ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.30.18607

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КІБЕРПРОСТОРІ

Володимир Хорошко[1], Михайло Шелест[2], Юлія Ткач[3], Михайло Шелест[3], Ігор Дюба[4]

[1]Національний авіаційний університет
[2,3,4] Національний університет «Чернігівська політехніка»

ХОРОШКО Володимир Олексійович, д.т.н., професор
Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функціонування складних систем.
Публикации: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

ШЕЛЕСТ Михайло Євгенович, д.т.н., професор
Рік та місце народження: 1954 рік, м. Ромни, Україна.
Освіта: Національний університет «Львівська політехніка».
Посада: професор кафедри кібербезпеки та математичного моделювання.
Наукові інтереси: інформаційна безпека, оцінювання вразливосте, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографія, підручники, навчально-методичні посібники та декларативні патенти.
E-mail: michel3141@gmail.com.
Orcid ID: 0000-0001-7110-4876.

ТКАЧ Юлія Миколаївна, д. пед. н., професор
Рік та місце народження: 1979, м. Чернігів, Україна.
Освіта: Чернігівський національний технологічний університет (зараз НУ "Чернігівська політехніка"), 2012 рік; Чернігівський державний педагогічний університет ім. Т.Г. Шевченка, 2001.
Посада: завідувач кафедри кібербезпеки та математичного моделювання з 2010 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 80 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: tkachym79@gmail.com.
Orcid ID: 0000-0002-8565-0525.

ДЮБА Ігор Миколайович, викладач
Рік та місце народження: 1986, м. Чернігів, Україна
Освіта: Чернігівський національний технологічний університет (зараз НУ "Чернігівська політехніка"), 2008 рік;
Посада: викладач кафедри кібербезпеки та математичного моделювання з 2023 р.
Наукові інтереси: програмування, кібербезпека, технології комп'ютерного зору.
E-mail: idyuba@gmail.com.
Orcid ID: 0009-0007-3669-6424.

Анотація. *На основі проведеного аналізу проблеми забезпечення інформаційної безпеки в кіберпросторі визначено джерела кібернетичних загроз, якими можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи терористи та екстремістські угрупування, транснаціональні корпорації та фінансово-промислові групи. Зроблено висновок, що забезпечення кібербезпеки вимагає узгодженого, комплексного підходу на чолі з державою, однак у тісному співробіт-*

ництві з приватним сектором та громадянським суспільством, без якого неможливо вирішити дане питання. Встановлено, що вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня та сфери організації захисту. В залежності від загроз уможливлюється завдання щодо диференціації як різних рівнів і видів загроз так і різних рівнів і видів захисту. Однак, загроза та небезпека є атрибутивними компонентами системи кібербезпеки, отже, їх існування та реалізація, а також негативні наслідки є природними компонентами системи інформаційної безпеки. Саме загрози та небезпека дають змогу побачити недоліки в системі управління кібербезпекою, і водночас слугують імпульсом до вдосконалення, тобто до розвитку. Отже, важливим методом забезпечення інформаційної безпеки є метод розвитку.

***Ключові слова**: інформаційна безпека, кіберпростір, кіберзлочинність, кібертероризм, кіберрозвідка, кібервійна.*

Постановка проблеми

Осмислення тероризму як соціально негативного явища стало предметом наукових розробок у 70-80 роках XX сторіччя, перед усім у частині опрацювання окремих сегментів юридичних, політичних, історичних, військових та інших наук. Однак, на сьогодні ця проблема не втратила своєї актуальності, навпаки, потребує комплексного вирішення. Це пов'язано зі світовими тенденціями щодо транскордонності тероризму, тобто вихід цього явища за межі певної держави, регіону чи інших континентів та спрямованість на планетарний масштаб. Коли йдеться про масштаби та всебічно багатовекторність тероризму третього тисячоліття слід наголошувати що він вимагає значних матеріальних ресурсів. За підрахунками деяких фахівців, мінімальний бюджет терористичних угрупувань становить майже 20 мільярдів доларів.

Сучасний світ потребує єдиних стандартів у сфері забезпечення кібербезпеки для того, щоб усі країни мали єдине розуміння кібернетичної загрози.

Сьогодні кіберзлочинність – масштабна проблема, а шкідливі програми поширюються з метою незаконного отримання грошей. Розвиток мережі інтернет став одним із ключових чинників, що визначили ці зміни. Компанії та деякі користувачі вже не мислять без цього своє життя, і все більше фінансових операцій проводиться все більше через Інтернет. Кіберзлочинці усвідомили які величезні можливості щодо «заробітку» грошей за допомогою шкідливого коду з'явилося останнім часом і багато із сучасних шкідливих програм створені на замовлення, при чому, або для терористів, або для подальшого продажу злочинцям.

