ISSN 2411-3816

УДК 004.621.3

В.Д. Козюра,
кандидат технічних наук, доцент, професор Національної академії Служби безпеки України, м. Київ,
В.О. Хорошко,
доктор технічних наук, професор, професор Національного авіаційного університету, м. Київ

СИСТЕМА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В УКРАЇНІ

У статті розглянуті загрози кібербезпеці та національній безпеці України. До переліку протиправних дій віднесено: несанкціоноване втручання в роботу комп'ютерів та абонентської системи; несанкціонований збут або розповсюдження інформації з обмеженим доступом; створення та використання шкідливих програмного забезпечення та технічних засобів; несанкціоновані дії з інформацією, яка обробляється в комп'ютерах; здійснення несанкціонованого доступу до інформації в інформаційній системі; незаконне використання чи розповсюдження копій баз даних таких систем тощо.

Для здійснення кібернетичної безпеки України слід: провести огляд кібербезпекової сфери держави, що дозволив би чітко визначити сучасний її стан; розробити на підґрунті моделей розвитку світового кібернетичного простору власну модель та реалізувати її; впорядкувати політику держави у сфері інформаційної та кібернетичної безпеки.

Ключові слова: *кібербезпека, кіберпростір, кіберзагроза, інформаційна безпека, інформаційний простір.*

В статье рассмотрены угрозы кибербезопастности и национальной безопасности Украины. В перечень противоправных действий отнесены: несанкционированное вмешательство в работу компьютеров и абонентской системы; несанкционированный сбыт или распространение информации с ограниченным доступом; создание и использование вредоносных программного обеспечения и технических средств; несанкционированные действия с информацией, обрабатываемой в компьютерах; осуществление несанкционированного доступа к информации в информационной системе; незаконное использование или распространение копий баз данных таких систем и тому подобное.

Поэтому для осуществления кибернетической безопасности Украины следует: провести обзор кибербезопасности сферы страны, который позволил бы четко определить современное ее состояние; разработать на основе моделей развития мирового кибернетического пространства собственную модель и реализовать ее, упорядочить политику государства в сфере информационной и кибербезопастности.

Ключевые слова: *кибербезопасность, киберпространство, киберугрозы, информационная безопасность, информационное пространство.*

Paper deals with the threats to cybersecurity and national security of Ukraine. Therefore, the list of unlawful actions includes: unauthorized interference with the work

of computers and subscriber system; unauthorized sales, or distribution of restricted information; creation and use of malicious software and hardware; unauthorized actions and information that is processed in computers; unauthorized access to information in the information system; illegal use or distribution of copies of databases of such systems, etc.

Therefore, in order to implement the cybernetic security of Ukraine, it is necessary: to conduct an overview of the cybersecurity sphere of the state, which would allow to determine clearly its current state; to develop, on the basis of models of development of the world cybernetic space, its own model, and to realize it; to regulate state policy in the field of informational and cybernetic security.

Keywords: *cybersecurity, cyberspace, cyber threats, information security, information space.*

В Україні деструктивні інциденти (рис. 1) у сфері високих технологій, під якими розуміємо порушення встановленого рівня їх безпеки, набули значних масштабів, їх поява, починаючи з кінця минулого тисячоліття, вже неодноразово зафіксована [1; 2; 3] й, як і для інших країн світу, дає підстави стверджувати про стійку тенденцію щодо збільшення їх кількості [4].

