Співробітники поліції знають кримінальний закон, а також основи збору доказів і питання передачі правопорушників правосуддю. Технічний персонал орієнтується в комп'ютерах і мережах, їхній роботі, вміє відслідковувати інформацію в них. Кожний має свою "половинку ключа" до нанесення поразки кіберзлочинцям. Тому основною метою держави повинне бути з'єднання цих двох суб'єктів, аби показати, як вони можуть і повинні працювати разом, захищаючи від кіберзлочинів, припиняючи і попереджаючи їх, залучаючи до суду осіб, що використовують сучасні технології для заподіяння шкоди громадянам, організаціям, бізнесу і суспільству. Насамперед, виявлення, попередження і припинення злочинів в інформаційно-телекомунікаційній сфері і сприяє забезпеченню інформаційної безпеки України.

Література

1. Шиндер Д.Л. Киберпреступность: перед лицом проблемы. - www.crime-research.org.
2. Мирошников Б.Н. Борьба с киберпреступлениями - одна из составляющих информационной безопасности Российской Федерации. - www.crime-research.org.
3. Калюжний Р.А., Цимбалюк В.С. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю. - www.crime-research.org.
4. Інформаційна безпека: сутність та проблеми (матеріали круглого столу). - Запоріжжя,1998.

КОМПЛЕКСНИЙ ПІДХІД ДО БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В ЄВРОПІ

В.Г. Пядишев
кандидат технічних наук, доцент
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету нутрішніх справ

Боротьба з транскордонною злочинністю, яка зачіпає інформаційно-комунікаційні мережі (кіберзлочинність) є одним з пріоритетів внутрішньої стратегії безпеки ЄС. Щоб протистояти так званим кібер-атакам в безмежному просторі, Європейський Союз і Рада Європи розробили загальні стратегії, оперативні заходи та законодавство.

Злочини за рамками національних кордонів.

Питання національної безпеки.

Інтернет відкрив інформаційні потоки, але також зробив можливим цілий ряд нових транснаціональних злочинів. Злочинці можуть поставити під загрозу безпеку національних держав і / або цивільних свобод їхніх громадян.

Організовані злочинці використовують кіберпростір, щоб викрадати кошти або вчиняти шахрайство. Вони також проникають в комп'ютерні мережі з метою крадіжки даних або комерційної таємниці, або знищити документи. Кіберзлочинність може пошкодити основну інфраструктуру, від якої залежить суспільство, що впливає на

здоров'я, безпеку, та й інфраструктуру, яка життєво важлива для економічного і соціального добробуту (наприклад, електростанції, транспортні мережі, урядових мережі).

Міжнародний захист.

Першим глобальним документом, спрямованим на запобігання дій, спрямованих проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і комп'ютерних даних стала Будапештська конвенція 2001 р [1], розроблена за сприянням Ради Європи. Цей юридичний документ спрямований для полегшення виявлення, розслідування, криміналізації і переслідування такої діяльності як на внутрішньому, так і на міжнародному рівнях. Зазначену Конвенцію було доповнено Протоколом про акти ксенофобії і расизму, вчинені за допомогою комп'ютерних систем.

Стратегічний та оперативний підхід ЄС.

ЄС продемонстрував свій підхід до боротьби з кіберзлочинністю заходами стратегічного, законодавчого та оперативного рівнів.

На стратегічному рівні Стокгольмська програма 2009 містить низку заходів з протидії кіберзлочинності. За "Оцінкою Європолом загроз Серйозні і організованою злочинності - 2013" (SOCTA) [2] вважається, що кіберзлочинність — це загроза, яка постійно зростатиме для ЄС у вигляді великомасштабних порушень даних, онлайнового шахрайства і сексуальної експлуатації дітей, одночасно рухома жаданням наживи кіберзлочинність стає засобом забезпечення інших видів злочинної діяльності. 6-7 червня 2013 "Рада юстиції та внутрішніх справ" визначила кіберзлочинність, як один з дев'яти пріоритетів ЄС у боротьбі з серйозною і організованою злочинністю між 2014 і 2017 рр. Висновки Ради від 25 червня 2013 року [3] допомагають у формуванні Стратегії Кібербезпеки ЄС , а також загальної стратегії ЄС в цій галузі.

На оперативному рівні, після створення Європейської мережі та Агентства інформаційної безпеки (ENISA) [4] у 2004 році було створено Європейський центр з кіберзлочинності (EC3) [5]. Розташований в Європолі, EC3 покликаний стати головним центром в боротьбі ЄС проти кіберзлочинності, який надаватиме підтримки державам-членам і установам Європейського союзу. Він почав свою діяльність в січні 2013 року. Кіберзлочинність стала також одним із пріоритетів "Механізму взаємної оцінки ЄС" по боротьбі з організованою злочинністю: потенціал всіх держав-членів в цій області розглянуто на сьомому раунді оцінювання, починаючи з кінця 2014 року.

