Література:

1. Конвенція Ради Європи про кіберзлочинність: від 21.11.2001 [електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

2. Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» http://zakon2.rada.gov.ua/laws/show/96/2016.

3. Кіберзлочинність у всіх його проявах:види, наслідки та способи боротьби [Електронний ресурс] http://gurt.org.ua/articles/34602/.

4. Кримінальний процесуальний кодекс України//Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88. Редакція від 03.08.2017 р. [Електронний ресурс] http://zakon5.rada.gov.ua/laws/show/4651-17.

5. Наказ Національної поліції України від 10.11.2015 № 85 «Про затвердження Положення про Департамент кіберполіції Національної поліції України».

Деякі аспекти міжнародного співробітництва правоохоронних органів у сфері боротьби з кіберзлочинністю

Косаревська О.В.
кандидат педагогічних наук, доцент,
доцент кафедри кібербезпеки
та інформаційного забезпечення ОДУВС
Шутило С.В.
слухач 2 курсу магістратури
факультету №4 ОДУВС

Сучасні інформаційні технології є новим засобом масової комунікації оскільки вони охоплюють практично всі сфери людської діяльності. Слід відзначити, що технічне удосконалення телекомунікаційних систем глобального зв'язку і спрощення доступу до використання інформаційних технологій веде до трансформації злочинності, яка для реалізації протиправних намірів переміщується у кіберпростір.

Сама мережа інтернет створює існування кіберзлочинності ознаками якої є: висока латентність, за рахунок можливості здійснювати протиправні дії швидко, безконтактно з жертвою, на великій відстані і багаторазово.

Беручи до уваги той факт, що з кожним днем кіберзлочинність зростає та розповсюджується і жодна держава сьогодні вже не спроможна самостійно протистояти цій небезпеці, з'явилася наявна необхідність активізації міжнародного співробітництва у цій сфері.

Огляд сучасної наукової думки, стосовно проблеми міжнародної взаємодії правоохоронних органів у сфері протидії кіберзлочинності, що відбилося у роботах: Бондаренка О.О., Бутузова В.М., Гвоздецької В.В., Глобенко Г.І., Гусева В.О., Лешукової І.В., Літвінова М.Ю та інш., доводить актуальність цієї проблеми, яку, на наш погляд, слід розглядати в наступних аспектах.

1. Оскільки, сьогодні як на міжнародному, так і на національному рівні відсутнє універсальне визначення «кіберзлочинності» чи «комп'ютерного злочину», вкрай необхідним є узгодження термінологічного апарату визначення міжнародної кіберзлочинності, що дозволить більш точно визначити її межі, а також правильно кваліфікувати дії винних осіб.

2. Окремі недоліки в системі міжнародного законодавства стосовно захисту глобальних інформаційних мереж від кібератак відбуваються за рахунок існуючої неузгодженості національних та міжнародних правових актів, стосовно закріплення єдиного правового механізму міжнародної взаємодії правоохоронних органів у забезпеченні трансграничного доступу до інформації щодо суб'єктів транснаціональної кіберзлочинності та комп'ютерного тероризму.

3. Також слід наголосити на відсутність єдиних стандартів та сталих методик по фіксуванню і тимчасовому зберіганню виявлених електронних доказів під час проведення оперативно-розшукових і розвідувальних заходів, що проводяться міжнародними поліцейськими структурами.

Одним із важливих підходів щодо боротьби з кіберзлочинністю у транснаціональному аспекті і розвитку міжнародної співпраці, було створення та спроби стандартизації відповідної нормативно-правової бази, що на теперішній час активно застосовується в багатьох країнах.

На міжнародному рівні першим документом у цій сфері стала «Конвенція про кіберзлочинність», прийнята Радою Європи 23 листопада 2001 р. та Додатковий протокол до Конвенції, направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського і ксенофобського характеру від 28 січня 2003 р.

Так Конвенцією наголошуються спільні дії на національному та міждержавному рівнях з припинення несанкціонованого втручання в роботу комп'ютерних систем, незаконного перехоплення даних і втручання в комп'ютерні системи.

Відповідно цьому всі кіберзлочини Конвенція ділить на чотири види:

- злом комп'ютерних систем;
- шахрайство;
- заборонений контент;
- порушення авторських прав.[1]

При цьому слід констатувати, що Конвенція не надає конкретного визначення, хоча і окреслює коло суспільно-небезпечних діянь, що повинні набути статусу кіберзлочинів на рівні національних законодавств (ратифікована більш ніж 20 країнами), а саме передбачає такі правопорушення, як: незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання у дані, втручання у систему, зловживання пристроями, підробка та шахрайство пов'язані з комп'ютерами.

Важливу роль у боротьбі з кіберзлочинністю відіграють і інші міжнародні угоди в цій галузі, зокрема: рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 року, Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського Союзу та міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект SCB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA).

Сучасна стратегія міжнародної співпраці у сфері протидії комп'ютерної злочинності і пріоритетні напрями її реалізації полягають в укладанні міждержавних угод, організації міждержавної оперативно-розшукової діяльності, прийнятті міждержавного регламенту і вдосконаленні інтеграційних процесів у рамках міждержавних організацій, обґрунтуванні необхідності розробки і прийнятті відповідної комплексної міждержавної програми. Усі інтереси в інформаційній сфері підрозділяються на інтереси особи, держави та суспільства. Сукупність потреб, задоволення яких забезпечує існування і можливість прогресивного розвитку кожного громадянина, суспільства і держави - це частина національних інтересів, без реалізації яких неможливо забезпечити стабільний стан держави і суспільства, а також нормальний розвиток країни як незалежного суб'єкта міжнародних відносин.