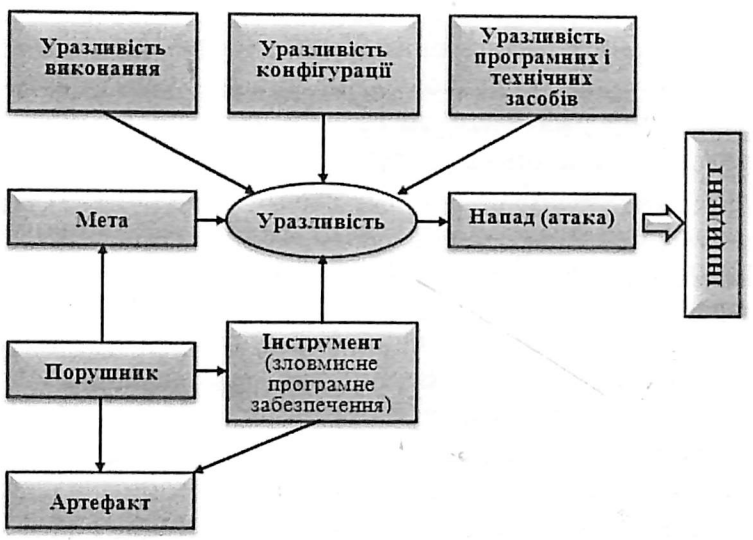

Рис. 1. Діаграма виникнення інциденту у сфері високих технологій

Такий стан справ простежується останнім часом, перш за все, у сфері комп'ютерних та Інтернет-технологій, де, наприклад, лише за період з 2005 по 2016 рік кількість викритих інцидентів збільшилася приблизно у 2,7 рази.

Для розв'язання інцидентів, як свідчать результати проведеного аналізу, порушники використовують певні технології та інструменти, що передбачають використання уразливостей у процесах виконання обраної послідовності дій або в конфігурації системи захисту та використовуваних нею програмного забезпечення (ПЗ), технічних засобів (ТЗ), а також створення уразливостей, якщо таких не існує. Саме тому найбільш пріоритетним напрямом керівництво України вважає нині реформування інформаційної безпеки, доктрина якої затверджена Указом Президента України № 514/209 від 8 липня 2009 року (зараз дороблюється). Одним із головних завдань доктрини на державному рівні визначено забезпечення

ISSN 2411-3816

конфіденційності, цілісності та доступності до інформації в національних інформаційних ресурсах (ІР) шляхом створення надійної системи захисту людини, суспільства та держави в цілому від впливу внутрішніх і зовнішніх, навмисних та/або випадкових кібернетичних втручань і загроз.

Ураховуючи це вже зараз у Адміністративному та Кримінальному кодексах України до переліку протиправних дій, які зусиллями терористичних і кримінальних кіберугруповань, хакерів-одинаків та/або певних спеціальних служб можуть створювати загрозу національним інтересам й, перш за все, кібербезпеці нашої держави, віднесено:

– несанкціоноване втручання в роботу комп'ютерів та абонентської системи (АС);

– несанкціонований збут або розповсюдження інформації з обмеженим доступом (ІзОД);

– створення та використання шкідливих ПЗ і ТЗ;

– несанкціоновані дії з інформацією, яка обробляється в комп'ютерах та комп'ютерних мережах;

– здійснення незаконного доступу до інформації в інформаційній системі (ІС);

– незаконне виготовлення чи розповсюдження копій баз даних таких систем тощо.

Протидіяти таким діям на теренах України нині спроможні:

– центральні органи виконавчої влади, що реалізують державну політику, перш за все, у сфері інформатизації та телекомунікацій, захисту державних ІР в інформаційно-телекомунікаційних системах (ІТС), а також криптографічного та технічного захисту інформації;

– органи державної влади, підприємства, організації (зокрема приватні) та установи, що експлуатують об'єкти критично важливої інфраструктури або здійснюють господарську діяльність у сфері захисту інформації в ІТС;

– Національний банк України, який формує та реалізує державну політику із забезпечення інформаційної та кібербезпеки банківських установ;

– підрозділи спеціального призначення, що виконують завдання із забезпечення кібернетичної безпеки України на кшталт адекватного реагування на прояви агресій потенціальних протиборчих сторін із застосуванням кібернетичної зброї, здійснюють досудове слідство у справах про злочини у сфері інформаційних технологій;

– оператори (провайдери) телекомунікацій тощо.

Тим не менше все це, з огляду на тенденції розвитку національного кібернетичного простору, потребує від України координації зусиль державного і приватного секторів у протидії новим викликам в інформаційній сфері та вказує на необхідність подальшого секторального вироблення принципів і механізмів реагування на можливі комп'ютерні інциденти.