Аналіз останніх досліджень і публікацій

Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежить від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційними та комунікаційними технологіями, або в більш широкому розумінні – кіберпростору. Водночас зростання залежності від інформаційно-телекомунікаційних технологій робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору. В цих умовах головним завданням держави є вжиття заходів що дозволять принципово зменшити (а подекуди унеможливити повністю) негативні наслідки від кібератак.

Джерелами кібернетичних загроз можуть бути міжнародні злочинні групи хакерів, окремі підготовлені у сфері інформаційних технологій злочинці, іноземні державні органи терористи та екстремістські угрупування, транснаціональні корпорації та фінансово-промислові групи, тощо. Є загроза використання проти інтересів України кібернетичних засобів не з середини держави, але й із-за меж її кордонів. Такою ж реальною є загроза використання української інформаційної структури як «транзитного майданчика» для приховування атак на інформаційну інфраструктуру третьої сторони.

Україна послідовно виходить з того, що кіберпростір є відкритим простором – відкритим до інновацій, вільного розповсюдження ідей, інформації та обміну думками.

Мета та постановка завдання

Заходи із забезпечення кібербезпеки жодним чином не можуть суперечити принципу гарантування прав та свобод українських громадян, в тому числі права на недоторканність приватного життя та свободи спілкування.

Забезпечення кібербезпеки вимагає узгодженого, комплексного підходу на чолі з державою, однак у тісному співробітництві з приватним сектором та громадянським суспільством, Без якого неможливо вирішити дане питання. Розглянемо основні загрози в сфері кібербезпеки відносно України.

Виклад основного матеріалу дослідження

Кібертероризм та кіберрозвідка

Ціль: низка вітчизняних підприємств, порушення роботи яких становить загрозу життю та здоров'ю громадян, може стати ціллю для здійснення терористичних актів, в тому числі із застосуванням сучасних інформаційних технологій. Не меншою загрозою є вчинення протиправних дій на шкоду третім країнам, що здійснюється із використанням вітчизняної інформаційної інфраструктури, що загрожують талому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем. Інформація з обмеженим доступом що циркулює в національних інформаційних ресурсах є стійким об'єктом зацікавленості з боку інших держав, організацій та осіб.

Крім того, все більшого поширення набуває політично вмотивована діяльність в кіберпросторі груп активістів, які здійснюють атаки на урядові та приватні сайти, що призводить до порушення роботи інформаційних ресурсів, а також репутаційних та матеріальних збитків.

Кіберзлочинність

Злочини з використанням сучасних інженерно-телекомунікаційних технологій стають вже звичайною проблемою в житті українських громадян. При цьому новітні технології застосовуються не лише для

скоєння традиційних видів злочинів, але й для скоєння нових видів злочинів, характерних перед усім для розвинутого інформаційного суспільства. Найбільше увага злочинів зосереджується на спробах порушення роботи або несанкціонованого використання можливостей інформаційних систем державного, кредитно-банківського, комунального, оборонного, виробничого секторів. Все ще актуальною залишається проблема боротьби із дитячою порнографією та порушення авторських та суміжних прав.

Кібервійна

Воєнна сфера зазнає чи не найдраматичніших змін внаслідок розбудови глобального кіберпростору. Більшість країн світу активно трансформують свої потенціали у сфері оборони у напрямі посилення кібернетичних можливостей ведення бойових дій та захисту від аналогічних дій з боку супротивника, оскільки все актуальнішими стають нові типи загроз. З урахуванням мережевоцентричної війни, яку веде росія проти України, ЗС України, оборонний потенціал нашої держави стає більш чутливим до кіберзагроз. Впровадження провідними країнами сучасних кіберозброєнь перетворює кіберпростір на окрему, поряд з традиційними земля, повітря, море, космос, сферу ведення бойових дій, а у найближчому майбутньому, рівень обороноздатності країни буде визначатись у тому числі наявністю у неї ефективних підрозділів для ведення бойових дій в кіберпросторі та здатність протистояти кіберзагрозам в сфері оборони, тобто кібервійськам.

Вразливість інформаційної інфраструктури держави

За останній час дедалі частіше об'єктами кібератак та кіберзлочинів стали інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які забезпечують безпеку, оборону, захист від надзвичайних ситуацій, а також сервери їх офіційних Internet представництв та електронної пошти. Різке збільшення зафіксованих випадків кібератак на державні інформаційні ресурси свідчить про посилення діяльності хакерських рухів з метою порушення роботи інформаційно-телекомунікаційних систем державних органів.

