http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 11.04.2006, №68

23. Про Стратегічний оборонний бюлетень України. [Електронний ресурс]. – Доступний з http:// zakon2.rada.gov.ua/laws/show/ 771/2012/print1361272038412688

24. Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-XII. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 01.12.1992.

25. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgd c-2007-r.pdf.

26. Соловйов С.Г. Інформаційна складова державної політики та управління : монографія / С.Г. Соловйов, О.Є. Бухтатий, Ю.В. Нестеряк та ін.; за заг. ред. Н.В. Грицяк; Нац. акад. держ. упр. при Президентові України. – К. : Вид-во К.І.С., 2015. – 319 с.

27. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.

Попередження та розслідування кіберзлочинів

Мельникова Е.О.
студентка 1 курсу ЮД-748
юридичного факультету ДДУВС
Гавриш О.С.
науковий керівник, викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Станом на сьогодні, жертвами кіберзлочинців можуть стати не лише люди, а і цілі держави. За оцінками Інтерполу, темпи зростання злочинності у цій сфері, наприклад, у глобальній мережі Інтернет, є найшвидшими на планеті. Кількість злочинів, що мають прояв у цієї галузі, зростає пропорційно кількості користувачів комп'ютерних мереж. Сьогодні у світі дослідження проблем боротьби зі злочинами в

кіберпросторі приділяється значна увага, що обумовлено об'єктивними процесами розвитку інформаційно-телекомунікаційних технологій і їх впровадженням у різні сфери громадської діяльності. 27.06.2017 о 11:00 проти України було розпочато масові кібератаки з використанням модифікованої для України версії вірусу "wannacry" – "криптолокера".[1] Ця кібератака була наймасштабнішою за всю історію України.

На 2016 рік в Україні було зафіксовано 1018 кіберзлочинів. З яких найбільша кількість здійснювалася у Києві. Проте на 2017 рік ця кількість значно зменшилася – 705. Найбільша кількість – у Чернівецькій області.[2]

Кіберзлочини - вкрай складна і комплексна сфера, тому дослідники шкідливих додатків часто повинні виступати експертами в розглядах високотехнологічних злочинів. Під час розслідування багато індикаторів можуть пролити світло на особистість кіберзлочинця. Деякі частини шкідливого коду можуть включати псевдонім лиходія або бути запрограмовані в «фірмовому стилі». Це може стати відправною точкою в пошуку злочинця. Дослідники використовують псевдоніми, або інші натяки з вірусу, або поштову адресу, асоційований з одним з доменів, які беруть участь в атаці, а потім прочісують спільноти на кшталт Facebook, Twitter, YouTube, вікіпедію та інші джерела користувацького контенту в надії на те, що злочинець десь то використовував ті ж псевдонім або пошту. Безумовно потрібно гармонізувати закони в різних країнах. Злочинці знають, де закони по їх галузі м'якші і що робити, щоб не потрапити на замітку і уникнути арешту.

Попередження кіберзлочинів складається зі стратегій і заходів, спрямованих на зниження ризику вчинення злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і усього суспільства. У більшості випадках стратегії протидії кіберзлочинності є невідокремною частиною стратегій забезпечення кібербезпеки. Обстеження, проведені у більш розвинутих країнах, показують, що більшість індивідуальних користувачів Інтернету нині вживають основні запобіжні заходи.

Хоча в половині країн діють закони про захист даних, які передбачають вимоги відносно захисту і використання персональних даних, проте в деяких – зроблені виключення для цілей розслідувань правоохоронних органів, згідно з якими постачальники послуг Інтернету та постачальники електронних засобів зв'язку зобов'язані зберігати певні дані користувачів упродовж певного терміну.

Фахівці виділяють такі елементи організації діяльності правоохоронних органів у глобальних інформаційних мережах:

– вивчення та оцінка обстановкив мережах;

– здійснення оптимальної розстановки сил і засобів, забезпечення взаємодії;

– управління, планування і контроль; координація дій суб'єктів правоохоронних органів.[3]

Питання пошуку шляхів протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги міжнародної спільноти. На даний час Будапештська конвенція є фундаментом для розробки законодавства у боротьбі з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства.

Будапештська Конвенція вимагає від держав:

- криміналізувати атаки на комп'ютерні дані і системи (тобто незаконний доступ, нелегальне перехоплення, втручання в дані, втручання у систему, зловживання пристроями), а також правопорушення з використанням комп'ютерів (підробка і шахрайство), правопорушення, пов'язані зі змістом (дитяча порнографія) та правопорушення у сфері авторських і суміжних прав;

- вдосконалювати законодавство для того, щоб компетентні органи змогли проводити розслідування кіберзлочинів і зберігати електронні докази найефективніше, включаючи термінове збереження комп'ютерних даних, термінове збереження і часткове розкриття даних про рух інформації, обшук і арешт комп'ютерних даних, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації;

- розширювати міжнародне співробітництво з іншими країнами-учасницями Конвенції через загальні (екстрадиція, взаємна допомога добровільне надання інформації тощо) і спеціальні заходи (термінове збереження та розкриття збережених даних про рух інформації, взаємна допомога щодо доступу до комп'ютерних даних, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж тощо). [4]

Протидіяти кіберзлочину можна, наприклад:

1.Внести зміни до КК України з посиленням відповідальності за злочин у сфері комп'ютерних та інформаційних технологій;