УДК 341.4

СВІТОВІ ТЕНДЕНЦІЇ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Йона О.О., Казакова Н.Ф.

GLOBAL TRENDS FIGHT CYBERCRIME

Yona O., Kazakova N.

Показується, що сформована в світі ситуація з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами та побудову моделі, спрямованої на забезпечення кібербезпеки країни.

Ключові слова: *кіберзлочинність, кібербезпека, кіберзагроза, тенденції, статистика.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими та практичними завданнями. Як показано в [1], широке використання сучасних інформаційних технологій у державних та недержавних структурах, а також у суспільстві в цілому, висуває вирішення проблем інформаційної безпеки в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини.

Постановка проблеми у загальному вигляді. Залучення комп'ютерних технологій до все більшої кількості сфер діяльності держави, наближає Україну не тільки до світових стандартів та тенденцій, але й до їх негативних наслідків. Економіка, логістика та безпека країни все більше залежать від технічної інфраструктури та її захищеності. Для підвищення ефективності боротьби з кіберзлочинністю, Україна досить давно почала відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Світовий досвід у цій області закликає до створення системи глобального обміну інформацією. Як свідчать результати досліджень та численних суспільних опитувань, питання кіберзлочинності непокоїть не тільки державу в цілому, а й кожного окремо взятого її мешканця. У цьому сенсі вивчення досвіду зарубіжних країн, які мають достатній досвід боротьби з кіберзлочинами, було б достатньо актуальним.

Аналіз останніх досліджень та публікацій. Питання, винесене в заголовок статті, зрізних точок зору вивчається багатьма вченими. Особлива увага проблемі приділяється у західних країнах. Вивчення вітчизняними вченими та дослідниками стану наукової розробленості проблем співпраці та взаємодії правоохоронних органів різних держав у боротьбі з кіберзлочинністю, також не стоїть на місці. Втім, їх дослідження свідчить, що на сучасному етапі спеціальні дослідження з проблем кіберзлочинності є не достатньо активними. Проте необхідно відзначити, що окремі аспекти такої співпраці розглядалися в наукових роботах Ю. М. Батуріна, П. Д. Біленчука, В. Б. Вєхова, В. О. Голубєва, М. Д. Діхтяренко, Б. Х. Толеубекова і деяких інших вчених [1]. Т.ч., ***метою статті***, зважаючи на праці вказаних вчених та на матеріали, що доступні в мережі Інтернет, є стисле узагальнення світових тенденцій боротьби з кіберзлочинністю.

Виклад основного матеріалу. У 2012 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту про стан світової кібербезпеки [2]. Звіт, який був складений брюссельською компанією Security & Defence Agenda, вперше повідомив у відкритих джерелах про поточну готовність до кібератак інформаційних систем різних країн. Звіт був складений спеціально для того, щоб допомогти урядам та організаціям зрозуміти, наскільки вони кібернетично захищені в порівнянні з іншими країнами.

Базою для складання звіту були дослідження групи експертів у складі 80 фахівців з двадцяти семи країн. Вони надали компанії Security & Defence Agenda офіційні висновки про поточну готовність до кібератак інформаційних систем різних країн – див. далі.

Крім групи експертів, до дослідження були залучені представники 250 світових лідерів у галузях IT-технології, інформаційної безпеки, захисту інформації, боротьби з кіберзлочинністю та ін. з 21 країни. Технологією дослідження передбачалося та було виконане їх анонімне опитування. За результатами роботи групи експертів та після обробки результатів опитування, Security & Defence Agenda провела ранжування та встановила рейтинг по 5-бальній системі. При цьому була досліджена поточна готовність до кібератак інформаційних систем 23 країн. Стан готовності для окремих країн був продемонстрований на прикладі рейтингу McAfee, який там використовується у якості основного засобу боротьби з кіберзлочинами – табл. 1.

Таблиця 1

Стан готовності до кібератак інформаційних систем окремих країн

Рейтинг	Країна
5	–
4,5	Фінляндія, Ізраїль, Швеція
4	Данія, Естонія, Франція, Німеччина, Нідерланди, Іспанія, Великобританія, США
3,5	Австралія, Австрія, Канада, Японія
3	Китай, Італія, Польща, Росія
2,5	Бразилія, Індія, Румунія
2	Мексика

Найвищий результат, тобто 4,5 бали, було поставлено всього 3 країнам, які мають досить невелику площу: Швеції, Ізраїлю та Фінляндії. Ще 8 країн, включаючи США, Великобританію, Францію та Німеччину, отримали друге місце з 4 балами. Росія та Польща зайняли 4 місце з 3-бальним результатом. З тих даних звіту Security & Defence Agenda, неясно, чи були виставлені якісь бали для України.