Серед підрозділів та формувань спеціального призначення найбільше навантаження в ході вирішення завдань щодо протидії внутрішнім і зовнішнім загрозам національної безпеки України кібернетичного характеру останнім часом лягає на:

– Державну службу спеціального зв'язку та захисту інформації (ДССЗЗІ) України, що реалізує державну політику в сфері захисту інформації в інформаційно-телекомунікаційних мережах;

– Службу безпеки України, що реалізує державну політику у сфері охорони інформації з обмеженим доступом, яка є власністю держави;

– Міністерство внутрішніх справ України, що здійснює досудове слідство у справах про злочини у сфері інформаційних технологій;

– Службу зовнішньої розвідки України (СЗР) [3; 4; 5; 6].

У складі ДССЗЗІ України виконання завдань з визначення рівня та порядку захисту від кібернетичних загроз інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем об'єктів критично важливої інформаційної інфраструктури залежно від категорій, до яких ці об'єкти віднесено, покладено на затверджений у 2007 році Центр реагування на комп'ютерні інциденти, який нині пройшов повну акредитацію в міжнародних інституціях та є частиною всесвітньої організації FIRST.

У червні 2009 року на виконання статті 35 Конвенції про кіберзлочинність, ратифікованої Законом України від 07.09.2005 № 2824-IV, при СБ України на базі спеціального підрозділу для боротьби з кіберзагрозами утворений Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. У рамках мережі міжнародних контактних пунктів країн "Великої Сімки" [5] він співпрацює з ФБР, Секретною службою Великобританії, Поштовою інспекційною службою США, Національною поліцією Королівства Нідерландів, CISSS Франції, ВКА Німеччини, МНБ Казахстану, ФСБ Росії та на виконання вимог Конвенції реалізує заходи, що забезпечують протидію кіберзлочинності. Окрім цього, керівництвом СБ України запропонована модель організаційної структури Єдиної загальнодержавної системи протидії кіберзлочинності (ЄЗДСПК), Положення про яку затверджено Постановою КМ України від 15 серпня 2007 р. № 1051, а рішення щодо початку її створення ухвалено Указом Президента України "Про виклики та загрози національній безпеці України у 2011 році" від 10 грудня 2010 р. № 1119/2010. У рамках ЄЗДСПК передбачається розгорнути:

– національну систему моніторингу та реагування на загрози безпеці кіберпростору;

– національну систему захисту критично-важливої інфраструктури;

– системи заходів з нівелювання загроз і вразливості кіберпростору тощо.

У перспективі система має об'єднати спецслужби, правоохоронні органи, органи державного регулювання у сфері інформатизації, телекомунікації та захисту інформації для своєчасного виявлення, протидії і розслідування злочинних проявів з використанням інформаційних технологій, у тому числі у взаємодії зі структурами приватної форми власності, науковими та навчальними закладами у сфері інформаційної безпеки [5]. Важливе значення в її діяльності має бути приділене вивченню заходів забезпечення, перш за все, кібернетичної безпеки.

Усвідомлюючи ступінь та динаміку поширення комп'ютерних інцидентів теренами України, у липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, був утворений новий структурний підрозділ – Департамент боротьби з кіберзлочинністю і торгівлею людьми МВС України [7]. На нього покладаються завдання з формування та реалізації державної політики у цій сфері правоохоронної діяльності, напрацювання методичних рекомендацій протидії злочинам такої категорії, організація міжнародного співробітництва у справах про комп'ютерні правопорушення, розробка та

ISSN 2411-3816

внесення відповідних змін до чинного законодавства. Крім того, до обов'язків цього підрозділу входить виявлення та документування організованих груп транснаціонального і регіонального характеру, учасники яких спеціалізуються на вчиненні злочинів із використанням високих технологій та телекомунікаційних систем.

На військовому рівні завдання щодо планування та реалізації заходів протидії і нейтралізації кіберзагроз національним інтересам України у воєнній сфері, підготовки кібернетичної безпеки об'єктів критично важливої інформаційної інфраструктури держави до функціонування в особливий період та в умовах воєнного стану, впровадження новітніх інформаційних технологій у сфері оборони головним чином покладені на Генеральний штаб (ГШ) Збройних сил (ЗС) України, зокрема, на Головне управління зв'язку та інформаційних систем ГШ ЗС України, Центральне управління захисту інформації та криптології ЗС України, Департамент розробок та закупівлі ОВТ МО України, а також на Головне управління розвідки МО України [7]. Нині, враховуючи, що відповідно до статей 3, 10 та 11 Закону України "Про оборону України" одним із заходів підготовки держави до оборони в мирний час є входження України у світовий інформаційний простір та створення і захист власного інформаційного та кіберпросторів, у ГШ ЗС України розпочато процес створення системи забезпечення інформаційної безпеки України у воєнній сфері та кібернетичної безпеки у сфері оборони.