Існуючі зараз форми міжнародної співпраці правоохоронних органів у сфері протидії кіберзлочинності мають суттєві недоліки, у зв'язку з відсутністю єдиного підходу у процедурі формування, використання доказової бази у справах про ці злочини, а також у встановленні, розшуку і притягненні до відповідальності кіберзлочинців. Слід погодитись з думкою окремих авторів (Васильєв А.А., Пазинич Т.А., Пашнєв Д.В., Сивухін В.С.), які наголошують на доцільність розширення функцій Управління боротьби з кіберзлочинністю МВС України, стосовно реєстрації в Єдиному реєстрі досудових розслідувань відомостей про кримінальні правопорушення (про які повідомляють представники правоохоронних органів інших країн) та ініціювати початок кримінальних проваджень, що мають транснаціональний характер і зачіпають інтереси нашої держави, суспільства чи окремих громадян. Крім того вони висувають пропозиції щодо об'єднання всіх функцій (крім запитів про екстрадицію або тимчасовий арешт) цього єдиного органу України з координації діяльності цілодобової контактної мережі у сфері розслідування злочинів, пов'язаних з комп'ютерними системами.

На підставі вищевикладеного, на нашу думку, дієвими заходами загальнодержавного рівня по вдосконаленню міжнародного співробітництва у сфері боротьби з кіберзлочинністю слід вважати:

1. Розробку нових механізмів захисту даних глобальних інформаційних мереж від кібератак, шляхом вдосконалення національного законодавства та його імплементації до європейських стандартів.

2. Забезпечення трансграничний доступу правоохоронних органів та міжнародних інституцій по боротьбі із кіберзлочинністю до даних про:

- суб'єктів кіберзлочинів;
- фіксування і тимчасового зберігання виявлених електронних доказів по вчиненню транснаціональної кіберзлочинності, які були виявлені під час оперативно-розшукових і розвідувальних заходів.

3. Розробку та узгодження єдиних стандартів з методики розкриття кіберзлочинів для міжнародних поліцейських структур.

4. Вдосконалення спеціальної професійної підготовки кадрів кіберполіції України, шляхом створення сприятливих умов для залучення іноземних фахівців (ІТ-спеціалістів) в рамках обміну міжнародного досвіду у сфері протидії кіберзлочинності.

5. Забезпечення належного матеріально-технічного оснащення підрозділів кіберполіції, шляхом запровадження системи додаткових матеріальних заохочень спеціалістів у сфері інформаційних систем і технологій за результатами розкриття кіберзлочинів.

Література:

1. Конвенція Ради Європи про кіберзлочинність: від 21.11.2001 [електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575.

2. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності [Електрон-ний ресурс] / В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика). – Вип. 19. – 2008. – С. 240–246. – Ре-жим доступу: http://nbuv.gov.ua/j-pdf/boz_2008_19_28.pdf.

3. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю [Електронний ресурс]/ М. Ю. Літвінов // Право і Безпека. –2014. – № 1(52). – С. 85–89. – Режим доступу: http://pb.univd.edu.ua/?controller=service&action=download&download=17028.

4. Сивухін В. С. Конституційні засади транскордонного доступу як форми міжнародного співробітництва у боротьбі з організованою кіберзлочинністю [Електронний ресурс] / В. С. Сивухін // Боротьба з організованою злочинністю і корупцією (теорія і практика). –2013. – № 1(29). – С. 257–264.- Режим доступу: http://nbuv.gov.ua/j-pdf/boz_2013_1_31.pdf.

Проблема підготовки фахівців кібербезпеки для органів Національной поліції

Мирошниченко В.О.
кандидат технічних наук, доцент,
доцент кафедри економічної та
інформаційної безпеки Дніпропетровського
державного університету внутрішніх справ
Матвійчук І.В.
курсант 4 курсу факультету підготовки
фахівців для органів досудового
розслідування Дніпропетровського
державного університету внутрішніх справ

На сьогоднішній день наше існування неможливе без тісної взаємодії з кібертехнікою, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людей і держави. Але людство, поставивши собі на службу телекомунікації і глобальні комп'ютерні мережі, не передбачало, які можливості для злочинних діянь створюють ці технології. На сьогодні жертвами злочинців, що діють у віртуальному просторі, можуть стати не лише люди, але і цілі країни. При цьому безпека тисяч користувачів інтернет простору залежна від декількох злочинців. Кількість злочинів, що здійснюються в кіберпросторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, по оцінках Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті.

Небезпека кіберзлочинності як для всього світу, так і для України визнають і вітчизняні правоохоронні органи, як найбільш актуальну проблему. Так, на наш погляд, кіберзлочинність (злочинність у сфері високих технологій) в даний час є однією з найбільш серйозних погроз національній безпеці України в інформаційній сфері.

Створення підрозділу з висококваліфікованими працівниками у сфері кібербезпеки є, на нашу думку, однією з актуальних проектів, так як дана сфера є найбільш незахищеною і привертає увагу багатьох осіб, які посягають на приватне життя та інші блага, пов'язанні з інтернет простором.

Метою роботи є аналіз указу президента та висвітлення проблеми недостатньою підготовки фахівців, діяльність яких пов'язана з гарантуванням безпеки у кіберпросторі.

Першим кроком, у розвитку безпеки громадян та захисту їх конфіденційної інформації, було законодавче закріплення указу президента станом на 15 березня 2016 року, а саме "Стратегія кібербезпеки України", даний указ закріплює забезпечення безпеки у кіберпросторі, шляхом застосування сукупності правових, організаційних, інформаційних заходів, що, безпосередньо,