Зі звіту Security & Defence Agenda можна виділити результати опитування експертів. Статистика свідчить про наступне:

– 57% світових експертів вважають, що в кіберпросторі відбувається «гонка озброєнь»;

– 36% вважають, що кібербезпека є важливішою проблемою, ніж протиракетна оборона;

– 43% визначили кібернетичне створення перешкод або нанесення збитків життєво важливим інфраструктурам, як найбільшу загрозу з катастрофічними економічними наслідками;

– 45% респондентів вважають, що кібербезпека настільки ж важлива, як безпека кордонів держави;

– 56% відмічають, що існує необхідність вирішення проблеми підготовки кваліфікованих кадрів з питань боротьби з кіберзлочинністю.

Звіту Security & Defence Agenda містить велику кількість зауважень від групи експертів. Найбільш суттєві з них, це:

– необхідність глобального обміну інформацією в режимі реального часу;

– приватному та державному секторам потрібні фінансові стимули для поліпшення кібернетичної безпеки;

– правоохоронним органам по боротьбі з транскордонною кіберзлочинністю потрібно більше повноважень;

– необхідна методична доробка та впровадження у технології боротьби з кіберзлочинністю кращих практик інститутів міжнародної безпеки;

– існуюче дипломатичне упорядкування глобальних кібердомовленостей повинне стати більш адресованим;

– для допомоги громадянам потрібно удосконалити та розширити мережу кампаній з інформування населення про методи захисту від кібератак.

Практично всі фахівці кожної з 27 країн, які були опитані в ході складання звіту, одностайно зійшлися у тому, що для підвищення ефективності боротьби з кіберзлочинністю необхідний глобальний обмін інформацією. Крім того, всі вони відзначили необхідність не просто забезпечення обміну інформацією, а саме його оперативність та швидкість у прийняті управляючих рішень.

Європейське агентство з мережевої та інформаційної безпеки (англ.: *European Network and Information Security Agency* – ENISA) у своїй «Програмі надійності та захисту ключової інформаційної інфраструктури» (англ.: *Cisco International Internship Program* – CIIP), як і експерти, які були залучені Security & Defence Agenda, також наполягає на необхідності налагодження співпраці з метою гарантій узгодженості характерних методик кіберборотьби [3].

На сьогоднішній день у багатьох зарубіжних країнах налагоджена система співробітництва та обумовлена необхідність обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністб на ключові позиції.

Для України така тенденція є, в цілому, позитивною: поки власна стратегія щодо захисту кіберпростору тільки розробляється, надзвичайно цінною є можливість ознайомлення з досвідом країн, які працюють в зазначеному напрямку не перший рік. І хоча загальний вигляд такої стратегії може сильно варіюватися залежно від політики та технічних суб'єктивних факторів, багато чого залишається цілком придатним. Так, навіть при поверхневому огляді стратегій кібербезпеки різних країн [3], можна виділити об'єднуючі ключові позиції:

– побудова урядової моделі, спрямованої на забезпечення кібербезпеки;

– визначення адекватного механізму, в основному у вигляді суспільно-державного

партнерства, який дозволить приватним та державним зацікавленим сторонам обговорювати та затверджувати політики, пов'язані з проблемою кібербезпеки;

– планування та визначення необхідних політик та регулюючих механізмів, чітке позначення ролей, прав та відповідальності для приватного та державного сектора у сфері протидії кіберзлочинності;

– визначення цілей та способів розвитку державних можливостей, а також необхідної законодавчої бази для участі у міжнародній боротьбі з кіберзлочинністю;

– визначення ключових інформаційних інфраструктур, у тому числі – основних активів, сервісів та взаємозалежностей;

– підвищення готовності, зменшення часу реакції на інциденти, розробка плану відновлення після збоїв та розробка механізмів захисту для ключових інформаційних інфраструктур;

– розробка системного та інтегрованого підходу до державного управління ризиками;

– визначення цілей інформаційних програм та затвердження їх у якості пріоритетних, покликаних прищепити користувачам нові моделі поведінки та моделі роботи;

– доказ необхідності нової програми освіти в якій робиться акцент на навчання IT-фахівців та професіоналів в області кібербезпеки;

– розвиток міжнародної співпраці.