На ефективність діяльності спеціальних структурних підрозділів ДССЗЗІ, СБ, МВС, СЗР та МО України значною мірою впливає відсутність у вітчизняному законодавстві визначень, перш за все, таких термінів, як "кіберзахист", "кібербезпека", "комп'ютерна злочинність" і "комп'ютерний тероризм". Ураховуючи це, керівництвом держави здійснюються певні кроки для того, щоб максимально наблизити Україну до міжнародних позицій вирішення цих проблемних питань.

Зважаючи на певні труднощі, з якими фахівці з кіберзахисту від СБ, ДССЗЗІ, МО і МВС України стикаються в процесі роботи, та неможливість самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному і кіберпросторах, з плином часу настала гостра потреба в пошуку ними шляхів співробітництва з аналогічними організаціями світового суспільства. Фактично програмним документом для нашої держави на підтвердження цьому став вислів Співголови Спільної робочої групи Україна – НАТО з питань воєнної реформи, згідно з яким: "суттєво підвищити рівень безпеки кіберпростору" сучасного інформаційного суспільства можна лише "завдяки тісній міждержавній співпраці, використовуючи для цього всі наявні можливості і механізми, які є в розпорядженні кожної з країн" [6].

Викладене вище дає підстави стверджувати, що з моменту здобуття незалежності Україна як самодостатня і суверенна держава йде шляхом налагодження співробітництва з міжнародними інституціями, прагне створити комплексну систему протидії внутрішнім і зовнішнім загрозам власному кібернетичному простору. Тим не менше, як зазначають вітчизняні та західні фахівці, нині існує ціла низка проблем, що заважають нашій державі, яка прагне до Європейського співтовариства, це зробити. До найбільш значущих серед них слід віднести:

– деградацію науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інфосфері та низький рівень конкурентоздатності в ній;

– значну уразливість інфосфери України через надмірно широке впровадження до неї західних програмних продуктів та використання матеріально-технічних засобів іноземного виробництва;

– непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами та силовими структурами України, що спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення кваліфікованими фахівцями з цих питань;

– відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати та координувати діяльність зазначених правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному та кіберпростору України та керувати проведенням комплексних навчань з проблеми забезпечення кібернетичної безпеки держави в інфосфері;

– відсутність єдиного понятійно-термінологічного поля кібербезпеки України як головної складової інформаційної безпеки та системних нормативно-правових документів, які б регламентували діяльність зазначених відомств, правоохоронних і силових структур у сфері кіберзахисту тощо.

Такий стан справ фактично є каталізатором для реалізації втручань і загроз в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами її критично важливої інформаційної (кібернетичної) інфраструктури, виникнення техногенних катастроф тощо. Це, у свою чергу, вимагає від керівництва країни формування надійної системи кібернетичної безпеки національних інтересів шляхом започаткування низки міжвідомчих, а можливо, й міждержавних ініціатив на кшталт:

1) проведення аналізу ІТ-ринків та організації взаємодії ІТ-мереж;

2) визначення понятійно-категорійного апарату і потенційних загроз власній кібернетичній безпеці;

3) формування критеріїв віднесення об'єктів кіберпростору до критично важливої інформаційної та кіберінфраструктури;

4) удосконалення механізмів надання взаємодопомоги в технічних і методологічних аспектах випереджувального виявлення джерел, фіксації та оперативного обміну інформацією про факти здійснення кібератак;

5) вироблення та реалізація єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ-інфраструктури від деструктивного кібервпливу;

6) створення нової сучасної навчально-наукової бази для підготовки фахівців, здатних до оцінювання і прогнозування можливих ризиків від кібернападів та їх наслідків для інформаційної і кіберінфраструктури;

