

ТЕНДЕНЦІ ЗАХИСТУ ВІД КІБЕРЗЛОЧИНІВ

Надія Казакова¹, Олена Йона²

Кафедра Інформаційних систем в економіці,
Одеський національний економічний університет,
Україна, м. Одеса, вул. Преображенська, 8
1. kaz2003@ukr.net
2. eyona@mail.ru

It is shown that the current situation in the world of cyber-crime 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.

I. ВСТУП

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.

II. ПРОБЛЕМА

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.

III. АНАЛІЗ ДОСЛІДЖЕНЬ, МЕТА

Питання, винесене в заголовок статті, з різних 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. Т.ч., *метою статті*, зважаю-

чи на зазначене та з врахуванням матеріалів, які доступні в мережі Інтернет, є стисле узагальнення світових тенденцій боротьби з кіберзлочинністю.

IV. РЕЗУЛЬТАТИ

У 2012 році американська компанія, розробник антивірусного програмного забезпечення McAfee, що належить Intel Corporation, виступила спонсором у створенні глобального звіту про стан світової кібербезпеки. 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-технологій, 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&DefenceAgenda 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 – таблиця приводиться у доповіді. Згідно до неї 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&DefenceAgenda, неясно, чи були виставлені якісь бали для України.

Зі звіту Security&DefenceAgenda виділено статистику результатів опитування експертів. Статистика приводиться у доповіді.

Звіт Security&DefenceAgenda містить велику кількість зауважень від групи експертів. Найбільш суттєві з них приведено у доповіді. Втім, практично всі фахівці кожної з 27 країн, які були опитані в ході складання звіту, однак 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 прийнятті управляючих рішень.

Європейське агентство з мережевої та інформаційної безпеки – ENISA, у своїй «Програмі надійності та захисту ключової інформаційної інфраструктури» –

СПР, як і експерти, які були залучені Security&DefenseAgenda, також наполягає на необхідності налагодження співпраці з метою гарантій узгодженості характерних методик кіберборотьби.

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 кіберзлочинністю 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, можна виділити об'єднуючі ключові позиції (наводяться у доповіді).

Питання боротьби з кіберзлочинністю в нашій країні є дуже актуальним. У літературі до цих тез, яка присвяченій динаміці злочинів у сфері високих технологій в банківській системі та інших сферах людської діяльності, містяться дані про існування стійкої тенденції до збільшення кількості кіберзлочинів в Україні. При цьому, протягом останніх років кількість розкритих злочинів у сфері ІТ-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] Скопа, О. О. Роль телекомунікацій в сучасному бізнесі [Текст] / О. О. Скопа, Н. Ф. Казакова // Наукові праці УДАЗ. – Одеса : УДАЗ. – 1999. – № 2. – С. 11-12.
- [2] Йона, О. О. Світові тенденції боротьби з кіберзлочинністю [Текст] / О. О. Йона, Н. Ф. Казакова // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ : СНУ ім. В. Даля. – 2013. – № 15(204). – Ч. 1. – С. 59-62.
- [3] Казакова, Н. Ф. Міжнародна регламентація правового регулювання та стандартизації аудиту інформаційної безпеки [Текст] / Н. Ф. Казакова, Е. А. Плешко, К. Б. Айвазова // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ : СНУ ім. В. Даля. – 2013. – № 15(204). – Ч. 1. – С. 172-181.
- [4] Казакова, Н. Ф. Доповнення до концепції інформаційної безпеки [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. – К. : Державний науково-дослідний інститут МВС України. – 2010. – № 3(22). – С. 74-80.
- [5] Зеленцова, Ж. Ю. Конвергенція глобальної мережі як новий етап розвитку: Обзор инфраструктурных решений и технологий с целью нахождения решений для повышения безопасности обработки данных при облачных вычислениях [Текст] / Ж. Ю. Зеленцова, Н. Ф. Казакова // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля. – 2013. – № 4(12). – С. 23-40.
- [6] Казакова, Н. Ф. Проблеми правового забезпечення захисту баз даних [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля. – 2012. – № 2(8). – С. 73-76.
- [7] Удосконалення принципів та методів інформаційного забезпечення, інформаційної та фінансово-економічної безпеки підприємств та організацій сфери економіки, бізнесу та фінансів [Звіт про НДР] : (пром. ж.) / О. О. Скопа, Н. Ф. Казакова, О. В. Орлик, Ю. В. Щербина, А. О. Петров, С. Л. Волков, О. І. Мацків, О. Г. Єсіна, А. Ю. Вакула, О. О. Фразе-Фразенко, А. В. Мінін, О. Ю. Йона, Є. В. Вавілов, К. Б. Айвазова // ОНЕУ ; кер. О. О. Скопа. – 0112U007713. – Одеса, 2013. – 236 с.
- [8] Казакова, Н. Ф. Аналіз напрямів розвитку інформаційної безпеки у комп'ютерних системах та мережах на основі застосування програмних засобів захисту інформації [Текст] / Н. Ф. Казакова // Вісник Львівського національного аграрного університету: Агроінженерні дослідження. – Львів : Львівськ. нац. агроуніверситет. – 2010. – № 14. – С. 47-57.
- [9] Скопа, А. А. Політика предупреждения угроз информационной безопасности в практической деятельности Одесского филиала ОАО «Укртелеком» [Текст] / А. А. Скопа, Н. Ф. Казакова, С. Т. Сорока // Вісник Національного технічного університету «ХПІ». – Х. : НТУ «ХПІ». – 2012. – № 17. – С. 42-47.
- [10] Казакова, Н. Ф. Принципи побудови захищених інтелектуальних мереж [Текст] / Н. Ф. Казакова // Вісник ДУІКТ. – К. : ДУІКТ. – 2009. – № 4. – Т. 7. – С. 381-388.
- [11] Казакова, Н. Ф. Автоматизація процесу адаптації інформаційних систем до інцидентів інформаційної безпеки / Н. Ф. Казакова, Є. В. Вавілов // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля. – 2013. – № 4(12). – С. 49-56.
- [12] Скопа О.О., Казакова Н.Ф. Аналіз розвитку сучасних напрямів інформаційної безпеки автоматизованих систем // Системи обробки інформації. – Випуск № 7(79): Безпека та захист інформації в інформаційних системах. – Харків: Харківський ун-т Повітряних Сил ім. І. Кожедуба. – 2009. – С. 48-54.

