Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК 343.98

Дмитро Володимирович ШВЕЦЬ,
кандидат педагогічних наук, перший проректор Харківського національного університету внутрішніх справ

ДЕРЖАВНІ МЕХАНІЗМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

На сучасному етапі розвитку суспільства все більше відчувається значущість інноваційних процесів, що відбуваються в нашому суспільстві у зв'язку з глобальною інформатизацією. Але разом з позитивними досягненнями, інформатизація супроводжується побічними, негативними явищами криміногенного характеру, до яких відносять комп'ютерну злочинність. Це, безумовно, вимагає негайного створення системи протидії даному різновиду злочинності на державному рівні. Для сучасного суспільства (в період його переходу від індустріального етапу розвитку до нового – постіндустріального, інформаційного) актуальність цієї проблеми не викликає сумнівів. За різними експертними оцінками у всьому світі втрати від діяльності кіберзлочинців складають щорічно від 300 до 800 млрд євро.

На міжнародному рівні у ряді нормативно-правових актів визнано, що кіберзлочинність погрожує не лише національній безпеці окремих країн, але і безпеці людства та міжнародному правопорядку. Стратегія державних підходів та механізмів з поліпшення інформаційних систем повинна сприяти скороченню масштабів кіберзлочинності та створити основні принципи національної політики протидії кіберзлочинності в міжнародному кіберпросторі. Протидія кіберзлочинності в широкому розумінні включає у себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності.

Враховуючи міжнародний характер кіберзлочинності, у боротьбі з нею життєво важливе значення має гармонізація національних законодавств. Проте, гармонізація повинна враховувати регіональні вимоги і можливості. Велике значення регіональних аспектів в здійсненні стратегій боротьби з кіберзлочинністю підкреслює той факт, що багато правових і технічних стандартів було погоджено між країнами світу.

Глобальна програма кібербезпеки заснована на п'яти основних принципах: 1) правові заходи; 2) технічні й процедурні заходи; 3) організаційні структури; 4) створення потенціалу; 5)

міжнародна співпраця. Зрозуміло, що українська система державних механізмів боротьби з кіберзлочинністю повинна використовувати всі ці принципи.

Серед п'яти принципів, при розгляді стратегії боротьби з кіберзлочинністю, ймовірно, правові заходи є найбільш важливими. По-перше, ці заходи вимагають прийняття основних положень кримінального законодавства, що передбачають кримінальну відповідальність за такі дії, як комп'ютерне шахрайство, незаконний доступ, спотворення даних, порушення авторських прав, розповсюдження дитячої порнографії тощо. Механізми й інструменти, необхідні для розслідування кіберзлочинів, можуть істотно відрізнятися від тих, що використовуються для розслідування загальних злочинів. У зв'язку з міжнародним масштабом кіберзлочинності необхідно додатково доробити основи національного законодавства, з тим, щоб мати можливість спільної співпраці з правоохоронними органами за кордоном.

Ефективна боротьба з кіберзлочинністю вимагає розвиненої організаційної структури. Не маючи правильно створеної системи відповідних органів, яка дозволяє уникнути дублювання та чітко розподіляє повноваження, навряд чи можна чекати на комплексне вирішення юридичних, технічних та соціальних аспектів даної проблеми. Кіберзлочинність є глобальним явищем. Для того, щоб мати можливість ефективно розслідувати кіберзлочини, необхідно не тільки гармонізувати законодавство, але й розробити відповідні механізми міжнародної співпраці.

Рівень довіри повинен зрости не лише між державами, але й між приватним і державним секторами. Одним з найбільш важливих елементів в попередженні кіберзлочинів є навчання користувача. Деякі кіберзлочини, особливо ті, які пов'язані з шахрайством типу «спуфінг», як правило, обумовлені не відсутністю засобів технічного захисту, а непоінформованістю або простою безвідповідальністю. Існують різні програмні продукти, що дозволяють автоматично визначати деякі шахрайські веб-сайти, хоча, на жаль, не всі. Попри те, що засоби технічного захисту продовжуватимуть розвиватися і доступні програмні продукти регулярно оновлюватимуться, такі продукти поки ще не можуть замінити інші підходи. Стратегія захисту користувача, що заснована тільки на програмних продуктах, ще не дає гарантії повного захисту користувачів.

Важливу роль відіграє також беззаперечне дотримання встановлених правил і процедур інформаційної безпеки. Наприклад, якщо користувачі знають, що їх фінансові установи ніколи не зв'язуватимуться з ними по електронній пошті з проханням повідомити пароль або деталі банківського рахунку, вони не стануть жертвами фішингу або атаки з метою крадіжки ідентифікації. Навчання користувачів Інтернету скорочує кількість потенційних жертв кіберінцидентів. Держава повинна розробити відповідну інформаційну програму розумної поведінки щодо попередження кіберзлочинності. До її поширення слід долучити громадські кампанії, школи, інформаційні центри і ВНЗ, реалізовуючи приватно-державні партнерства.

Проблема протидії комп'ютерної злочинності – це комплексна проблема. Закони України та інші нормативні документи у сфері кібербезпеки повинні відповідати сучасному рівню розвитку інформаційних технологій. З цією метою необхідно проводити цілеспрямовану роботу з гармонізації й удосконалення законодавства, що регулює поширення інформації в телекомунікаційних мережах. Одним з пріоритетних напрямків є також організація взаємодії і координації зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою, а також розвиток державно-приватного партнерства.

Одержано 01.11.2017