Директива "кібер-атаки".

На законодавчому рівні по боротьбі з кіберзлочинністю було здійснено ряд заходів, наприклад, таких, як "Директива-2011" [6] по боротьбі з сексуальним насильством і сексуальною експлуатацією дітей та дитячої порнографією (для інтегрування до національного законодавства в державах-членах до 18-грудня 2013). Особливо актуальною є "Директива-2013" про атаки на інформаційні системи [7], яка замінила "Рамкове рішення Ради 2005" і мала бути інтегрована до 4 вересня 2015 р.. Ця Директива встановлює мінімальні правила, що стосуються визначення кримінальних правопорушень у цій галузі і санкції щодо осіб, визнаних винними у них. Основні злочини, визначені в Директиві, це незаконний доступ до інформаційних систем, незаконне втручання в системи або дані, а також незаконне перехоплення передачі даних. Зокрема, більш суворі кримінальні санкції вимагаються за так звані "ботнетні" атаки [8], при яких велика кількість комп'ютерів заражаються для того, щоб управляти ними віддалено для виконання завдань в автоматичному режимі без відома користувача. Отже,

масштабні кібер-атаки можуть швидко поширюватися через Інтернет. Штрафи також можуть бути накладені на юридичних осіб, таких, як компанії, в разі виявлення злочинних дій їм на користь. Проте Директива має на меті збалансований підхід — з уникненням можливої надмірної криміналізації.

Оперативна співпраця та законодавство.

Директива також покращує оперативну співпрацю між національними правоохоронними службами держав-членів і відповідними установами ЄС (Євроюст, Європол та його Європейський центр по боротьбі з кіберзлочинністю, а також ENISA). Держави-члени повинні в межах восьми годин відповідати на надзвичайні запити, пов'язані з кібер-атаками. На основі інформації, що надаватиметься державами-членами, установи ЄС проводитимуть оцінку загроз і стратегічний аналіз кіберзлочинності. Всі такі заходи повинні також відповідати чинному законодавству ЄС про недоторканність приватного життя і електронного зв'язку та захист інформації, що є невід'ємною частиною комплексного підходу до ефективної протидії кіберзлочинності.

Директива "NIS".

З метою формування нової стратегії ЄС щодо кіберзлочинності, Європейська комісія в лютому 2013 року запропонувала директиву про заходи щодо забезпечення високого загального рівня мережевої та інформаційної безпеки (NIS) [9] по всьому Союзу. Завдяки взаємозв'язку мережевих та інформаційних систем, значні перебої їх в одній державі-члені може вплинути на інші держави-члени і Союз в цілому. Стійкість і стабільність мережевих та інформаційних систем, а також безперервність основних послуг мають важливе значення для нормального функціювання внутрішнього ринку, зокрема, для подальшого розвитку єдиного цифрового ринку. Ця директива вимагає, щоб всі держави-члени створили “Команди реагування на комп’ютерні надзвичайні ситуації” (CERT) [10] і прийняли національні стратегії NIS та плани співробітництва. В якості основних інновацій, запропонована директива вимагає обов'язкового повідомлення з боку операторів ринку про інциденти, які мають істотний вплив на безпеку основних послуг.

На основі доповіді Комітету з внутрішнього ринку і захисту прав споживачів (доповідач Andreas Schwab, ЄНП, Німеччина) у березні 2014 року Європейський парламент проголосував за внесення змін до запропонованої директиви. Після цього новий законодавчий орган матиме завдання забезпечити угоду з Радою щодо остаточної формі директиви.

Кіберзлочинність і вплив одкровень Сноудена.

На стратегію ЄС з кібер-безпеки також вплинуть підсумки розслідування Європарламентом одкровень по справі Едварда Сноудена. Згідно зі звітом, прийнятим на пленарному засіданні в березні 2014 року на підставі розслідування, проведеного Комітетом з громадянських свобод, юстиції та внутрішніх справ [11], кібер-стратегія ЄС повинна бути розширена, щоб захистити ЄС від можливих зловмисних намірів зовнішніх держав і зміцнити ІТ-безпеку та відмовостійкість ІТ-систем. Отже, мандат Європолу має бути посилений, щоб він дозволяв почати свої власні розслідування у випадку підозри шкідливої атаки на мережі та інформаційні системи. ЄС повинен, однак, уникати змін до статті 32 згаданої Конвенції Ради Європи про кіберзлочинність. Останнє робить транскордонний доступ правоохоронних органів до серверів і комп'ютерів, розташованих в інших юрисдикціях, юридично можливим без багатосторонніх угод та інших документів про співпрацю в правоохоронній галузі. Крім того, Комісія, ENISA та органи Європи зі

стандартизації мають розробити мінімальні стандарти щодо безпеки і конфіденційності та керівні принципи для ІТ-систем, мереж і послуг, включаючи послуги хмарних обчислень, щоб краще захистити особисті дані громадян ЄС та цілісність всіх ІТ-систем. Сполучені Штати закликаються приєднатися до Конвенції Ради Європи [12] про захист фізичних осіб стосовно автоматизованої обробки персональних даних (Конвенція 108), так само, як вони приєдналися до Конвенції про кіберзлочинність 2001, зміцнюючи тим самим загальну правову основу трансатлантичних відносин в цій галузі.