Питання боротьби з кіберзлочинністю в нашій країні є дуже актуальним. У [4], присвяченій динаміці злочинів у сфері високих технологій в банківській системі, містяться дані про існування стійкої тенденції до збільшення кількості кіберзлочинів в Україні. При цьому, протягом останніх років кількість розкритих злочинів у сфері IT-технологій в Україні майже не змінилося, хоча в сфері комп'ютерних та Інтернет-технологій, кількість розкритих злочинів збільшилося в кілька разів. Така ситуація корелюється з перерахованими вище проблемами та свідчить про те, що збільшення рівня захищеності інформації в нашій країні потребує підтримки і розвитку.

Висновок. У середовищі, де постійно з'являються та еволюціонують кіберзагрози, не можна залишатися незахищеним: сформована в світі ситуація зобов'язує до постійного вдосконалення методів боротьби з кіберзлочинами та стимулює побудову державної моделі, спрямованої на забезпечення кібербезпеки країни.

Література

1. Войціховський, А. В. Міжнародне співробітництво у боротьбі з кіберзлочинністю [Електронний ресурс] // Портал : Національна бібліотека імені В. І. Вернадського. – Режим доступу \www/ URL : http ://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf. – Заголовок з контейнера, доступ вільний, 28.06.2013.

2. McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // Портал : An Intel Company. – Режим доступу \www/ URL : http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx. – Заголовок з екрану, доступ вільний, 28.06.2013.

3. Государственные стратегии кибербезопасности [Електронний ресурс] // Портал : Security Lab. – Режим доступу \www/ URL : http://www.securitylab.ru/analytics/429498.php. – Заголовок з екрану, доступ вільний, 28.06.2013.

4. Безпека банківської діяльності : монографія / Казакова Н. Ф., Панфілов В. І., Скачек Л. М., Скопа О. О., Хорошко В. О. ; за ред. проф. Хорошко В. О. – К. : ПВП «Задруга», 2013. – 282 с. – ISBN 978-966-2970-82-1.

References

1. Vojcihovs'kij, A. V. Mizhnarodne spivrobitnictvo u borot'bi z kiberzlochinnistju [Elektronnij re¬surs] // Portal : Nacional'na biblioteka imeni V. I. Vernads'kogo. – Rezhim dos-tupu \www/ URL : http ://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf. – Zagolovok z kontejnera, dostup vil'nij, 28.06.2013.

2. McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Elektronnij re¬surs] // Portal : An Intel Company. – Rezhim dos¬tupu \www/ URL : http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx. – Zagolovok z ekranu, dostup vil'nij, 28.06.2013.

3. Gosudarstvennye strategii kiberbezopasnosti [Elektronnij re¬surs] // Portal : Security Lab. – Rezhim dos¬tupu \www/ URL : http://www.securitylab.ru/analytics/429498.php. – Zagolovok z ekranu, dostup vil'nij, 28.06.2013.

4. Bezpeka bankivs'koї dijal'nosti : monografija / Kazakova N. F., Panfilov V. I., Skachek L. M., Skopa O. O., Horoshko V. O. ; za red. prof. Horoshko V. O. – K. : PVP «Zadruga», 2013. – 282 s. – ISBN 978-966-2970-82-1.

Йона О.О., Казакова Е.О.

МИРОВЫЕ ТЕНДЕНЦИИ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Показывается, что сложившаяся в мире ситуация с киберпреступностью, требует постоянного усовершенствованию методов борьбы с ней и построение модели, направленной на обеспечение кибербезопасности страны.

Ключевые слова: *киберпреступность, кибербезопасность, киберугрозы, тенденции, статистика.*

Yona O.O., Kazakova N.F.

GLOBAL TRENDS FIGHT CYBERCRIME

It is shown that the current situation in the world of cybercrime requires constant improvement of methods of struggle. Is it necessary to build a model that aims to ensure cyber security of the country.

Keywords: *cyber crime, cyber security, cyber threats, trends and statistics.*

Олена Олегівна Йона – здобувач кафедри Інформаційних систем в економіці, Одеський національний економічний університет

Надія Феліксівна Казакова – доцент кафедри Інформаційних систем в економіці, кандидат технічних наук, Одеський національний економічний університет

Рецензент: Петров Олександр Степанович – д.т.н, професор, СНУ ім. В. Даля, м. Луганськ.