переважній більшості країн "базовий" закон про захист даних (якщо він існує) поширюється саме на публічний сектор і має, як правило, досить стандартну структуру та зміст. Труднощі можуть мати місце тільки в деяких федеральних країнах, оскільки, хоча на федеральному рівні і прийнято законодавство про захист даних, деякі штати або території можуть його не мати. Набагато складніше прийняти рішення про транскордонну передачу даних між компаніями приватного сектора, оскільки в більшості неєвропейських (і в деяких європейських) країн законодавство про захист даних у приватному секторі відсутнє або знаходиться на явно недостатньому рівні. Потрібне детальне вивчення місцевих законів у таких країнах, щоб адекватно оцінити прийняті в них стандарти захисту персональних даних. Справа ця нелегка, оскільки в багатьох країнах закони не є легко доступними, ясними і очевидними. Такі оцінки рівня правового захисту даних на галузевому рівні або навіть на рівні компаній повинні час від часу переглядатися для того, щоб оцінити що відбуваються зміни, які можуть мати місце [3].

Підводячи підсумки, слід зазначити наступне. Будь-яке рішення на передачу персональних даних за кордон

грунтується на довірі до реципієнта і до правових положень про захист даних, існуючих в країні-імпортері. Існування конкретних законів і органу влади із захисту даних дає певну ступінь впевненості суб'єкту даних і імпортеру даних. Однак бувають випадки, коли оцінити рівень захисту даних в країні-імпортері вельми важко або рівень цей оцінюється як незадовільний, в той час як безпосередній реципієнт даних заслуговує довіри своєю практикою обробки даних і внутрішніми заходами щодо забезпечення захисту та безпеки даних. У таких випадках органи влади щодо захисту даних в країнах-експортерах, як правило, обмежують чи забороняють передачу даних за кордон. Рада Європи, OECD та Комісія ЄС єдині в думці, що в багатьох подібних випадках може бути досягнутий компроміс за допомогою використання прямих договорів про передачу і захист (хоча їх застосування обмежене), а також галузевих або корпоративних Кодексів практики. Проте всі ці заходи "ad hoc", рекомендовані на найближче майбутнє, можуть розглядатися тільки як тимчасове рішення. Вирішення цих проблем на постійній основі ще тільки належить знайти.

Джерела:

1. Castells M. The Information Age: Economy, Society and Culture. – Vol. I-III. – The Power of Identity. – Blackwell, 1996-97. – 352 p.

2. Bell D. The Coming Post-Industrial Society. A Venture in Social Forecasting. – N.Y. Basic Books, Inc., 1973. – 544 p.

3. Cross-border information. [Electronic resource] – Available at : http://www.crossborderinformation.com/