На базі того, що було раніше сказано сформулюємо принципи забезпечення кібербезпеки України. Реалізація основних засад забезпечення кібербезпеки України має здійснюватися при неухильному дотриманні таких принципів:

– верховенство права, законності та пріоритету, додержання прав і свобод громадян;

– невідворотності відповідальності за вчинення кіберзлочинів;

– пріоритетності запобіжних заходів;

– комплексного здійснення правових, організаційних, технічних, криптографічних, інформаційних та інших заходів;

– партнерство держави та приватного сектору з метою вироблення нових більш оптимальних рішень кіберзахисту;

– пріоритетного розвитку та підтримки вітчизняної науково-інформаційної сфери;

– відповідальності суб'єктів забезпечення кібербезпеки за захист національної інформаційної інфраструктури;

– дієвості, комплексності та постійності заходів забезпечення кібербезпеки держави;

– співпраці на міжнародному рівні, з метою вироблення єдиних підходів та ефективної взаємодопомоги протидій кіберзагрозам.

Протидія реальним загрозам та мінімізація потенційних загроз потребує низки кроків держави в ключових сферах життєдіяльності, що мають особливе значення для забезпечення кібербезпеки. З тією метою, держава у партнерстві з суспільством, недержавним та приватним сектором, а також громадянами, з метою посилення кібербезпеки України буде при формуванні власної політики кібербезпеки керуватися певними пріоритетами.

1. У зовнішньополітичній сфері:

– підвищити роль України як активного учасника формування стандартів світової політики по відношенню до кіберпростору;

– підтримувати міжнародні ініціативи у сфері кібербезпеки з урахуванням національних інтересів України;

– сприяти недопущенню мілітаризації;

– неухильно дотримуватись взятих на себе міжнародних зав'язувань в сфері кібербезпеки та боротьби з кіберзлочинністю;

– підвищувати рівень міжнародного співробітництва у сфері забезпечення кібербезпеки на загально державному та відомчому рівнях;

– сприяти створенню міжнародних правил поведінки держав у кіберпросторі та удосконаленню міжнародної нормативно-правової бази у відповідності до кібербезпекових викликів національній та міжнародній безпеці;

– підтримувати як існуючі багатосторонні навчання із протидії кібернападам на державну та приватну інформаційну інфраструктуру, так і ініціювати нові види таких навчань.

2. У сфері державної та внутрішньо-політичної безпеки:

– встановити обов'язкові вимоги щодо кіберзахисту критичних об'єктів національної інформаційної інфраструктури в незалежності від форми власності, порядок захисту та контролю за його дотримання;

– здійснювати заходи реформування системи захисту інформації з обмеженим доступом з урахуванням реалій сьогодення задля уникнення витоків таємної інформації;

– посилити боротьбу з кібертероризмом та кібершпигунством, захист від їх проявів критичних об'єктів національної інформаційної інфраструктури;

– забезпечити імплементацію Положення Ради Європи про кіберзлочинність у національне законодавство;

– удосконалити кримінальне законодавство, виділити окремі склади законів де об'єктом протиправних посягань є елементом національної критичної інформаційної інфраструктури;

– сприяти розвитку мережі команд реагування на комп'ютерні надзвичайні події.

3. У військовій сфері:

– здійснювати підготовку до застосування ЗсУ в умовах кібервійни;

– створення можливості для відбиття військових агресій в кіберпросторі з урахуванням нових викликів та загроз;

– захистити військову інформаційну інфраструктуру від реальних та потенційних кіберзагроз.

4. У соціальній, гуманітарній та науково-педагогічній сферах:

– розвивати та координувати науково-дослідні роботи у галузі кібербезпеки;

– забезпечити внесення змін до навчальних планів та програм середньої та вищої освіти, підготовки науково та науково-педагогічних кадрів, що спрямовані на інформування основних цільових груп про кіберзагрози та методи протидії їм;

– розробляти загальнодержавні програми підвищення рівня обізнаності населення щодо кіберзагроз;

– підтримування зусилля громадянського суспільства та бізнесу щодо підвищення обізнаності населення з актуальних кіберзагроз;

– сприяти більш активній політиці державних інституцій щодо інформування населення про кіберзагрози;

– сприяти розробці вітчизняної інноваційної продукції що може бути використана з метою посилення безпеки держави.

Щодо виконання принципів та положень кібербезпеки необхідно проводити аналіз стану забезпечення інформаційної безпеки у кіберпросторі. При цьому, вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня та сфери організації захисту. В залежності від загроз уможливлюється завдання щодо диференціації як різних рівнів і видів загроз так і різних рівнів і видів захисту. Що стосується інформаційної сфери безпеки в кіберпросторі то у ній зазвичай виділяють:

– програмно-технічні;

– управлінські;

– технологічні;

– мережевий;

– процедурний.