- [13] Хорошко, В. О. Наукові задачі синтезу організаційно-технологічної схеми створення програмного забезпечення для комп'ютерних мереж з обмеженим доступом [Текст] / В. О. Хорошко, Н. Ф. Казакова // Захист інформації. – К. : НАУ. – 2009. – № 4(45). – С. 11-18.
- [14] Казакова, Н. Ф. Повышение адаптивности и достоверности вероятностной модели оценки живучести системы защиты шифрования [Текст] / Н. Ф. Казакова, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля. – 2009. – № 2(2). – С. 69-73.
- [15] Казакова, Н. Ф. Исследование информационных потоков в комплексных системах защиты информации и метод расчета пропускной способности [Текст] / Н. Ф. Казакова, Е. О. Тискина, В. А. Хорошко // Інформаційна безпека. – Луганськ : СНУ ім. В. Даля. – 2009. – № 2(2). – С. 105-115.
- [16] Казакова, Н. Ф. Організація процесу розробки програмного забезпечення для захищених інформаційних систем [Текст] / Н. Ф. Казакова // Сучасний захист інформації. – К. : ДУІКТ. – № 2. – С. 48-56.
- [17] Казакова, Н. Ф. Застосування програмно реалізованого прогностичного контролю для вирішення практичних завдань забезпечення якості надання послуг у захищених інформаційних мережах [Текст] / Н. Ф. Казакова // Сучасна спеціальна техніка. – К. : Державний науково-дослідний інститут МВС України. – 2012. – № 2(29). – С. 86-95.
- [18] Кобозева, А. А. Стеганографический метод обеспечения информационной безопасности морской связи [Текст] / А. А. Кобозева, И. И. Мараква, А. А. Скопа // Збірник наукових праць НУК. – Николаев : НУК. – 2006. – № 3(408). – С. 155-161.
- [19] Щербина, Ю. В. Проблемы оценки защищенности автоматизированных систем [Текст] / Щербина Ю.В., Скопа А.А. // Захист інформації. – К. : ДУІКТ. – 2008. – № 4(41). – С. 23-29.
- [20] Мінін, А. В. Біноміальні моделі випробування живучості захищених інформаційних каналів [Текст] / А. В. Мінін, О. О. Скопа, М. Александер // Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ : СНУ ім. В.Даля. – 2012. – № 8(179). – Ч. 1. – С. 42-58.
- [21] Щербина, Ю. В. Принципи вибору формальних параметрів при побудові профілей захисту інформаційних ресурсів [Текст] / Ю. В. Щербина, С. Л. Волков, О. О. Скопа // Восточно-Европейский журнал передовых технологий. – Х. : Технологический центр. – 2012. – № 5/2(59). – С. 31-33.
- [22] Скопа, О. О. Безпека фінансового ринку та фінансової стабільності як суспільне благо [Текст] / О. О. Скопа, О. О. Йона // Вчені записки університету «КРОК». Серія: Економіка. – К. : Ун-т економіки та права «Крок». – 2012. – № 32. – Т. 1. – С. 117-122.
- [23] Скопа, О. О. Проблематика якості послуг інтернет-провайдерів [Текст] / О. О. Скопа, С. Л. Волков, К. Б. Айвазова // Збірник наукових праць Одеської державної академії технічного регулювання та якості. – Одеса : ОДАТРЯ. – 2013. – № 1(2). – С. 27-31.
- [24] Скопа, О. О. Інтелектуальні автономні системи: концептуальні положення створення та функціонування [Текст] / О. О. Скопа, Є. В. Вавілов // Бюлетень інтелекту. – Харків : ХНУРЕ. – 2013. – № 1(80). – С. 35-40.
- [25] 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.

ТЕНДЕНЦІЇ ЗАХИСТУ ВІД КІБЕРЗЛОЧИНІВ. *Показується, що сформована в світі ситуація з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинцями та побудову моделі, спрямованої на забезпечення кібербезпеки країни.*

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

ТЕНДЕНЦИИ ЗАЩИТЫ ОТ КИБЕРПРЕСТУПЛЕНИЙ. *Показывается, что сложившаяся в мире ситуация с киберпреступностью, требует постоянного усовершенствования методов борьбы с ней и построение модели, направленной на обеспечение кибербезопасности страны.*

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

TRENDS OF PROTECTION AGAINST CYBER CRIMES. *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.

Надія Феліксівна Казакова, Одеський національний економічний університет, доцент кафедри Інформаційних систем в економіці, кандидат технічних наук, 050-512-98-99; e-mail: kaz2003@ukr.net
Олена Олегівна Йона, Одеський національний економічний університет, викладач кафедри Інформаційних систем в економіці, 050-694-77-44; e-mail: eynona@mail.ru