МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

МАТЕРІАЛИ
Всеукраїнської
науково-практичної конференції

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

21 жовтня 2016 року
м. Одеса

Міністерство внутрішніх справ України

Одеський державний університет внутрішніх справ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали

Всеукраїнської науково-практичної конференції

21 жовтня 2016 року

Одеса
ОДУВС
2016

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)
К 38

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № 4 від 03 листопада 2016 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ.
К38 конф., м. Одеса, 21 жовтня 2016 р. – Одеса : ОДУВС, 2016. – 232 с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на всеукраїнську науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 21жовтня 2016 року.

У матеріалах конференціїприділено увагу актуальним теоретичним та практичним проблемамзабезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем та технологій в боротьбі з кіберзлочинністю та надано обгрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникамправоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантамвищих навчальних закладів.

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)

ISBN 678-717-7020

.

Нормативно-правові засади використання високотехнологічних і програмних інструментів у боротьбі з кіберзлочинністю

Лефтеров Л.В.
старший інспектор Департаменту Кіберполіції НП України,
ад'юнкт кафедри кримінального права та кримінології ОДУВС

Бабенко А.М.
доктор юридичних наук, доцент
професор кафедри кримінального права і кримінології
Одеського державного університету внутрішніх справ

Темпи інноваційного розвитку при сьогоденному змаганні технологій дуже високі. Кожен день розробляється більше 100 тисяч нових зразків шкідливого програмного забезпечення. За деякі шкідливі програмні модулі сплачуються суми, які перевищують мільйон доларів. За оцінкою Центра стратегічних і міжнародних досліджень (Center for Strategic and International Studies) збиток від кіберзлочинності для світової економіки становить понад 445 мільярдів доларів на рік[3].

Згідно з висновками звіту організації, які хочуть проявляти пильність, повинні бути готові виявити будь-яку атаку. Швидка мобілізація включає в себе раннє визначення напряму дії загрози і причини атаки. Також швидкі дії, кваліфіційні навички та вміння використовувати у своїй діяльності високотехнологічні і програмні інструменти повинні бути присутніми у працівника підрозділів боротьби з кіберзлочинністю.

Розділ II Конституції України з метою захисту прав і свобод громадян, забезпечує таємницю листування, недоторканність особистих даних, заборону збирання особистих даних [1, ст. 21-29].Однак вказані права – виключають можливість швидкого реагування за тяжкими кіберзлочинами та особливо тяжкими злочинами загального характеру в яких використовуються електронно обчислювальні мережі.

Основними принципами якісного та результативного реагування у зазначених вище випадках, є виявлення «гарячих слідів», що були залишені зловмисником. Основним фактором отримання електронної інформації є порядок повноцінного аналізу і упорядковування відомостей наданих потерпілою стороною. З інцидентами у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, відповідальність за які передбачена Розділом 16 Кримінального кодексу України, одним з основних доказових чинників є результати запису інформації про події з об'єктами (в рамках комп'ютерної мережі, або з автоматизованою системою). Цей процес також називається аудитом, дані про який вкладаються системою у файл с записами про події у хронологічному порядку (файл реєстрації, протокол, журнал або лог-файл).

Лог-файли можуть містити вичерпну інформацію про:

- загальні дані про дії з ядром системи (контроль доступу програм в мережу);
- завантаження системи (зберігає основні системні події, журнал операційної системи);
- дані про звернення до сервера, інформацію щодо помилок веб-сервера (логи веб-сервера);
- запити до баз даних, помилки сервера (логи сервера баз даних);
- спроби входу в панель, поновлення ліцензії та панелі, статистику використання ресурсів сервера (логи хостингової панелі);
- дані щодо всіх відправлених і доставлених повідомленнях, помилки поштового сервера (логи поштового сервера);
- дані щодо виявлення шкідливого програмного забезпечення у системі (журнал антивірусної програми).

З нормативно-правової точки зору, аналізування наданих протоколів, не є порушенням процесуального законодавства, а навпаки на етапі первинної перевірки факту, надає змогу визначити безпосередню кваліфікацію кримінального правопорушення [4, ст. 16].