Література

1. Convention on Cybercrime. Details of Treaty No.185 // Council of Europe Treaty Office. Reference ETS No.185. Entry into Force 01/07/2004 [Електронний ресурс]. – Режим доступу: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

2. Serious and Organised Crime Threat Assessment (SOCTA) [Електронний ресурс]. – Режим доступу: https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment

3. Council Conclusions and recommendations of 25 June 2013 [Електронний ресурс]. – Режим доступу: http://www.google.ru/url?url=http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/genaff/137614.pdf&rct=j&q=&esrc=s&sa=U&ved=0ahUKEwjC4t76jqzQAhUBWywKHQ8fBJoQFggTMAA&usg=AFQjCNHWKLcrlNeHbjepWMAb9CATMxTE_Q

4. European Union Agency for Network and Information Security // From Wikipedia, the free encyclopedia [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/European_Union_Agency_for_Network_and_Information_Security

5. European Cybercrime Centre // From Wikipedia, the free encyclopedia [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/European_Cybercrime_Centre

6. Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA

7. directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

8. Ботнет // Материал из Википедии — свободной энциклопедии [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Ботнет

9. Network Information Service // Материал из Википедии — свободной энциклопедии [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Network_Information_Service

10. Компьютерная группа реагирования на чрезвычайные ситуации // Материал из Википедии — свободной энциклопедии [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Компьютерная_группа_реагирования_на_чрезвычайные_ситуации

11. European Parliament Committee on Civil Liberties, Justice and Home Affairs // From Wikipedia, the free encyclopedia [Електронний ресурс]. – Режим доступу:

https://en.wikipedia.org/wiki/European_Parliament_Committee_on_Civil_Liberties,_Justice_and_Home_Affairs

12. Convention for the protection of individuals with regard to automatic processing of personal data // From Wikipedia, the free encyclopedia. – Режим доступу: https://en.wikipedia.org/wiki/Convention_for_the_protection_of_individuals_with_regard_to_automatic_processing_of_personal_data

ЕКОНОМІЧНА КІБЕРНЕТИКА

Пекарський С.С.
студент 3-го курсу навчально-наукового
інституту фінансів економіки та менеджменту
Полтавського національного технічного університет ім. Ю. Кондратюка

Пекарський С.П.
кандидат юридичних наук
доцент кафедри спеціальних дисциплін та адміністративної діяльності
Донецького юридичного інституту МВС України

Розповсюдження інформаційних технологій, комп'ютерних систем охопило всі галузі економічного розвитку України. Своєю чергою економічна кібернетика визначається як науковий напрям що використовує ідеї, методи й засоби кібернетики для вивчення економічних систем [1]. Окрім того ми погоджуємося з думкою, що економічна кібернетика вивчає економіку та її структурні й функціональні елементи. Також щоб знайти оптимальні рішення для управління ними існують три основні напрями розвитку економічної кібернетики [1]:

- теорія економічних систем і моделей – розробка методологічного системного аналізу й моделювання економічних процесів,
- теорія інформаційних технологій в економіці – дослідження в економічних системах технологій збирання, накопичення, зберігання й обробки інформації,
- теорія систем управління в економіці – вдосконалення ефективності економічних систем через поліпшення продуктивності управлінської праці з використанням можливостей технічних засобів обробки інформації.

Отже ми приходимо до висновку, що економічна кібернетика досліджує процеси управління економікою країни народним господарством, галуззю, районом, виробничим комплексом, цехом дільницею та ін. [1].

Враховуючи значимість економічної кібернетик в розвитку правових явищ сучасного суспільства нам необхідно визначити місце її в управлінській діяльності. Отже економічна кібернетика як напрямок економічної думки, який продовжує самостійно розвиватися, поєднує в собі розвиток знань про економіку й управління в сполученні з розвитком економіко-математичних методів дослідження й інформаційно-комунікаційних технологій. Своєю чергою це визначає місце економічної кібернетики в сучасних методах і формах управлінської діяльності на всіх рівнях – від макро- до мікроекономічних процесів. Перш за все економічна кібернетика пов'язана із застосуванням обчислювальної