На програмно технічному рівні здійснюється ідентифікація та перевірка дійсності користувачів, управління доступом, протоколювання та аудит, криптографічне перетворення, сканування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація та контроль організаційних, технологічних і технічних заходів на всіх рівнях збоку єдиної системи кібербезпеки.

На технологічному рівні здійснюється реалізація політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій.

На мережевому рівні дана політика реалізується у формі координації дії компонентів системи управління, які пов'язані між собою однією метою.

На процедурному рівні вживаються заходи, що реалізуються обслуговуючим персоналом. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичних захист, підтримання працездатності, планування реанімаційних робіт та інше.

Захист інформації в кіберпросторі не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек, їх залежність як від рівня розвитку тієї чи іншої цивілізації, але й від контексту та оцінки, що проводиться, наявності всебічних даних по факторах загроз, алгоритм вирахування коефіцієнту ймовірності настання та розміру негативних наслідків, наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпеки.

Втім, не слід покладати надію на створення абсолютної системи безпеки, оскільки, як зазначається, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи кібербезпеки, отже, їх існування та реалізація, а також негативні наслідки є природними компонентами системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління кібербезпекою, і водночас слугують імпульсом до вдосконалення, тобто до розвитку. Отже, важливим методом забезпечення інформаційної безпеки є метод розвитку.

Висновки. У цілому ж слід зазначити, що вибір цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці у кіберпросторі становить собою важливу проблему і складову частину діяльності по реалізації основних напрямів державної політики у сфері національної та інформаційної безпеки.

У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, військового, політичного та інших станів суспільства, держави та особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

Список літератури

[1]. Закон України «Про національну безпеку України» [Електронний ресурс] / Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

[2]. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] / Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[3]. Закон України «Стратегія кібербезпеки України» [Електронний ресурс] / Режим доступу до ресурсу: https: // zakon.rada.gov.ua / laws / show /447/ 2021#Text.

[4]. Браіловський М.М. Аналіз кіберзахищеності інформаційних систем / М.М. Браіловський, С.В. Зибін,А.А. Кобозєва, В.О. Хорошко, Ю.Є. Хохлачова. К: ФОП Ямчинський О.В., 2021. Звос.

[5]. Грищук Р.В. Основи кібернетичної безпеки / Р.В. Грищук, Ю.Г. Даник. Житомир : ЖНАЕУ, 2016. 636 с.

[6]. Дубов Д.В. Кібезбезпека: світові тенденції та виклики для України /Д.В. Дубов, М.А. Ожеван. К: НІСД, 2011. 30 с.

[7]. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. К: ДУТ, 2015. 288 с.

[8]. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. К: ТОВ «СІК ГРУП Україна», 2015, 449 с.

УДК 004.056.5

Khoroshko V., Shelest M., Tkach Yu., Diuba I. Provision of information security in cyberspace

Abstract. *On the basis of the analysis of the problem of ensuring information security in cyberspace, the sources of cyber threats have been determined, which can be international criminal groups of hackers, individual criminals trained in the field of information technologies, foreign state bodies, terrorists and extremist groups, transnational corporations and financial and industrial groups. It was concluded that ensuring cyber security requires a coordinated, comprehensive approach led by the state, but in close cooperation with the private sector and civil society, without which it is impossible to solve this issue. It has been established that the choice of methods for analyzing the state of ensuring information security depends on the specific level and scope of the organization of protection. Depending on the threats, the task of differentiating both different levels and types of threats and different levels and types of protection becomes possible. However, threat and danger are attribute components of the cyber security system, therefore, their existence and implementation, as well as negative consequences, are natural components of the information security system. It is threats and danger that make it possible to see the shortcomings in the cyber security management system, and at the same time serve as an impetus for improvement, that is, for development. Therefore, an important method of ensuring information security is the development method.*

Keywords: *information security, cyber space, cybercrime, cyber terrorism, cyber intelligence, cyber war.*

Хорошко Володимир Олексійович, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Volodymyr Khoroshko, Professor of the Department of Information Technology Security of the National Aviation University.

Шелест Михайло Євгенович, професор кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Mykhailo Shelest, Professor of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University.

Ткач Юлія Миколаївна, завідувач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Yuliia Tkach, Head of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University.

Дюба Ігор Миколайович, викладач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Ihor Diuba, Lecturer of the Department of Cybersecurity and Mathematical Simulation, Chernihiv Polytechnic National University.

Отримано *17 лютого 2024 року*, затверджено редколегією *1 квітня 2024 року*