Використання програмних та високотехнологічних інструментів для аналізування лог-файлів є невід'ємною частиною якісного розкриття кіберзлочинів. Насамперед, слід зазначити, що технічні характеристики файлів журналу мають формат тексту або таблиць, що дозволяє у своїй діяльності використовувати комп'ютерні текстові редактори та пакети офісних додатків, з функцією сортування і пошуку даних.

Отриману в ході аналізу електрону інформацію слід використовувати для подальшого збору доказів в рамках кримінального провадження. Частіше за все при пошуку осіб використовуються інформація про IP-адреси.

IP-адреса це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах [5, ст. 113].Аналізування IP-адрес або доменних імен Веб-сайтів здійснюється за допомогою вільних сервісів які працюють за Інтернет протоколами «WHOIS». Сервіси WHOIS використовується для запитів до бази даних, щодо визначення власника доменної зони, отримання відомостей про IP-адресу, або автономного системного номера в Інтернеті. Згідно вимог ICANN (Internet Corporation for Assigned Names and Numbers - міжнародна некомерційна організація, щодо регулювання питань, пов'язаних з доменними іменами, IP-адресами і іншими аспектами функціонування Інтернету) та «Угоди про акредитацію реєстраторів» від червня 2013 року, в рамках реєстрації доменних імен та IP-адрес в WHOIS, реєстратор повинен представити, або розмістити в базі даних реєстру наступні елементи даних:

- Ім'я реєстратора;
- найменування оператора або провайдера (щодо належності IP-адрес);
- контактні дані реєстратора або оператора (провайдера);
- первісна дата створення реєстраційної записи;
- дата закінчення терміну реєстрації;
- найменування та поштову адресу власника зареєстрованого імені;
- ім'я, поштову адресу, адресу електронної пошти, номер телефону, а також (за наявності) номер факсу контактної особи з технічних питань для зареєстрованого імені;
- ім'я, поштову адресу, адресу електронної пошти, номер телефону, а також (за наявності) номер факсу контактної особи з адміністративних питань для зареєстрованого імені [6].

Слід зазначити, що до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини [2, ст. 21].Аналіз та збирання цифрової інформації у вигляді IP-адрес не є конфіденційними даними про фізичну особу. Також інформація не є конфіденційною, якщо особа самостійно надала згоду на її опублікування та обробку. У цьому випадку якісним програмними інструментами виступають самостійно сформовані бази даних загально доступних соціальних мереж.

Подібних масиви даних, також можуть нести в собі помилкову або неправдиву інформацію, тому важливо використання у своєї діяльності все більших сервісів та програмних інструментів що можуть допомоги у боротьбі з кіберзлочинністю. Високотехнологічні і програмні інструменти можуть застосовуватись на всіх етапах кримінального процесу та використовуватись у якості доказової бази. Неодмінним фактором долучення отриманих відомостей у якості доказів до кримінального провадження є їх допустимість. Саме в цьому випадку підготовка усіх даних повинна проводитись згідно чинного законодавства.

Література:

1. Конституція України / Відомості Верховної Ради України від 23.07.1996 — 1996 р.;
2. Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, N 48);
3. Report: Cybercrime and espionage costs $445 billion annually [Електронний ресурс] // Washingtonpost. – 2014. – Режим доступу до ресурсу: https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html;
4. Юрасов А.В. Основы электронной коммерции / А. В. Юрасов., 2008. – 480 с. – (Телеком);
5. Комп'ютерні мережі / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.;
6. Соглашение об аккредитации регистраторов [Електронний ресурс] // icann. – 2013. – Режим доступу до ресурсу: https://www.icann.org/resources/unthemed-pages/approved-with-specs-2013-10-31-ru

ЗМІСТ

ПЛЕНАРНЕ ЗАСІДАННЯ

СЕКЦІЯ 1
ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

СЕКЦІЯ 2
АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

СЕКЦІЯ 3
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

СЕКЦІЯ 4
ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

Наукове видання

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали
Всеукраїнської науково-практичної конференції

21 жовтня 2016 року

Підписано до друку 03.11.2016.Формат 60х90/8. Папір офсетний.
Гарн. «Times New Roman» Друк цифровий. Ум. друк .арк. 26,1.
Наклад 500 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.
тел. 0487024884; 0949547884 email – ndrvv1@gmail.com