7) розробка єдиних механізмів аудиту та сертифікації програмно-апаратних комплексів, які використовуються в державній і військовій системах управління;

8) модернізації існуючих та/або розробки нових захищених інформаційних технологій, що впливають на:

– формування політики безпеки щодо здійснення контролю мережевого доступу;

– проведення на підставі існуючих рішень із забезпечення безпеки аналізу можливих ризиків та уразливостей;

– проектування систем захисту, а також формування вимог, що пред'являються до засобів і механізмів захисту, які використовуються;

– виділення ресурсів, ранжирування обраних контрзаходів за ступенем важливості, реалізацію та тестування найбільш пріоритетних;

– розробку та супроводження системи виявлення атак тощо;

9) організації міжвідомчої взаємодії та координації державних органів при оцінюванні реальних і потенційних загроз в інформаційній сфері, а також вироблення та реалізації заходів щодо їх усунення;

10) удосконалення міждержавних консультативних механізмів з питань законодавчого забезпечення і регулювання діяльності у сфері боротьби з кіберзлочинністю і кібертероризмом та внесення змін до низки існуючих нормативно-правових актів України, які регулюють відносини у сфері захисту інформації в інформаційно-телекомунікаційних системах та визначають загальні вимоги і організаційні засади забезпечення захисту інформації, що є власністю держави, або інформації з обмеженим доступом;

11) створення міжнародного експертного центру з питань регулювання взаємовідносин у галузі телекомунікацій та зв'язку тощо.

Окрім цього, було б раціональним удосконалити організаційно-правові норми міжнародної взаємодії з питань боротьби з кіберзлочинністю і кібертероризмом та запропонувати світовій спільноті внести зміни і доповнення до низки існуючих міжнародних нормативно-правових документів.

Висновки. У результаті це дасть можливість:

1) провести огляд кібербезпекової сфери держави, що дозволив би більш чітко визначити сучасний стан її нормативного забезпечення та основні проблеми, які мають бути вирішені вже найближчим часом;

2) розробити на підґрунті моделей розвитку світового кібернетичного простору (модель США та російсько-китайська модель) власну модель та реалізувати її (довідково: основним протиріччям цих двох моделей є те, що США пропонує розвиток Інтернету здійснювати вільно, не обмежуючи нормами національних законодавств, а РФ – КНР пропонують національні сегменти мереж Інтернету контролювати на законодавчому рівні);

3) впорядкувати політику України у сфері інформаційної та кібербезпеки і виробити так звані загальні правила поведінки в кіберпросторі;

4) визначитись з розбіжностями між військовими та цивільними об'єктами в інформаційному та кіберпросторах і сформулювати вимоги щодо безпеки для ключових доменів;

5) визнати міжнародним злочином проведення кібератак і кібероперацій на об'єктах інформаційної та кіберінфраструктури України, які спроможні привести до виникнення техногенних катастроф або надзвичайних ситуацій;

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Бутузов В.М., Павловський В.Д., Скалозуб Л.П.* та ін. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій; за ред. Романюка Б.В., Скулиша Є.Д. Київ: 2011. 404 с.

2. *Бутузов В.М.* Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз). Київ: КІТ, 2010. 408 с.

3. *Бурячок В.Л., Шарий О.В.* Кіберзлочинність і кібертероризм – загрози національній безпеці та інтересам України. Вісник воєнної розвідки. Київ: ВДА ГУР МО України. Вип. 21. 2010. С. 24–29.

4. *Семенов Ю.А.* Обзор материалов ведущих фирм, работающих в сфере сетевой безопасности. URL: http://book.itep.ru/10/2012.htm (дата звернення: 01.11.2017).

5. *Бурячок В.Л.* Основи формування державної системи кібернетичної безпеки. Київ: НАУ, 2013. 432 с.

6. *Пермяков О.Ю., Вернер І.С.* Інформаційне протиборство: реалії і тенденції. Арсенал XXI століття. 2002. № 2. С. 17–20.

7. Актуальні проблеми інформаційної безпеки України (Аналітична доповідь УЦЕПД). Національна безпека і оборона. 2014. № 1. С. 2–50.

Отримано 06.11.2017

Рецензент Рибальський О.В., д.т.н., проф.